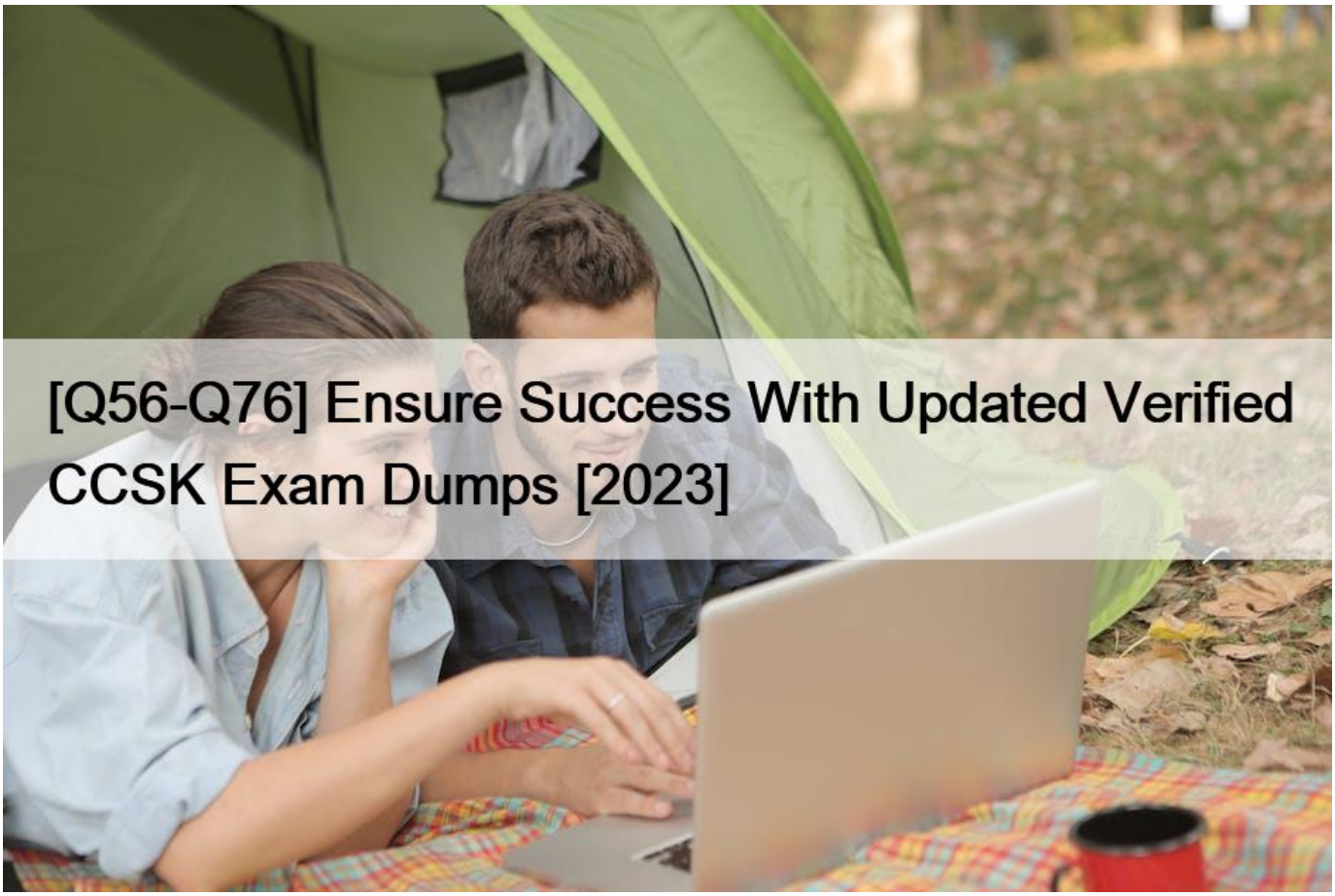
[Q56-Q76 Ensure Success With Updated Verified CCSK Exam Dumps [2023



Ensure Success With Updated Verified CCSK Exam Dumps [2023]
Exam Materials for You to Prepare & Pass CCSK Exam.

QUESTION 56

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
* False
* True

QUESTION 57

Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?
* Code Review
* Static Application Security Testing (SAST)
* Unit Testing
* Functional Testing
* Dynamic Application Security Testing (DAST)

QUESTION 58

Which of the following authentication is most secured?
* Active Directory
* Bio metric Access
* Username and encrypted password
* Multi-factor Authentication

All privileged user accounts should use multi-factor authentication(MFA). If possible, all cloud accounts(even individual user accounts) should use MFA. It’s one of the single most effective security controls to defend against a wide range of attacks. This is also true regardless of the service model: MFA is just as important for SaaS as it is for IaaS.

