[May 16, 2022 Get New CCSK Certification ? Valid Exam Dumps Questions [Q101-Q125

[May 16, 2022] Get New CCSK Certification – Valid Exam Dumps Questions [Q101-Q125]

[May 16, 2022] Get New CCSK Certification &ndash; Valid Exam Dumps Questions
100% Passing Guarantee - Brilliant CCSK Exam Questions PDF

Average Salary of Certificate of Cloud Security Knowledge (CCSK) Exam Certified Professionals

The average salary of a Certificate of Cloud Security Knowledge (CCSK) Exam Certified Professional is:

- Europe: 50,000 EURO- United State: 60,550 USD- India: 4,477,000 INR- England: 45,000 POUND **QUESTION 101**

Credentials and cryptographic keys must not be embedded in source code or distributed in public facing repositories such as GitHub.
* True
* False

This is true. Credentials and cryptographic keys must not be embedded in source code or distributed in public facing repositories such as GitHub, because there is a significant chance of discovery and misuse.

Keys need to be appropriately secured and a well- secured public key infrastructure (PKI) is needed to ensure key-management activities are carried out.

QUESTION 102

The characteristics and traits of an individual that when aggregated could reveal the identity of that person. are known as:
* Indirect indicators
* Indirect Identifiers
* Indirect Identity Marks
* Indirect identifications
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.

QUESTION 103

Which of the following is an effective way of segregating different cloud networks and datacenters in a hybrid cloud environment?
* Virtual LANs
* Dedicated Hosting
* Virtual Private Networks
* Bastion Virtual Network
One emerging architecture for hybrid cloud connectivity is &#8220;bastion&#8221; or &#8220;transit&#8221; virtual networks:

. This scenario allows you to connect multiple, different cloud networks to a data center using a single hybrid connection. The cloud user builds a dedicated virtual network for the hybrid connection and then peers any other networks through the designated bastion network.

. Second-level networks connect to the data center through the bastion network, but since they aren&#8217;t peered to each other they can&#8217;t talk to each other and are effectively segregated. Also, you can deploy different security tools, firewall rulesets, and Access Control Lists in the bastion network to further protect traffic in and out of the hybrid connection.

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

QUESTION 104

Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?
* Infrastructure
* Datastructure
* Infostructure
* Applistructure
* Metastructure

QUESTION 105

Which of the following is NOT true about CSA Cloud control metrix (CCM)?
* Maps controls to existing standards like ISO 27001
* Contains security controls divided in several domains
* Define the Cloud Audit Methodolog
* Also includes controls related to processing of personal data.
Remember that CCM is a security framework and does not include any methodology The Cloud Security Alliance Cloud Controls

Matrix(CCM) is an essential and up-to-date security controls framework that is addressed to the cloud community and stakeholders. A fundamental richness of the CCM is its ability to provide mapping and cross relationships with the main industry-accepted security

QUESTION 106

What is true of companies considering a cloud computing business relationship?
* The laws protecting customer data are based on the cloud provider and customer location only.
* The confidentiality agreements between companies using cloud computing services is limited legally to the company, not the provider.
* The companies using the cloud providers are the custodians of the data entrusted to them.
* The cloud computing companies are absolved of all data security and associated risks through contracts and data laws.
* The cloud computing companies own all customer data.

QUESTION 107

Which are the two major categories of network virtualization commonly seen in cloud computing today?
* Virtual Private Networks and Converged Network
* Software Defined Networks and Virtual Private Networks
* Software Defined Networks and Virtual LANs(VLANs)
* Virtual LANS(VLANs)and Converged Networks
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&#8217;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)

QUESTION 108

Who is responsible for Application Security in Software as a Service(SaaS) service model?
* Cloud Customer
* Cloud Service Provider
* Cloud Carrier
* It&#8217;s a shared responsibility between Cloud Service Provider and Cloud Customer
Its always a shared responsbility

QUESTION 109

In Platform as a Service (PaaS), platform security is a responsibility of:
* Customer

* Cloud service provider
* It&#8217;s a shared responsibility
* Neither of them

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

QUESTION 110

Which of following responsibilities can never be transferred. even during cloud adoption?

