

CloudSecurityAlliance.CCSK.v2022-03-31.q113

Exam Code:	CCSK
Exam Name:	Certificate of Cloud Security Knowledge (v4.0) Exam
Certification Provider:	Cloud Security Alliance
Free Question Number:	113
Version:	v2022-03-31
# of views:	5021
# of Questions views:	1130
https://www.freepdfdumps.com/CloudSecurityAlliance.CCSK.v2022-03-31.q113.html	

NEW QUESTION: 1

Which form of storage has features are typically minimal. allowing you to only store, retrieve, copy and delete files as well as the ability to control which users can undertake these actions?

- A. Object Storage
- B. Volume Storage
- C. Ephemeral Storage
- D. Block Storage

Answer: A (LEAVE A REPLY)

Object Storage has features are typically minimal, allowing you to only store, retrieve, copy, and delete files as well as the ability to control which users can undertake these actions.

NEW QUESTION: 2

Which of the following help to intermediate IAM between an organization's existing identity providers and many different cloud services used by the organization?

- A. Federated Identity Provider
- B. Relying Party
- C. Cloud Access Security Broker
- D. Active Director

Answer: (SHOW ANSWER)

One of the better-known categories heavily used in cloud security is Federated Identity Brokers. These services help intermediate IAM between an organization's existing identity providers(internal Security Guidance v4.0 Copyright2017. Cloud Security Alliance. All rights reserved or cloud-hosted directories) and the many different cloud services used by the organization. They can provide web-based Single Sign

On(SS0). helping ease some of the complexity of connecting to a wide range of external services that use different federation configurations.

Reference: CSA Security Guidelines V.4(reproduced here for the educational purpose)

NEW QUESTION: 3

Cloud customer can do vulnerability assessment of their whole infrastructure on cloud just like they conduct vulnerability assessment of their traditional infrastructure.

- A. True
- B. False

Answer: (SHOW ANSWER)

It is false.

Customer will have to take permission and give notification to cloud service provider.

The cloud owner (public or private) will typically require notification of assessments and place limits on the nature of assessments. This is because they may be unable to distinguish an assessment from a real attack without prior warning.

Ref: CSA Security Guidelines V4.0

NEW QUESTION: 4

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 (LEAVE A REPLY)

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

NEW QUESTION: 5

"Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms" Which of the following characteristics defines this

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

Your SLA with your cloud provider ensures continuity for all services.

- A. True

B. False

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

Why is a service type of network typically isolated on different hardware?

- A. It requires distinct access controls
- B. It has distinct functions from other networks
- C. It requires unique security
- D. It manages resource pools for cloud consumers
- E. It manages the traffic between other networks

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 8

What is resource pooling?

- A. Placing Internet ("cloud") data centers near multiple sources of energy, such as hydroelectric dams.
- B. The dedicated computing resources of each client are pooled together in a colocation facility.
- C. None of the above.
- D. The provider's computing resources are pooled to serve multiple consumers.
- E. Internet-based CPUs are pooled to enable multi-threading.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 9

ENISA: A reason for risk concerns of a cloud provider being acquired is:

- A. Mass layoffs may occur
- B. Arbitrary contract termination by acquiring company
- C. Non-binding agreements put at risk
- D. Provider may change physical location
- E. Resource isolation may fail

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 10

Ensuring the use of data and information complies with organizational policies, standards and strategy- including regulatory, contractual, and business objectives, known as:

- A. IT Governance
- B. Data Governance
- C. Corporate Governance
- D. Enterprise Governance

Answer: ([SHOW ANSWER](#))

It is definition of Data Governance

NEW QUESTION: 11

Which of the following is a key consideration in Data security but does not feature in Data Security Life cycle?

- A. Storage Location
- B. Storage Device
- C. Storage protocol
- D. Access Method

Answer: A (LEAVE A REPLY)

The lifecycle represents the phases information passes through but doesn't address its location or how it is accessed.

NEW QUESTION: 12

An important consideration when performing a remote vulnerability test of a cloud-based application is to

- A. Obtain provider permission for test
- B. Use techniques to evade cloud provider's detection systems
- C. Use application layer testing tools exclusively
- D. Use network layer testing tools exclusively
- E. Schedule vulnerability test at night

Answer: A (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 13

Whose responsibility is to maintain security incident and event management(SIEM) capabilities in PaaS (Platform as a Service) model?

- A. Cloud Carrier
- B. Cloud Service provider
- C. Cloud Customer
- D. Cloud Access Security Broker

Answer: B (LEAVE A REPLY)

In forms of service models, it is cloud service provider's responsibility to maintain security incident and event management(SIEM) capabilities

NEW QUESTION: 14

Which data security control is the LEAST likely to be assigned to an IaaS provider?

- A. Encryption solutions
- B. Asset management and tracking
- C. Access controls
- D. Physical destruction
- E. Application logic

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 15

An important consideration when performing a remote vulnerability test of a cloud-based application is to

- A. Use network layer testing tools exclusively
- B. Use techniques to evade cloud provider's detection systems
- C. Schedule vulnerability test at night
- D. Obtain provider permission for test
- E. Use application layer testing tools exclusively

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

Who is responsible for Data Security in Software as a Service(SaaS) service mode?

