Study Guide

Cloud Concepts,, Architecture and Design for the CCSP ®

# Checklist of Exam Objectives: Areas to Study

## ❏ 1.1 Understand Cloud computing Concepts

### Cloud computing definitions

### Cloud computing roles and responsibilities (e.g., cloud service consumer, cloud service provider, cloud service broker, regulator)

### Key cloud computing characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)

### Building block technologies (e.g., virtualization, storage, networking, databases, orchestration)

## ❏ 1.2 Describe cloud reference architecture

### Cloud computing activities

### Cloud service capabilities (e.g., application capability types, platform capability types, infrastructure capability types)

### Cloud service categories (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)

### Cloud deployment models (e.g., public, private, hybrid, community, multi-cloud)

### Cloud shared considerations (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and service-level agreements (SLA), auditability, regulatory, outsourcing

### Impact of related technologies (e.g., data science, machine learning, artificial intelligence (AI), blockchain, Internet of Things (IoT), containers, quantum computing, edge computing, confidential computing, DevSecOps)

## ❏ 1.3 Understand security concepts relevant to cloud computing

### Cryptography and key management

### Identity and access control (e.g., user access, privilege access, service access)

### Data and media sanitization (e.g., overwriting, cryptographic erase

### Network security (e.g., network security groups, traffic inspection, geofencing, zero trust network)

### Virtualization security (e.g., hypervisor security, container security, security, ephemeral computing, serverless technology)

### Common threats

### Security hygiene (e.g., patching baselining)

## ❏ 1.4 Understand design principles of secure cloud computing

### Cloud secure data lifecycle

### Cloud-based business continuity (BC) and disaster recovery (DR) plan

### Business Impact Analysis (BIA) (e.g., cost-benefit analysis, return on investment (ROI))

### Functional security requirements (e.g., portability, interoperability, vendor lock-in)

### Security considerations and responsibilities for different cloud categories (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS))

### Cloud design patterns (e.g., SANS security principles, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture)

### DevOps Security

## ❏ 1.5 Evaluate cloud service providers

### Verification against criteria (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS)

### System/subsystem product certifications (e.g., common criteria (CC), Federal Information Processing Standard (FIPS) 140-2

# Exam Essentials: What you need to know

#### Golden Keys:

##### Security is security and moving to the cloud will not necessarily provide better, or worse, security.

##### If an organization has a poor security program, then moving to the cloud may just make things more complex

##### Security in the cloud depends on contracts and Service Level Agreements (SLAs)

##### The ‘Cloud’ is a very generic term that can represent many different service models and implementations, often varying by vendor. It is important to understand which model is being discussed when contemplating or managing a cloud deployment

##### Legal and regulatory requirements may restrict where data many be held, accessed, or processed

# Important Terminology

#### Data Owner — the individual that is responsible for the protection of data throughout the data lifecycle. An organization may have more than one data owner, but there must always be one individual that is held accountable for each data element

#### Encryption — The process of rendering sensitive data unreadable through substitution and transposition using a mathematical function (algorithm)

#### Confidentiality — the protection of sensitive data from unauthorized disclosure

#### Due Care — the actions taken by a reasonable, prudent person to protect others from unreasonable harm

#### Due Diligence — the enforcement of the actions of due care

#### Integrity — The measure of accuracy or precision of an entity or process

#### Availability — The measure of the criticality of an entity and the value of the entity to supporting a business process

#### Hashing Algorithms — a mathematical function used to detect changes to data and thereby support integrity

#### Non-repudiation — The ability to link actions to an individual entity

#### Threat — Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. CNSS 4009

#### Attack — Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. CNSSI 4009

#### Asset — an entity with value to its owner

#### Vulnerability — Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source CNSSI 4009

#### Residual Risk — Portion of risk remaining after security measures have been applied CNSSI 4009

#### Risk Acceptance — The level of risk within the limits set by the risk owner

#### Information Security Risk — The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. NIST SP800-30r1

#### Chain of Custody — a documented record of all actions related to evidence throughout the evidence lifecycle

#### Incident — an adverse event with the potential to affect business mission

#### Social Engineering — the manipulation of a person to induce them to do something they should not do

#### Compliance — proven adherence to standards

# Self-Assessment Questions: Test your Understanding

###### The organization has a system that operates on-prem and backs up data to the cloud. What is this an example of?

###### Cloud bursting

###### Community cloud

###### Software as a Service (SaaS)

###### Separation of Duties (SoD)

###### The organization is conducting a risk assessment that determines the risk of using a cloud provider for sensitive data storage. What should the organization be especially aware of?

