CCSK Test Tips

1. A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction. Workloads always run somewhere on a processor and consume memory.
2. It is true that any given processor and memory will nearly always be running multiple workloads, often from different tenants.
3. The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly. The absolute top security priority is segregation and isolation of network traffic to prevent tenants from viewing another's traffic.
4. Use elastic servers when possible and move workloads to new instances.
5. The Infrastructure layer is the most important for securing because it is considered to be the foundation for secure cloud operations
6. 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.
7. Object-based storage in a private cloud is NOT a cloud computing characteristic that impacts incident response.
8. 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.
9. 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.
10. Client/Application Encryption, Link/Network Encryption, Proxy-Based Encryption are the three valid options for protecting data as it moves to and within the cloud.
11. A Code Review is a type of application security testing that involves manual activity that is not necessarily integrated into automated testing.
12. 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.
13. SAST should incorporate checks on API calls to the cloud service.
14. For cloud consumers to be able to properly configure and manage their network security, cloud providers must expose security controls.
15. Identity is defined as the unique expression of an entity within a given namespace.
16. Big Data as a Service is NOT a common storage option with IaaS.
17. The distributed data collection component of big data is focused on the mechanisms used to ingest large volumes of data, often of a streaming nature.

18. It is true that consumers of IaaS are primarily responsible for containment, eradication, and recovery from incidents.
19. 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.
20. An encryption method can be utilized along with data fragmentation to enhance security.
21. Utilize a client/application encryption method when object storage is used as the back-end for an application.
22. A cloud customer CANNOT submit the CCM on behalf of a CSP to CSA Security, Trust & Assurance Registry (STAR).
23. 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.
24. The most significant security difference between traditional infrastructure and cloud computing is the management plane.
25. The “Segregation by default” opportunity helps reduce common application security issues.
26. An Intrusion Prevention System is NOT normally a method for detecting and preventing data migration into the cloud. (Monitor them for large migrations/activity using tools such as Database Activity Monitoring and File Activity Monitoring)
27. Encryption is usually managed on multi-tenant storage using multiple keys per data owner.
28. Provisioning is NOT an example of Security as a Service (SecaaS).
29. A potential concern of using Security as a Service (SecaaS) is lack of visibility.
30. In volume storage, the data dispersion method is often used to support resiliency and security.
31. When searching for data across cloud environments, a client may not have the ability or administrative rights to search or access all the data hosted in the cloud.
32. It is true that REST APIs are the standard for web-based services because they run over HTTPS and work well across diverse environments.
33. If there are gaps in network logging data, you can “instrument” the technology stack with your own logging.
34. It is true that all cloud services utilize virtualization technologies.
35. 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.
36. An important consideration when performing a remote vulnerability test of a cloud-based application is to obtain provider permission for the test.
37. The Cloud Provider is responsible for the security of the physical infrastructure and virtualization platform
38. When mapping functions to lifecycle phases, the Create and Use functions are required to successfully process data.

39. 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.
40. 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.
41. A service type of network is typically isolated on different hardware because it has distinct functions from other networks.
42. 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.
43. It is arguably false that cloud storage will most often utilize the same types of data storage used in traditional data storage technologies. CSA: “Since cloud storage is virtualized it tends to support different data storage types than used in traditional storage technologies.”
44. Perimeter security is focused on protecting the management plane components, such as web and API servers, from attacks. It includes both lower-level network defenses as well as higher-level defenses against application attacks.
45. 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.
46. The barriers to developing full confidence in security as a service (SecaaS) include Compliance, multi-tenancy, and vendor lock-in.
47. In the Secure Deployment meta-phase, the CSA focuses on security and testing activities when moving code from an isolated development environment to production.
48. A cloud deployment of two or more unique clouds is known as a Hybrid Cloud.
49. The Architectural Relevance column in the CCM indicates the applicability of cloud security to control Physical, Network, Compute, Storage, Application or Data.
50. 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.
51. Hybrid Cloud is commonly used to describe a non-cloud data center **bridged directly** to a cloud provider.
52. 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). An SDLC should be modified to address application security in a Cloud Computing environment based on updated threat and trust models.
53. Cloud built-in firewalls typically offer fewer features than newer physical firewalls.
54. 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.