- A. Cloud Service Provider
- B. Cloud Customer
- C. Cloud Carrier
- D. It's a shared responsibility between Cloud Service Provider and Cloud Customer

Answer: B ([LEAVE A REPLY](#))

Remember that data security will always remain responsibility of the cloud customer in all service models

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 17

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: ([SHOW ANSWER](#))

GRC is responsibility of the customer across all service models.

NEW QUESTION: 18

Who is responsible for infrastructure security in Infrastructure as a service(IaaS) model?

- A. Cloud Service provider
- B. Cloud Service User
- C. Cloud Service Architect
- D. Shared responsibility between cloud service provider and cloud service customer

Answer: (SHOW ANSWER)

Infrastructure security is shared responsibility between cloud service provider and cloud customer.

NEW QUESTION: 19

Which of the following ISO Standard provides Code of practice for information security controls based on ISO/IEC 27002 for cloud services?

- A. ISO 27018
- B. ISO 27034
- C. ISO 27032
- D. ISO 27017

Answer: D (LEAVE A REPLY)

ISO 27017 provides Code of practice for information security controls based on ISO/IEC27002 for cloud services.

NEW QUESTION: 20

The most pragmatic option for data disposal in the cloud is which of the following?

- A. Overwriting
- B. Crypto shredding
- C. Melting
- D. Cold fusion

Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

Which one of the following is NOT one of phases for cloud auditing?

- A. Define Audit objectives
- B. Conduct Audit
- C. Report data breaches
- D. Report lesson learned

Answer: C (LEAVE A REPLY)

Reporting data breaches is not part of Auditing and not a function of Auditors.

NEW QUESTION: 22

According to ISO 27018. data processor has explicit control over how CSPs are to use PII.

- A. True

B. False

Answer: B (LEAVE A REPLY)

In ISO 27018, it is the customer who has explicit right over how CSPs will use their information

NEW QUESTION: 23

According to CSA Security Guidelines, there are four layers of Logical Model for cloud computing. Which of the following is not one of the layers as defined by Cloud Security Alliance?

- A. Infrastructure**
- B. Metastructure**
- C. Applistructure**
- D. Softstructure**

Answer: D (LEAVE A REPLY)

The four layers of Logical Model for cloud computing according to Cloud Security Alliance are:

1. Infrastructure: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts.
2. Metastructure: The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.
3. Infostructure: The data and information. Content in a database, file storage, etc.
4. Applistructure: The applications deployed in the cloud and the underlying application services used to build them. For example, Platform as a Service features like message queues, artificial intelligence analysis, or notification services.

NEW QUESTION: 24

Due to multi-tenancy nature of cloud. there is the possibility that data belonging to one customer will be read or received by another. This is known as:

- A. Information Bleed**
- B. Wilful data disclosure**
- C. Data dispersion**
- D. Data disclosure**

Answer: A (LEAVE A REPLY)

Information Bleed With multiple customers processing and storing data over the same infrastructure, there is the possibility that data belonging to one customer will be read or received by another.

Moreover, even if this does not happen with raw data, it might be possible for one customer to detect telltale information about another customer's activity, such as when the customer is processing data, how long the procedure takes, and so on.

NEW QUESTION: 25

Which of the following is not one of the categories of risks as defined in, ENISA (European Network and Information Security Agency) document on Security risk and recommendation?

- A. Technical Risk
- B. Legal Risk
- C. Environmental Risk
- D. Policy and organisational risk

Answer: C (LEAVE A REPLY)

Environmental Risk are not defined as a category in the ENISA document however. all the other three are defined as categories.

NEW QUESTION: 26

Multi-tenancy and shared resources are defining characteristics of cloud computing. However, mechanisms separating storage, memory, routing may fail due to several reasons. What risk are we talking about?

- A. Isolation Failure
- B. Isolation Escalation
- C. Separation of Duties
- D. Route poisoning

Answer: (SHOW ANSWER)

According to ENISA (European Network and Information Security Agency) document on Security risk and recommendation, Isolation failure is considered as one of the top risk and is defined as follows Multi- tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g, so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional Oss.

NEW QUESTION: 27

Amount of risk that the leadership and stakeholders of an organization are willing to accept. is known as:

- A. Residual Risk
- B. Risk Tolerance
- C. Risk Limitation
- D. Risk Avoidance

Answer: (SHOW ANSWER)

Risk tolerance is the amount of risk that the leadership and stakeholders of an organization are willing to accept.

NEW QUESTION: 28

When a cloud customer uploads PII to a cloud provider, who becomes ultimately responsible for the security of that PII?

- A. Cloud Provider
- B. Regulator
- C. Cloud customer
- D. The individuals who are the subject of the PII

Answer: C (LEAVE A REPLY)

Under current law, the data owner is responsible for any breaches that result in unauthorized disclosure of PII; this includes breaches caused by contracted parties and outsourced services. The data owner is the cloud customer.

NEW QUESTION: 29

Big data includes high volume, high variety, and high velocity.

- A. True
- B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 30

Which of the following is most commonly used to program Application Programming Interface(API)?

- A. SOAP
- B. JSON
- C. HTTP
- D. REST

Answer: D (LEAVE A REPLY)

APIs are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over HTTP/S and thus work well across diverse environments.

