CCSK Test Tips

1. The primary security responsibilities of the cloud provider in the management infrastructure are building and properly configuring a secure network infrastructure.
2. Use elastic servers when possible and move workloads to new instances.
3. The Infrastructure layer is the most important for securing because it is considered to be the foundation for secure cloud operations
4. An entitlement matrix is used for defining a set of rules composed of claims and attributes of the entities in a transaction, which is used to determine their level of access to cloud-based resources.
5. Object-based storage in a private cloud is NOT a cloud computing characteristic that impacts incident response.
6. The CCM domain controls ARE mapped to HIPAA/HITECH Act and therefore the company mentioned could verify the CCM controls already covered as a result of their compliance with HIPPA/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.
7. A hybrid cloud represents a composition of two or more clouds that remain unique identities but are bound together by standardized or proprietary technology that enables data and application portability.
8. Password Encryption, Link/Network Encryption, Proxy-Based Encryption are the three valid options for protecting data as it moves to and within the cloud.
9. A Code Review is a type of application security testing that involves manual activity that is not necessarily integrated into automated testing.
10. Web security as a service be deployed for a cloud consumer by proxying or redirecting web traffic to the cloud provider and/or on the premise through a software or appliance installation.
11. SAST should incorporate checks on API calls to the cloud service.
12. For cloud consumers to be able to properly configure and manage their network security, cloud providers must expose security controls.
13. Identity is defined as the unique expression of an entity within a given namespace.
14. Big Data as a Service is NOT a common storage option with IaaS.
15. If the system or environment is built automatically from a template then changes made in production are overwritten by the next code or template change.
16. An encryption method can be utilized along with data fragmentation to enhance security.
17. Utilize a client/application encryption method when object storage is used as the back-end for an application.
18. A cloud customer CANNOT submit the CCM on behalf of a CSP to CSA Security, Trust & Assurance Registry (STAR).
19. It is false that a security failure at the root network of a cloud provider will not compromise the security of all customers because of multitenancy configuration.
20. The most significant security difference between traditional infrastructure and cloud computing is the management plane.

21. The “Segregation by default” opportunity helps reduce common application security issues.
22. An Intrusion Prevention System is NOT normally a method for detecting and preventing data migration into the cloud.
23. Encryption is usually managed on multi-tenant storage using multiple keys per data owner.
24. Provisioning is NOT an example of Security as a Service (SecaaS).
25. In volume storage, the data dispersion method is often used to support resiliency and security.
26. When searching for data across cloud environments, you might not have the ability or administrative rights to search or access all hosted data.
27. It is true that REST APIs are the standard for web-based services because they run over HTTPS and work well across diverse environments.
28. If there are gaps in network logging data, you can “instrument” the technology stack with your own logging.
29. It is true that all cloud services utilize virtualization technologies.
30. In the CCM tool, a Control Specification is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.
31. An important consideration when performing a remote vulnerability test of a cloud-based application is to obtain provider permission for the test.
32. The Cloud Provider is responsible for the security of the physical infrastructure and virtualization platform
33. When mapping functions to lifecycle phases, the Create and Use functions are required to successfully process data.
34. An identity is a distinct and unique object within a particular namespace. Attributes are properties which belong to an identity. Each identity can have multiple attributes.
35. It is true that if the management plane has been breached, you should confirm the templates/configurations for your infrastructure or applications have also not been compromised.
36. a service type of network typically isolated on different hardware because it has distinct functions from other networks.
37. A perceived advantage or disadvantage of managing enterprise risk for cloud deployments is that there is greater reliance on contracts, audits, and assessments due to lack of visibility or management.
38. It is arguably false that cloud storage will most often utilize the same types of data storage used in traditional data storage technologies.
39. Perimeter security is focused on protecting the management plane components, such as web and API servers, from attacks.
40. For third-party audits or attestations, it is critical for providers to publish and customers to evaluate the scope of the assessment and the exact included features and services for the assessment.
41. The barriers to developing full confidence in security as a service (SecaaS) include Compliance, multi-tenancy, and vendor lock-in.
42. In the Secure Deployment meta-phase, the CSA focuses on security and testing activities when moving code from an isolated development environment to production.
43. A cloud deployment of two or more unique clouds is known as a Hybrid Cloud.

44. The Architectural Relevance column in the CCM indicates the applicability of cloud security to control Physical, Network, Compute, Storage, Application or Data.
45. Blind spots occur in a virtualized environment, where network-based security controls may not be able to monitor certain types of traffic, due to the fact that virtual machines may communicate with each other over a virtual network all on the same host rather than a physical network between servers.
46. Hybrid Cloud is commonly used to describe a non-cloud data center **bridged directly** to a cloud provider.
47. According to ENISA, licensing risks refer to the scenario where a traditional software licensing scheme may lead to high costs or lack of compliance in cloud systems.
48. Software Defined Network firewall are policy sets that can only be applied to similar grouped assets.
49. An SDLC should be modified to address application security in a Cloud Computing environment based on updated threat and trust models.
50. If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, it may require a subpoena of the provider directly.
51. A container is known as a code execution environment running within an operating system that shares and uses the resources of the operating system.
52. The main considerations for key management are performance, accessibility, latency, and security.
53. Regarding the extent to which the CSA Guidance document is sufficient for legal advice in setting up relationships with cloud service providers, the CSA Guidance document provides an overview of selected issues and it is not a substitute for obtaining legal advice.
54. The three main aspects for data security controls are controlling, protecting, and enforcing.
55. The Incident Response, Notification and Remediation governance domain focuses on proper and adequate incident detection, response, notification, and remediation.
56. The "authorization" component of identity, entitlement, and access management is best described as “enforcing the rules by which access is granted to the resources”.
57. It is false that all assets require the same continuity in the cloud.
58. It is true that identified issues, risks, and recommended remediations are included when determining compliance.
59. The Compliance and Audit Management domain deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative
60. According to ENISA, VM hopping is using a compromised VM to exploit a hypervisor, used to take control of other VMs.
61. According to ENISA, system or O/S vulnerabilities are among the vulnerabilities contributing to a high risk ranking for Network Management.
62. According to ENISA, globalization is NOT one of the five key legal issues common across all scenarios.
63. According to ENISA, a reason for risk concerns of a cloud provider being acquired is non-binding agreements put at risk.