55. A container is known as a code execution environment running within an operating system that shares and uses the resources of the operating system.
56. The main considerations for key management are performance, accessibility, latency, and security.
57. 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.
58. The three main aspects for data security controls are controlling, protecting, and enforcing.
59. The Incident Response, Notification and Remediation governance domain focuses on proper and adequate incident detection, response, notification, and remediation.
60. The "authorization" component of identity, entitlement, and access management is best described as "enforcing the rules by which access is granted to the resources".
61. It is false that all assets require the same continuity in the cloud.
62. It is true that identified issues, risks, and recommended remediations are included when determining compliance.
63. 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
64. Data security is a key enforcement tool for information and data governance. As with all areas of cloud security, its use should be risk-based since it is not appropriate to secure everything equally.
65. It is true that the Virtual Machine Manager (hypervisor) compute virtualization abstracts an operating system from the underlying hardware.
66. Contracts are the primary tool of governance is the contract between a cloud provider and a cloud customer (this is true for public and private cloud).
67. If the cloud uses the same network address range as your on-premises assets, it is effectively unusable.
68. It is true that sending data to a provider's object storage over an API is likely much more reliable and secure than setting up your own SFTP server on a virtual machine in the same provider.
69. The cloud provider is responsible for ensuring the management plane is secure and necessary security features are exposed to the cloud user, such as granular entitlements to control what someone can do even if they have management plane access.
70. The cloud customer is responsible for properly implementing the available virtualized security controls and understanding the underlying risks, based on what is implemented and managed by the cloud provider.
71. The metastructure contains 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.

72. Bit-by-bit imaging of a cloud data source is generally difficult or impossible. For obvious security reasons, providers are reluctant to allow access to their hardware, particularly in a multi-tenant environment where a client could gain access to other clients' data.
73. While a VM is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still utilizing the kernel and other capabilities of the base OS.
74. In cloud computing, third-party audits and attestations are frequently used to assure compliance with aspects of the cloud provider's infrastructure, allowing a customer to build their own compliant services on top of the cloud platform.
75. The most important reason for knowing where the cloud provider will host the data is because the knowledge is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data.
76. It is true that APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.
77. CCM: The security requirements of the Identity and Access Management domain addresses the requirement to ensure appropriate access to resources and to enable the right individuals to access the right resources at the right times for the right reasons.
78. DAST tests running applications and includes tests such as web vulnerability testing and fuzzing.
79. It is true that DAST might be limited or require pre-testing permission from the provider.
80. SecDevOps or Rugged DevOps refers to integration of security testing into the application development process to produce harder, more secure, and more resilient applications.
81. CI/CD pipelines can enhance security through support of **immutable** infrastructure (fewer manual changes to production environments), automating security testing, and extensive logging of application and infrastructure changes when those changes run through the pipeline.
82. A benefit of application security in a cloud environment is isolated environments.
83. Single cloud assets are less resilient compared with a traditional infrastructure due to greater fragility of virtualized resources.
84. A key element of the Destroy phase of the Data Security Lifecycle is crypto-shredding (or cryptoshredding).
85. When considering business continuity and disaster recovery with a cloud provider, the Applistructure layer is concerned with code and message queues.
86. According to ENISA, VM hopping is using a compromised VM to exploit a hypervisor, used to take control of other VMs.
87. According to ENISA, system or O/S vulnerabilities are among the vulnerabilities contributing to a high risk ranking for Network Management.
88. According to ENISA, globalization is NOT one of the five key legal issues common across all scenarios.

89. According to ENISA, a reason for risk concerns of a cloud provider being acquired is non-binding agreements put at risk.
90. 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.
91. According to ENISA, to mitigate credential compromise or theft, cloud providers can implement anomaly-detection capabilities.