Reference: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

NEW QUESTION: 31

The entity that has the primary relationship with an individual from whom his/her PII is collected is known as:

- A. Data Controller
- B. Data processor
- C. Data custodian
- D. Data Manager

Answer: A (LEAVE A REPLY)

The data controller (typically the entity that has the primary relationship with an individual) is prohibited from collecting and processing personal data unless certain criteria are met.

For example, if the data subject has consented to the collection and proposed uses of his or her data, then the controller may collect and process data, according to the consent agreement.

Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:
https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

Which of the following are key Data functions?

- A. Access, Process & Store
- B. Access, Process & Save
- C. Access, Procure & Store
- D. Access, Procure & Save

Answer: A (LEAVE A REPLY)

The key data functions are Access, process & Store

NEW QUESTION: 33

Exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations, are called:

- A. Honepots
- B. Threats
- C. Threat Agents
- D. Vulnerabilities

Answer: D (LEAVE A REPLY)

NEW QUESTION: 34

Cloud Service Provider and Cloud Customer are jointly responsible for ownership of the all risks in shared responsibility model for security across all service models.

- A. True
- B. False

Answer: B (LEAVE A REPLY)

This is false. This is again a tricky question and one should be careful when answering this type of question. It is the cloud customer is who is ultimately responsible for the ownership

of risk in the cloud environment. Consumer just passes some of risk management responsibilities to the cloud service provider.

NEW QUESTION: 35

Which statement best describes the impact of Cloud Computing on business continuity management?

- A. Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
- B. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
- C. Geographic redundancy ensures that Cloud Providers provide highly available services.
- D. A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
- E. The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 36

Which of the following is an assurance program and documentation registry for cloud provider assessments?

- A. CSA Cloud Controls Matrix
- B. CSA Consensus Assessments Initiative Questionnaire
- C. CSA Star
- D. CSA governance charter

Answer: C (LEAVE A REPLY)

The Cloud Security Alliance STAR Registry is an assurance program and documentation registry or cloud provider assessments based on the CSA Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire. Some providers also disclose documentation for additional certifications and assessments(including self-assessments).

Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance(used for educational purpose here)

NEW QUESTION: 37

Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?

- A. Expected Engineering
- B. Chaos Engineering
- C. Planned Outages
- D. Resiliency Planning
- E. Organized Downtime

Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.

- A. False
- B. True

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

"Standards like the SSAE16 have a defined scope. which includes both what is assessed (e.g. which of the provider's services) as well as which controls are assessed. A provider can thus "pass" an audit that doesn't include any security controls. which isn't overly useful for security and risk managers. " True or False?

- A. True
- B. False

Answer: A ([LEAVE A REPLY](#))

This is true, When cloud assessment is done, it is very important to understand the scope of the audit and the standard used. In statement above, we can see that, audit scope ofSSAE16 is decided by cloud provider and can be very limited and one may not be get full visibility into the security of the cloud service provider.

NEW QUESTION: 40

Which of the following is true after your organization migrates the data to the cloud?

- A. It is totally secure because cloud service providers have more security.
- B. In case of data breach, you as a customer, will be still legally liable.
- C. Cloud service provider will be legally liable for any data breach.
- D. Breaches will be termed as loss of Intellectual property.

Answer: ([SHOW ANSWER](#))

Even after cloud migration. cloud customer is responsible for the data and ultimately liable for any data loss or breaches.

NEW QUESTION: 41

Which of the following is the correct pair of risk management standards?

- A. ISO27002 & ISO27005
- B. ISO27001 & ISO27018
- C. ISO31000 & ISO27017
- D. ISO27005 & ISO31000

Answer: ([SHOW ANSWER](#))

ISO27005 refers to processes for IT Risk Management whereas ISO31000 refers to Enterprise Risk Management

NEW QUESTION: 42

Centralization of log streams is characteristic of which devices?

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

Answer: ([SHOW ANSWER](#))

SIEM is a combination of Security Incident Management(SIM)and Security Event Management(SEM).

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralised reporting.

NEW QUESTION: 43

CCM: A hypothetical company called: "Health4Sure" is located in the United States and provides cloud based services for tracking patient health. The company is compliant with HIPAA/HITECH Act among other industry standards. Health4Sure decides to assess the overall security of their cloud service against the CCM toolkit so that they will be able to present this document to potential clients.

Which of the following approach would be most suitable to assess the overall security posture of Health4Sure's cloud service?

- A. The CCM domains are not mapped to HIPAA/HITECH Act. Therefore Health4Sure should assess the security posture of their cloud service against each and every control in the CCM. This approach will allow a thorough assessment of the security posture.
- B. The CCM domain controls are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result of their compliance with HIPAA/HITECH Act. They could then assess the remaining controls thoroughly. This approach saves time while being able to assess the company's overall security posture in an efficient manner.
- C. The CCM columns are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result of their compliance with HIPAA/HITECH Act. They could then assess the remaining controls. This approach will save time.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 44

Which of the following leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive?

- A. VLANS

- B. Micro LANs
- C. Micro segmentation
- D. BitVLANS

Answer: C (LEAVE A REPLY)

Micro segmentation(also sometimes referred to as hyper segregation) leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive. Since the entire networks are defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software- defined environments.

Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

NEW QUESTION: 45

Interoperability is the ability that enables the migration of cloud services from one cloud provider to another or between public cloud and a private cloud.