###### Multi-tenancy

###### Availability

###### Anonymization

###### Security of hash values

###### Identification of traffic based on IP address is probably an example of:

###### MAC filtering

###### Secure transport layer communications

###### Geofencing

###### Escrow

###### The organization is conducting a risk assessment that determines the risk associated with Internet of Things (IoT) devices. What is a common problem with IoT security?

###### Expensive

###### Lack of patching

###### Too much network segmentation

###### Lack of documentation

###### The organization is conducting a risk assessment that determines the risk of using the cloud and needs to know what cloud services they currently use. What can assist in identifying cloud services?

###### DMZ

###### VLAN

###### NIDS

###### CASB

###### An important part of any contract is?

###### Jurisdiction

###### Logging

###### ISO/IEC 27002 certification

###### Witness

###### How can an organization increase download speeds to remote users located around the world?

###### Internet of Things (IoT)

###### Single Sign-on (SSO)

###### Object storage

###### Edge computing

###### What is the best control to mitigate against social engineering?

###### Awareness

###### Firewall

###### Anti-virus

###### Access control

1. What is a key requirement of many privacy laws?
   1. Breach notification
   2. Encryption
   3. Availability
   4. Firewall configuration
2. What security principle should a Cloud Service Provider follow when handling the data of competing organizations?
   1. Dual control
   2. Awareness training
   3. Segregation of duties
   4. Logging
3. An organization has an agreement with a small cloud provider that only has one location to handle and process their data. What should the Cloud Consumer do to ensure availability of data?
   1. Have redundant power feeds
   2. Ensure physical access controls
   3. Move all data to another CSP
   4. Validate the BCP of the cloud provider
4. During which phase of the data lifecycle is the data classified?
   1. Destruction
   2. Archive
   3. Create
   4. Use
5. Who normally controls the encryption keys in a Software as a Service (SaaS) deployment?
   1. The data owner
   2. An escrow agent
   3. The Cloud Service Provider
   4. The Cloud Consumer
6. Which type of encryption algorithm is better suited for bulk data storage?
   1. Asymmetric
   2. Hashing
   3. Hybrid
   4. Symmetric
7. What is the purpose of data classification?
   1. Mandate consistent data handling practices
   2. Highlight data that must be protected
   3. Prevent data loss or corruption
   4. Meet legal requirements

# Answers to Self-Assessment Questions:

###### A – Since the data is only being stored at the CSP it is possible for the consumer to encrypt it and then just destroy the key if the consumer moves to another provider

###### C – All are good answers, but Law is the most important and overrides everything ese – Law is first then Policy then Standards

###### A - A covert channel is hidden; an overt channel is an obvious channel.

###### C – All of these should be done but the best answer is SLA. The SLA will mandate the other controls. Always look to the higher-level management answer in a case like this

###### D - A private cloud only handles data of a single organization

###### C - civil, tort or contract law is related to disputes between individuals

###### A - this is the definition of Recovery Point Objective

###### A – awareness is more effective than technical controls

###### A - many laws specify the need to protect data but do not specify the algorithms that must be used. Laws frequently require notification in the event of a breach.

###### C – The CSP should do all of these – but C is the most important – do not let CSP staff access the data of more than one competing organization. Dual control. Is a way to enforce SoD but will not ensure that the staff do not have access to the data of more than one client

###### D – A and B are the responsibility of the CSP not the consumer. The first step is to see of the CSP has an adequate (tested, realistic) BCP

###### C – The create and store phases often occur at the same time. This is when the classification level of the newly created data should be determined

###### C – The CSP handles both the network and storage keys in most SaaS environments

###### D – symmetric encryption is faster than asymmetric and better suited for bulk data encryption

###### A – the classification mandates the handling requirements for data classified at that level – thereby ensuring proper handling by all users throughout the data lifecycle. B and D are good answers but not the best because not all data must be classified according to legal requirements and while a label indicates data that must be protected, that is not the primary reason to label or classify it.