* Security
* Governance
* Infrastructure
* Application Development

The primary issue to remember when governing cloud computing is that an organization can never outsource responsibility for governance, even when using external providers. This is always true, cloud or not, but is useful to keep in mind when navigating cloud computing&#8217;s concepts of shared responsibility models Ref: CSA Security Guidelines V4.0

QUESTION 111

Which of the following best describes the relationship between a cloud provider and the customer?

* Contract
* Operational level Agreement
* Service Level Agreement
* Privacy Level Agreement

Contract is the most suitable answer here. It can be argued that Service Level Agreement could also be an answer but SLA is a negotiation/agreement for minimum service-levels expected. Contract is the document that defines the relation-ship between Cloud service provider and customer

QUESTION 112

Which provides guidelines for organizational information security standards including the selection, implementation, and management of controls taking into consideration the organization&#8217;s information security risk environments?

* ISO 27001
* ISO 27002
* NIST 800-9
* FIPS 140-2

ISO 27002 is a standard which provides detailed description of security controls and how they need to implemented to provide effective ISMS.

QUESTION 113

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

* Framing
* Dealing
* Responding
* Assessing

The risk-management process has four components

1. Framing risk

2. Assessing risk

3. Responding to risk

4. Monitoring risk

QUESTION 114

Which governance domain deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative?
* Legal Issues: Contracts and Electronic Discovery
* Infrastructure Security
* Compliance and Audit Management
* Information Governance
* Governance and Enterprise Risk Management

QUESTION 115

Which of the following is NOT a key subsystem recommended for monitoring in cloud environments?
* Network
* Disk
* CPU
* Cable
Network, CPU and Disk(storage) are key subsystems in cloud environment that should be monitored.

QUESTION 116

Which is the leading industry leading standard you will recommend to a web developer when designing web application or an API for a cloud solution?
* ISO 27001
* SOC2
* FIPS 140
* OWASP
OWASP is an open project and is leading industry standard for designing web applications and its security.

QUESTION 117

Private cloud model can be managed by third party who may not be part of the organization served by that private cloud.
* True
* False
This is true

This is a tricky question that you should look into carefully. Main purpose of private cloud is usage by one organization (use) but it can be managed by third party as well.

Definition: Private cloud

According to NIST, &#8220;the cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g, business units). It may be owned, managed, and operated by the organisation, a third party or some combination of them, and it may exist on or off premises. &#8220;

QUESTION 118

What item below allows disparate directory services and independent security domains to be interconnected?
* Coalition
* Cloud
* Intersection
* Union
* Federation

QUESTION 119

The ability of a cloud services datacentre and its associated components. including servers. storage. and so on. to continue operating in the event of a disruption. which may be equipment failure. power outage. or a natural disaster. known as:
* Redundancy
* Resiliency
* Disaster recovery
* Continuity
Resiliency is the correct answer but other options look very similar and is provided to create confusion.

One need to be careful while answering the question.

Resiliency is often confused with redundancy, Key difference is

A redundant system includes multiple channels to provide alternate paths for communications in case of individual failures.

&#8230; Resilience, on the other hand, refers to a system&#8217;s ability to adapt to failures and to resume normal operations when the failure has been resolved.

QUESTION 120

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?
* Data-overwriting
* Physically destroy the media
* Cryptographic erasure
* Zeroing
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.

QUESTION 121

In the IaaS hosted environment. who is ultimately responsible for platform security?
* Joint responsibility
* Cloud Service Provider

* System Administrator
* Customer

In IaaS hosted environment, Platform security is responsibility of the customer whereas infrastructure security is a shared responsibility between cloud service provider and the customer

QUESTION 122

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

* False
* True

Explanation

QUESTION 123

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

* Obtain provider permission for test
* Use techniques to evade cloud provider&#8217;s detection systems
* Use application layer testing tools exclusively
* Use network layer testing tools exclusively
* Schedule vulnerability test at night

QUESTION 124

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.

* Metastructure
* Infostructure
* Infrastructure
* Applistructure

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.

QUESTION 125

Which of the following is NOT a characteristic of Object Storage?

* Stored in cloud
* Accessed through web interface
* Has additional Metadata
* Cannot be accessed through web interface

Object storage: Similar to a file share accessed via APIs or a web interface. Examples include Amazon S3 and Rackspace cloud files.

Free CCSK braindumps download: https://www.validexam.com/CCSK-latest-dumps.html]