- A. True
- B. False

Answer: B (LEAVE A REPLY)

This is false, as this is the definition of Portability and not interoperability

NEW QUESTION: 46

Policy documentation and training is a:

- A. Technical control
- B. Administrative control
- C. Physical control
- D. Logical control

Answer: B (LEAVE A REPLY)

There are three, commonly accepted forms of Controls:

Administrative-These are the laws, regulations, policies, practices and guidelines that govern the overall requirements and controls for an Information Security or other operational risk program. For example, a law or regulation may require merchants and financial institutions to protect and implement controls for customer account data to prevent identity theft. The business, in order to comply with the law or regulation, may adopt policies and procedures laying out the internal requirements for protecting this data, which requirements are a form of control.

Logical -These are the virtual, application and technical controls (systems and software), such as firewalls, antivirus software, encryption and maker/checker application routines.

Physical -Whereas a firewall provides a "logical" key to obtain access to a network, a "physical" key to a door can be used to gain access to an office space or storage room. Other examples of physical controls are video surveillance systems, gates and barricades, the use of guards or other personnel to govern access to an office, and remote backup facilities.

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:
https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 47

John said that he is looking for cloud service which is self-serviced and has a on-demand capacity. Which service model is he referring to?

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

Answer: A (LEAVE A REPLY)

Following are the characteristics of IaaS service model of cloud computing:

1. Scale
2. Converged network and IT capacity pool
3. Self-service and on-demand capacity
4. High reliability and resilience

NEW QUESTION: 48

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 (LEAVE A REPLY)

This is a very confusing question and we need to understand that its a shared responsibility between cloud service provider and customer.

NEW QUESTION: 49

Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?

- A. Infostructure
- B. Datastructure
- C. Infrastructure
- D. Metastructure

E. Appliststructure

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 50

The characteristics and traits of an individual that when aggregated could reveal the identity of that person. are known as:

- A. Indirect indicators
- B. Indirect Identifiers
- C. Indirect Identity Marks
- D. Indirect identifications

Answer: B ([LEAVE A REPLY](#))

Indirect identifiers typically consist of demographic or socioeconomic information, dates, or events.

Although each standalone indirect identifier cannot identify the individual, the risk is that combining a number of indirect identifiers with external data can result in exposing the subject of the information.

For example, imagine a scenario in which users were able to combine search engine data, coupled with online streaming recommendations to tie back posts and recommendations to individual users on a website.

NEW QUESTION: 51

Which is the correct sequence of Cloud Data lifecycle phases?

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

Answer: ([SHOW ANSWER](#))

The correct order of data lifecycle is Create, Store, Use, Share, Archive, Destroy

NEW QUESTION: 52

Your SLA with your cloud provider ensures continuity for all services.

- A. False
- B. True

Answer: ([SHOW ANSWER](#))

Explanation

NEW QUESTION: 53

Which of the following is not part of STRIDE model?

- A. Spoofing
- B. Denial of Service
- C. Distributed Denial of Service

D. Elevation of Privilege

Answer: C (LEAVE A REPLY)

The letters in STRIDE threat model represent Spoofing of identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The other options are simply mixed up or incorrect versions of the same.

NEW QUESTION: 54

NIST defines five characteristics of cloud computing- Rapid Elasticity, Broad Network Access, On demand self-service, Metered Usage & Resource pooling. However, ISO/IEC17788 mentions one more characteristic in addition is those 5. Which of the following is that characteristic?

- A. Multitenancy
- B. Isolation
- C. Segregation
- D. Automation

Answer: (SHOW ANSWER)

ISO/IEC17788 lists six key characteristics. the first five of which are identical to the NIST characteristics.

The only addition is multitenancy. which is distinct from resource pooling.

Ref: CSA Security Guidelines V4.0

NEW QUESTION: 55

Which of the following uses security and encryption as means to prevent unauthorized copying and limitations on distribution to only those who pay?

- A. Data Encryption
- B. Data Dispersion
- C. Digital Rights Management(DRM)
- D. IPSEC

Answer: C (LEAVE A REPLY)

Digital rights management(DRM)was designed to focus on security and encryption as a means of preventing unauthorized copying and limitations on distribution of content to only those authorized(purchasers).

NEW QUESTION: 56

Which of the below hypervisors are 0S based and are more attractive to attackers?

- A. Type I
- B. Type II
- C. Type III
- D. Type V

Answer: B (LEAVE A REPLY)

Type II hypervisors are OS-based and more attractive to attackers. There are lot of vulnerabilities which are found not only on OS but also in applications residing on the OS.

NEW QUESTION: 57

"Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. " Which of the following characteristics defines this?

- A. Broad network access
- B. Resource pooling
- C. Rapid elasticity
- D. Measured service

Answer: D (LEAVE A REPLY)

Measured service is defined as "Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. "

NEW QUESTION: 58

Who decides the risk appetite of the organization?

- A. Senior Management
- B. Risk Officer
- C. CIO
- D. CEO

Answer: A (LEAVE A REPLY)

It is the Senior Management who decides the appetite of the organization

NEW QUESTION: 59

A cloud storage architecture that caches content close to locations of high demand is known as:

- A. Volume Data
- B. Block Data
- C. Ephemeral Storage
- D. Content Delivery Network(CDN)

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 60

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 (LEAVE A REPLY)

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.

NEW QUESTION: 61

In a cloud scenario, who is the data processor and who is the data controller?

