[Q26-Q41 Latest Cloud Security Alliance CCSK First Attempt, Exam real Dumps Updated [Dec-2023

Latest Cloud Security Alliance CCSK First Attempt, Exam real Dumps Updated [Dec-2023 Get the superior quality CCSK Dumps Questions from VCEPrep. Nobody can stop you from getting to your dreams now. Your bright future is just a click away! Q26. 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.

Q27. Which of the following pose the biggest risk in the organization?
* People
* Technology
* Access Controls
* DDoS Attacks
People pose the biggest risk in the organization.

People form the biggest risk as they can expose the sensitive data accidentally or on purpose.

Disgruntled employees or careless employees form a great threat to the organization.

Q28. If there are gaps in network logging data, what can you do?
* Nothing. There are simply limitations around the data that can be logged in the cloud.
* Ask the cloud provider to open more ports.
* You can instrument the technology stack with your own logging.
* Ask the cloud provider to close more ports.
* Nothing. The cloud provider must make the information available.

Q29. Which of the following Storage type is NOT associated with SaaS solution?
* Content Delivery network
* Raw Storage
* Volume Storage
* Ephemeral Storage
Volume storage is commonly associated with IaaS solutions.

All the other 3 options are related to SaaS solutions

Q30. CCM: A hypothetical start-up company called &#8220;ABC&#8221; provides a cloud based IT management solution. They are growing rapidly and therefore need to put controls in place in order to manage any changes in

their production environment. Which of the following Change Control & Configuration Management production environment specific control should they implement in this scenario?
* Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant)-impacting (physical and virtual) applications and system-

system interface (API) designs and configurations, infrastructure network and systems components.
* Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or

managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
* All cloud-based services used by the company&#8217;s mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
* None of the above

Q31. Stopping a function to control further risk to business is called:
* Mitigation
* Avoidance
* Acceptance
* Transference
Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realised.

Q32. Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?
* Planned Outages
* Resiliency Planning

* Expected Engineering
* Chaos Engineering
* Organized Downtime
Explanation/Reference:

Q33. Who is responsible for Governance, Risk & Compliance 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
Remember, GRC will always remain responsibility of the cloud customer in all service models

Q34. Which of the following is typically a policy set that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location?
* Intrusion Detection System
* Security Groups
* API Gateway
* Database Activity Monitor
SDN firewalls (e.g, security groups) can apply to assets based on more flexible criteria than hardware- based firewalls, since they aren&#8217;t limited based on physical topology. (Note that this is true of many types of software firewalls, but is distinct from hardware firewalls). SDN firewalls are typically policy sets that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location (within a given virtual network).

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

Q35. 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&#8217;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)

Q36. 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)

Q37. The amount of risk that the leadership and stakeholders of an organization are willing to accept is know as:
* Risk Acceptance
* Residual Risk
* Risk Tolerance
* Risk Residual

Risk tolerance is the amount of risk that the leadership and stakeholders of an organization are willing to accept. It varies based on asset and you shouldn&#8217;t make a blanket risk decision about a particular provider; rather, assessments should align with the value and requirements of the assets Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance(used for educational purpose here)

Q38. To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?
* Provider documentation
* Provider run audits and reports
* Third-party attestations
* Provider and consumer contracts
* EDiscovery tools

Q39. What of the following is NOT an essential characteristic of cloud computing?
* Broad Network Access
* Measured Service
* Third Party Service
* Rapid Elasticity
* Resource Pooling

Q40. One of the main reasons and advantage of having external audit is:
* Its cheaper
* Its independent
* Internal staff is less qualified than external auditors.
* Better tools used by external provider

All other answers are distractors. One of the primary reasons of doing external auditing is the independence of auditors.

Q41. Who is responsible for the safe custody, transport, data storage. and implementation of business rules in relation to the privacy?
* Data controller
* Data owner
* Data custodian
* Data processor

Data custodians are responsible for the safe custody. transport. data storage. and implementation of business rules

Guaranteed Success with Valid Cloud Security Alliance CCSK Dumps: https://www.vceprep.com/CCSK-latest-vce-prep.html