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

QUESTION 59

If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, how is the information likely to be obtained?
* It may require a subpoena of the provider directly
* It would require a previous access agreement
* It would require an act of war
* It would require a previous contractual agreement to obtain the application or access to the environment
* It would never be obtained in this situation

QUESTION 60

Which is the most common control used for Risk Transfer?
* Contracts
* SLA
* Insurance
* Web Application Firewall

Buying insurance is most common method of transferring risk.

QUESTION 61

ln order to determine critical assets and processes of the organization, it must first conduct a:
* Risk Assessment
* Business Impact Analysis(BIA)
* Datacentre monitoring
* Host hardening

This is a process known as the business impact analysis(BIA). We determine a value for every asset(usually in terms of dollars),,what it would cost the organization if we lost that asset(either temporarily or permanently), what it would cost to replace or repair that asset, and any alternate methods for dealing with that loss.

QUESTION 62

Which is the document used by Cloud Service Provider to declare the level of personal data protection and security that it sustains for the relevant data processing?
* Contract
* Service Level Agreement(SLA)

* Privacy Level Agreement(PLA)
* Privacy Charter

The PLA, as defined by the CSA, does the following Provides a clear and effective way to communicate the level of personal data protection offered by a service provider.

Works as a tool to assess the level of a service provider’s compliance with data protection legislative requirements and leading practices Provides a way to offer contractual protection against possible financial damages due to lack of compliance

QUESTION 63

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

* Cloud Service Provider
* Cloud Controller
* Cloud Processor
* Cloud Security Broker

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

QUESTION 64

Cloud Security provider is responsible for Platform Security in Platform as a Service(PaaS) model.

* True
* False

It is false. Platform security is a shared responsibility between cloud service provider and cloud service customer in Platform as a Service(PaaS) model.

QUESTION 65

ENISA: Lock-in is ranked as a high risk in ENISA research, a key underlying vulnerability causing lock in is:

* Lack of completeness and transparency in terms of use
* Lack of information on jurisdictions
* No source escrow agreement
* Unclear asset ownership
* Audit or certification not available to customers

QUESTION 66

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.

* Risk Impact
* Domain
* Control Specification

QUESTION 67

When Database as a Service is offered on Platform as a Service(PaaS) model, who is responsible for security features that needs to applied to the Databases?

* Cloud Service Provider
* Cloud Access Security Broker (CASB)
* Cloud Consumer
* Cloud Carrier

This is a tricky question.

When using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use, managing accounts, or even authentication methods.

Ref: CSA Security Guidelines v4.0

QUESTION 68

Lack of standard data formats and service interfaces can lead to:
* Vendor lock out
* Vendor lock in
* Denial of Service
* API Mis-management

Lack of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability, makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-House IT environment.

QUESTION 69

What can be implemented to help with account granularity and limit

blast radius with laaS an PaaS?
* Configuring secondary authentication
* Establishing multiple accounts
* Maintaining tight control of the primary account holder credentials
* Implementing least privilege accounts
* Configuring role-based authentication

QUESTION 70

Which of the following reports the cloud service provide normally share with customer WITHOUT any non-disclosure agreement and is in the public domain?
* SOC1 Type1
* SOC2 Type2
* SOC3
* SOC2 Type1

A Soc3 reports on the same information as a Soc2 report. The main difference between the two is that a Soc3 is intended fora 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

QUESTION 71

Which of the following is a key consideration in Data security but does not feature in Data Security Life cycle?
* Storage Location
* Storage Device
* Storage protocol
* Access Method

The lifecycle represents the phases information passes through but doesnt address its location or how it is accessed.

QUESTION 72

Logs, documentation, and other materials needed for audits and compliance and often serve as evidence of compliance activities are known as:
* Log Trail
* Documented Evidence
* Proof of Audit
* Artifacts
Artifacts are the logs, documentation, and other materials needed for audits and compliance; they are the evidence to support compliance activities. Both providers and customers have responsibilities for producing and managing their respective artifacts.

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

QUESTION 73

Centralization of log streams is charactertic of which devices?
* IDS
* IPS
* SIEM
* DLP
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.

QUESTION 74

Cloud customer and cloud service provider are jointly responsible legally for data breach or data loss in absence of any written clause regarding same in contract or SLA.
* True
* False
This is false, because, unless, specified cloud customer is legally liable for any loss to data

QUESTION 75

Which of the following establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information(PII) in accordance with the privacy principles in IS0/IEC 29100 for the public cloud computing environment?
* IS0 27017
* IS0 27018
* IS0 27032
* IS0 27034
IS0/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information(PII) in accordance with the privacy principles in IS0/IEC 29100 for the public cloud computing environment.

QUESTION 76

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

* Save
* Use
* Store
* Encrypt

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)

Updated CCSK Certification Exam Sample Questions:
https://www.examslabs.com/Cloud-Security-Alliance/Cloud-Security-Knowledge/best-CCSK-exam-dumps.html]