- A. Cloud Service Provider is the data controller and its customer is the data processor
- B. Database admin is the data controller and application owner is the data processor
- C. Cloud Service Provider is the data processor and its customer is the data controller
- D. Neither cloud service provider nor customer is data processor or data controller.

Answer: C (LEAVE A REPLY)

The customer determines the ultimate purpose of the processing and decides on the outsourcing or the delegation of all or part of the concerned activities to external organizations. Therefore, the customer acts as a controller.

When the service provider supplies the means and the platform, acting on behalf of the customer, it is considered to be a data processor.

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

Which of the following is NOT a key subsystem recommended for monitoring in cloud environments?

- A. Network
- B. Disk
- C. CPU
- D. Cable

Answer: (SHOW ANSWER)

Network, CPU and Disk(storage) are key subsystems in cloud environment that should be monitored.

NEW QUESTION: 63

Network logs from cloud providers are typically flow records, not full packet captures.

- A. False
- B. True

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 64

All cloud services utilize virtualization technologies.

- A. False
- B. True

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 65

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 66

The key focus of any business continuity or disaster recovery should be:

- A. Health and human safety
- B. Critical assets
- C. Critical infrastructure
- D. Financial documents

Answer: ([SHOW ANSWER](#))

The primary goal of whole business continuity and disaster recovery exercise should be health and human safety.

NEW QUESTION: 67

Which of the following is NOT part of Risk management process?

- A. Framing
- B. Dealing
- C. Responding

D. Assessing

Answer: B (LEAVE A REPLY)

The risk-management process has four components

1. Framing risk
2. Assessing risk
3. Responding to risk
4. Monitoring risk

NEW QUESTION: 68

Where does the encryption engine and key reside when doing file-level encryption?

- A. On the instance attached to the system
- B. Encryption engine resides on the server and keys on the client side
- C. On the KMS attached to the system
- D. On the client side

Answer: A (LEAVE A REPLY)

File-level encryption: Database servers typically reside on volume storage. For this deployment, you are encrypting the volume or folder of the database, with the encryption engine and keys residing on the instances attached to the volume.

External file system encryption protects from media theft, lost backups, and external attack but does not protect against attacks with access to the application layer, the instances OS, or the data

NEW QUESTION: 69

Ben was working on a project and hosted all its data on a public cloud. The project is now complete and he wants to remove the data Which of the following is best option for him in order to leave no remanence?

- A. Data-overwriting
- B. Physically destroy the media
- C. Cryptographic erasure
- D. Zeroing

Answer: C (LEAVE A REPLY)

All the options given are correct methods of destroying data but when it comes to data in cloud. the most suitable method is cryptographic erasure.

Definition: Cryptographic Erasure

Cryptographic erasure is the process of using encryption software (either built-in or deployed) on the entire data storage device. and erasing the key used to decrypt the data.

NEW QUESTION: 70

Which of the following phases of data security lifecycle typically occurs nearly simultaneously with creation?

- A. Save

- B. Use
- C. Store
- D. Encrypt

Answer: C (LEAVE A REPLY)

Storing is the act committing the digital data to some sort of storage repository and typically occurs nearly simultaneously with creation.

Reference: CSA Security Guidelines V.4(reproduced here for the educational purpose)

NEW QUESTION: 71

Which are the two major categories of network virtualization commonly seen in cloud computing today?

- A. Virtual Private Networks and Converged Network
- B. Software Defined Networks and Virtual Private Networks
- C. Software Defined Networks and Virtual LANs(VLANs)
- D. Virtual LANS(VLANs)and Converged Networks

Answer: D (LEAVE A REPLY)

There are two major categories of network virtualization commonly seen in cloud computing today:

. Virtual Local Area Networks (VLANs): VLANs leverage existing network technology implemented in most network hardware.

VLANs are extremely common in enterprise networks, even without Management Storage Service Management plane to nodes storage nodes (volumes) to compute nodes (instances) Internet to compute nodes Instances to instance Common networks underlying IaaS. They are designed for use in single-tenant networks (enterprise data centers) to separate different business units, functions, etc. (like guest networks). VLANs are not designed for cloud-scale virtualization or security and shouldn't be considered, on their own, an effective security control for isolating networks. They are also never a substitute for physical network segregation.

. Software Defined Networking(SDN): A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data. This allows us to abstract networking from the traditional limitations of a LAN.

Ref: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

NEW QUESTION: 72

Which of the standards is related to risk management?

- A. ISO 27005
- B. ISO 27001

Visit us at <https://www.examsboost.com/test/ccsk/>

- C. ISO 27002
- D. NIST 800-125

Answer: A (LEAVE A REPLY)

ISO 27005 'provides guidelines for information security risk management' and 'supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.'

NEW QUESTION: 73

Which of the following reports the cloud service provide normally share with customer WITHOUT any non-disclosure agreement and is in the public domain?

- A. SOC1 Type1
- B. SOC2 Type2
- C. SOC3
- D. SOC2 Type1

Answer: (SHOW ANSWER)

A Soc3 reports on the same information as a Soc2 report. The main difference between the two is that a Soc3 is intended for a general audience. These reports are shorter and do not include the same details as a Soc2 report, which is distributed to an informed audience of stakeholders. Due to their more general nature, Soc3 reports can be shared openly and posted on a company's website with a seal indicating their compliance

NEW QUESTION: 74

How can virtual machine communications bypass network security controls?

- A. Hypervisors depend upon multiple network interfaces
- B. VM images can contain rootkits programmed to bypass firewalls
- C. Most network security systems do not recognize encrypted VM traffic
- D. VM communications may use a virtual network on the same hardware host
- E. The guest OS can invoke stealth mode

Answer: D (LEAVE A REPLY)

NEW QUESTION: 75

Which of the following storages is typically used for swap files and other temporary storage needs and is terminated with its instance?

- A. Content Deliver
- B. Ephemeral Storage
- C. Object based Storage
- D. Raw Storage

Answer: B (LEAVE A REPLY)

Ephemeral storage: This type of storage is relevant for SaaS instances and exists only as long as its instance is up. It is typically used for swap files and other temporary storage needs and is terminated with its instance.

NEW QUESTION: 76

Which of the following items is NOT an example of Security as a Service (SecaaS)?

- A. Web filtering
- B. Spam filtering
- C. Provisioning
- D. Authentication
- E. Intrusion detection

Answer: ([SHOW ANSWER](#))

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**)

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 77

Which of following is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor?

- A. VM rootkit
- B. VM Escape
- C. VM HBR
- D. VM DOS

Answer: B ([LEAVE A REPLY](#))

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker access to the host operating system and all other virtual machines (VMs) running on that host.

NEW QUESTION: 78

All of the following are type of access controls except:

- A. Physical
- B. Natural
- C. Technical
- D. Administrative

Answer: ([SHOW ANSWER](#))

There is no control as such for Natural control.

There are three types of controls

1. Physical
2. Technical
3. Administrative

NEW QUESTION: 79

Single cloud assets are typically less resilient than in the case of traditional infrastructure.

- A. True
- B. False

Answer: ([SHOW ANSWER](#))

Cloud platforms can be incredibly resilient. but single cloud assets are typically less resilient than in the case of traditional infrastructure. This is due to the inherently greater fragility of virtualized resources running in highly-complex environments.

Reference: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

NEW QUESTION: 80

Which of the following processes leverages virtual network topologies to run more smaller and more isolated networks without incurring additional hardware costs?

- A. VLANs
- B. Grid networking
- C. Micro-segmentation
- D. Converged Networking

Answer: C ([LEAVE A REPLY](#))

Explanation:

This type of question are asked to create confusion.

Following are the five phases of SDLC:

1. Planning and requirements analysis: Business and security requirements and standards are being determined. This phase is the main focus of the project managers and stakeholders. Meetings with managers, stakeholders, and users are held to determine requirements. The software development lifecycle calls for all business requirements(functional and nonfunctional)to be defined even before initial design begins. Planning for the quality-assurance requirements and identification of the risks associated with the project are also conducted in the planning stage. The requirements are then analyzed for their validity and the possibility of incorporating them into the system to be developed.
2. Defining: The defining phase is meant to clearly define and document the product requirements to place them in front of the customers and get them approved. This is done through a requirement specification document, which consists of all the product requirements to be designed and developed during the project lifecycle.
3. Designing: System design helps in specifying hardware and system requirements and helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model. Threat modeling and secure design elements should be undertaken and discussed here.

4. Developing: Upon receiving the system design documents, work is divided into modules or units and actual coding starts. This is typically the longest phase of the software development lifecycle. Activities include code review, unit testing, and static analysis.

5. Testing: After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase.

During this phase, unit testing, integration testing, system testing, and acceptance testing are conducted.

NEW QUESTION: 81

Select the best definition of "compliance" from the options below.

A. The diligent habits of good security practices and recording of the same.

B. The awareness and adherence to obligations, including the assessment and prioritization of corrective actions deemed necessary and appropriate.

C. The process of completing all forms and paperwork necessary to develop a defensible paper trail.

D. The development of a routine that covers all necessary security measures.

E. The timely and efficient filing of security reports.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 82

How does running applications on distinct virtual networks and only connecting networks as needed help?

A. It provides dynamic and granular policies with less management overhead

B. It locks down access and provides stronger data security

C. It reduces the blast radius of a compromised system

D. It enables you to configure applications around business groups

E. It reduces hardware costs

Answer: (SHOW ANSWER)

NEW QUESTION: 83

Which of the following is NOT key Cloud computing characteristics?

A. On Demand self service

B. Metered pricing

C. Metered servicing

D. Broad Network Access

Answer: C (LEAVE A REPLY)

Often, this type of questions looks simple, but a confusion is created and you need to be careful while picking up the right options In our case, metered pricing and metered servicing looks similar but Metered pricing is one of the characteristics of cloud computing.

NEW QUESTION: 84

Which of the following is not an abuse or misuse of cloud services?

- A. Launching DDoS Attacks
- B. Email Spam
- C. Data Deletion
- D. Phishing campaigns

Answer: C (LEAVE A REPLY)

Please note here and understand the meaning of phrase "abuse or misuse of cloud Services". This phrase means to launch attacks or campaign by using cloud as a platform, mostly, public cloud.

NEW QUESTION: 85

Which is the primary tool for governance in Cloud Computing environment?

- A. Governance memo
- B. Service Level Agreement
- C. Operational level Agreement
- D. Contract

Answer: C (LEAVE A REPLY)

Contracts: The primary tool of governance is the contract between a cloud provider and a cloud customer(this is true for public and private cloud). The contract is your only guarantee of any level of service or commitment-assuming there is no breach of contract, which tosses everything into a legal scenario. Contracts are the primary tool to extend governance into business partners and providers.

Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance(used for educational purpose here)

NEW QUESTION: 86

CCM: In the CCM tool, a is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- A. Domain
- B. Control Specification
- C. Risk Impact

Answer: B (LEAVE A REPLY)

NEW QUESTION: 87

Containers can be implemented without the use of VMs at all and run directly on hardware.

- A. True
- B. False

Answer: (SHOW ANSWER)

Multiple containers can run on the same virtual machine or be implemented without the use of VMs at all and run directly on hardware. The container provides code running inside a restricted environment with only access to the processes and capabilities defined in the

container configuration. This allows containers to launch incredibly rapidly. since they don't need to boot an operating system or launch many(sometimes any) new services; the container only needs access to already-running services in the host OS and some can launch in milliseconds.

Reference: CSA Security Guidelines V.4(reproduced here for the educational purpose)

NEW QUESTION: 88

In which service model, cloud consumer is responsible to manage authorizations and entitlements only?

- A. Infrastructure as a Service (IaaS)
- B. Platform as a Service (PaaS)
- C. Software as a Service (SaaS)
- D. All of them

Answer: (SHOW ANSWER)

It is important to read the question carefully and then choose the best answer. Although cloud consumer is responsible for authorizations and entitlements across all service models but questions uses

"only". Therefore, answer is Software as a Service (SaaS) and a SaaS provider is responsible for perimeter security, logging/ monitoring/auditing, and application security.

NEW QUESTION: 89

What refers refer the model that allows customers to scale their computer and/ or storage needs with little or no intervention from or prior communication with the provider. The services happen in real time?

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

Answer: B (LEAVE A REPLY)

It is the characteristic of On-demand self-service that allows customers to scale their computer and/ or storage needs with little or no intervention from or prior communication with the provider

NEW QUESTION: 90

What item below allows disparate directory services and independent security domains to be interconnected?

- A. Union
- B. Cloud
- C. Coalition
- D. Federation
- E. Intersection

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 91

When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA?

- A. The regulations that are pertinent to the contract and how to circumvent them.
- B. The duration of time that a security violation can occur before the client begins assessing regulatory fines.
- C. The metrics defining the service level required to achieve regulatory objectives.
- D. The cost per incident for security breaches of regulated information.
- E. The type of security software which meets regulations and the number of licenses that will be needed.

Answer: ([SHOW ANSWER](#))

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 92

One of the part of STRIDE model is:

- A. Denial of Service
- B. Redundancy
- C. Security
- D. Reputation

Answer: ([SHOW ANSWER](#))

The six components that made STRIDE are:

1. Spoofing: Attacker assumes identity of subject
2. Tampering: Data or messages altered by an attacker
3. Repudiation: illegitimate denial of an event
4. Information disclosure: Information obtained without authorization
5. Denial of service: Attacker overloads system to deny legitimate access
6. Elevation of privilege: Attacker gains a privilege level above what is permitted

NEW QUESTION: 93

Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?

- A. Greater reliance on contracts, audits, and assessments due to lack of visibility or management.
- B. Decreased requirement for proactive management of relationship and adherence to contracts.
- C. Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
- D. More physical control over assets and processes.
- E. None of the above.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 94

John's Laptop was stolen. He had saved all his passwords in a text file stored in his laptop. Adversary used the passwords from the text file and gained access to company's network and sensitive databases, of which John was the data base administrator. It resulted in theft of thousands of customer information. This incident could have been prevented by?

- A. Monitoring through SIEM device
- B. Data Loss Prevention Implementation
- C. Using multi-factor authentication
- D. Web Application Firewall

Answer: ([SHOW ANSWER](#))

Use of multifactor authentication would have prevented adversary from logging in to the system. Other mechanisms would not help as they will see traffic coming from legitimate user.

NEW QUESTION: 95

An inherent weakness in an information system. security procedures. internal controls, or implementation that could be exploited by a threat source.

- A. Vulnerability
- B. Threat
- C. Risk
- D. ARO

Answer: A ([LEAVE A REPLY](#))

That's the definition of vulnerability

NEW QUESTION: 96

Sending data to a provider's storage over an API is likely as much more reliable and secure than setting up your own SFTP server on a VM in the same provider

- A. False
- B. True

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 97

Which of the following should be your top priority when designing a cloud security program for your organization?

- A. Configure IPSEC tunnels
- B. Prevention of DDoS Attack
- C. Consider OWASP guideline
- D. Protection of cloud management plan

Answer: [\(SHOW ANSWER\)](#)

In most cases, those APIs are both remotely accessible and wrapped into a web-based user interface.

This combination is the cloud management plane, since consumers use it to manage and configure the cloud resources, such as launching virtual machines (instances) or configuring virtual networks. From a security perspective, it is both the biggest difference from protecting physical infrastructure (since you can't rely on physical access as a control) and the top priority when designing a cloud security program. If an attacker gets into your management plane, they potentially have full remote access to your entire cloud deployment.

Ref: CSA Security Guidelines V4

NEW QUESTION: 98

Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

- A. True
- B. False

Answer: [A \(LEAVE A REPLY\)](#)

NEW QUESTION: 99

Private clouds can be hosted off-premises as well.

- A. True
- B. False

Answer: [A \(LEAVE A REPLY\)](#)

It is true. This is how Private cloud is defined.

Private Cloud: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premises or off-premises.

NEW QUESTION: 100

Which of the following is NOT one of the vulnerabilities that can lead to risk of "abuse of high privilege roles" or "Cloud provider malicious insider"?

- A. AAA Vulnerabilities
- B. System and OS vulnerabilities

- C. Poor enforcement of role definitions
- D. Lack of data centre hardware redundancy

Answer: D (LEAVE A REPLY)

Redundancy has nothing to do with abuse of high privilege roles. All others can lead to risk of risk of

"abuse of high privilege roles" or "Cloud provider malicious insider"

NEW QUESTION: 101

According to Cloud Security Alliance logical model of cloud computing, which of the following defines the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers.

- A. Metastructure
- B. Infostructure
- C. Infrastructure
- D. Applistructure

Answer: A (LEAVE A REPLY)

According to CSA Securityguidelines4.0. Metastucture is defined as the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.

NEW QUESTION: 102

To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?

- A. EDiscovery tools
- B. Provider and consumer contracts
- C. Third-party attestations
- D. Provider documentation
- E. Provider run audits and reports

Answer: (SHOW ANSWER)

NEW QUESTION: 103

What is true of searching data across cloud environments?

- A. The cloud provider must conduct the search with the full administrative controls.
- B. You can easily search across your environment using any E-Discovery tool.
- C. You might not have the ability or administrative rights to search or access all hosted data.
- D. All cloud-hosted email accounts are easily searchable.
- E. Search and discovery time is always factored into a contract between the consumer and provider.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 104

When the data is transferred to third party. who is ultimately responsible for security of data?

- A. Cloud Service Provider
- B. Cloud Controller
- C. Cloud Processor
- D. Cloud Security Broker

Answer: B (LEAVE A REPLY)

Whatever will be the scenario. Data controller will be responsible for security of data in cloud

NEW QUESTION: 105

On Demand Shelf Service is one of the key characteristics as defined by NIST.

- A. True
- B. False

Answer: B (LEAVE A REPLY)

This is false. Please read the question carefully.

Question: is asking

On Demand "Shelf" Service where the correct characteristic is "On Demand Self Service"

NEW QUESTION: 106

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 (LEAVE A REPLY)

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.

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam!

Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**)

Special Discount: Freepdfdumps)

NEW QUESTION: 107

An agreed-upon description of the attributes of a product. at a point in time that serves as a basis for defining change is called:

- A. Standardization
- B. Baseline
- C. Trusted Module
- D. Secured Server

Answer: B (LEAVE A REPLY)

A baseline is an agreed-upon description of the attributes of a product. at a point in time that serves as a basis for defining change.

NEW QUESTION: 108

Which is the key mechanism used by organisations that supports. assures and demonstrate compliance?

- A. Governance
- B. Risk Management
- C. Audits
- D. Gap Assessment

Answer: C (LEAVE A REPLY)

Although very closely related with audits-which are a key mechanism to support assure. and demonstrate compliance-there is more to compliance than audits and more to audits than using them to assure regulatory compliance.

Reference: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

NEW QUESTION: 109

In 2015, 4 million records were stolen from telecom company, XYZ Ltd, and later this information was used for scam calls to get bank information from the customers of XYZ. Which was of the following protection would have helped in minimising impact of the theft?

- A. Use of VPN
- B. Firewall
- C. Encryption
- D. Repudiation

Answer: C (LEAVE A REPLY)

Encryption of Data would have minimised the impact of the incident and it would have prevented data being used for scam calls.

NEW QUESTION: 110

ISO 27001 certification can be taken as proof to achieve Third-party assessment level in CSA star program.

- A. True
- B. False

Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 111

Which of the following is correct about Due Care & Due Diligence?

- A.** Due diligence is the act of investigating and understanding the risks a company faces whereas Due care is the development and implementation of policies and procedures to aid in protecting the company, its assets and its people from threats.
- B.** Due care is the act of investigating and understanding the risks a company faces whereas Due Diligence is the development and implementation of policies and procedures to aid in protecting the company, its assets and its people from threats.
- C.** Due care is technical control whereas Due Diligence is physical control.
- D.** None of the above definitions are correct.

Answer: A (LEAVE A REPLY)

Definitions:

Due diligence is the act of investigating and understanding the risks a company faces. Due care is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats

NEW QUESTION: 112

CCM: The following list of controls belong to which domain of the CCM?

GRM 06 - Policy GRM 07 - Policy Enforcement GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews GRM 10 - Risk Assessments GRM 11 - Risk Management Framework

- A.** Governance and Retention Management
- B.** Governance and Risk Management
- C.** Governing and Risk Metrics

Answer: B (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 113

Which of the following type of risk assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action?

- A.** Qualitative Analysis
- B.** Quantitative Analysis
- C.** Third party Risk Analysis
- D.** Outsourced risk analysis

Answer: B (LEAVE A REPLY)

Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers. This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action.

Valid CCSK Dumps shared by Actual4test.com for Helping Passing CCSK Exam! Actual4test.com now offer the **newest CCSK exam dumps**, the Actual4test.com CCSK exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCSK dumps with Test Engine here:

https://www.actual4test.com/CCSK_examcollection.html (305 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)