Study Guide

Cloud Data Security for the CCSP ®

# Checklist of Exam Objectives: Areas to Study

## ❏ 2.1 Describe cloud data concepts

### Cloud data lifecycle phases

### Data dispersion

### Data flow

## ❏ 2.2 Design and implement cloud data storage architecture

### Storage type (e.g., long-term, ephemeral, raw storage)

### Threats to storage types

## ❏ 2.3 Design and apply data security technologies and strategies

### Encryption and key management

### Hashing

### Data obfuscation (e.g.., masking anonymization)

### Tokenization

### Data loss prevention (DLP)

### Keys, secrets, and certificate management

## ❏ 2.4 Implement data discovery

### Structured data

### Unstructured data

### Semi-structured data

### Data location

## ❏ 2.5 Plan and implement data classification

### Data classification policies

### Data mapping

### Data labelling

## ❏ 2.6 Design and implement Information Rights Management (IRM)

### Objectives (e.g., data rights, provisioning, access management)

### Appropriate tools (e.g., issuing and revocation of certificates)

## ❏ 2.7 Plan and implement data retention, deletion, and archiving policies

### Data retention policies

### Data deletion procedures and mechanisms

### Data archiving procedures and mechanisms

### Legal hold

## ❏ 2.8 Design and implement auditability, traceability, and accountability of data events

### Definition of event sources and requirements of event attributes (e.g., Identity, IP address, geolocation)

### Logging, storage, and analysis of data events

### Chain of custody and non-repudiation

# Exam Essentials: What you need to know

#### Golden Keys:

##### Ultimate accountability and responsibility for data protection remains with the cloud consumer

##### Outsourcing the storage and/or processing of data does not transfer liability to the cloud service provider

##### Data classification is used to ensure data is provided the appropriate levels of protection

##### The data owner is the individual responsible for the protection of data throughout the data lifecycle

##### Protecting data in the cloud requires service level agreements (SLAs) and contracts

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

#### The data lifecycle:

##### Create

##### Store

##### Use

##### Share

##### Archive

##### Delete

# 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 can the organization do to protect data from compromise even if the organization changes cloud providers?

###### Crypto-erasure

###### Hashing

###### Physical destruction of hardware

###### Overwriting

###### 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?

###### Cost

###### Availability

###### Legal mandates

###### Lack of skilled staff

###### A hidden channel that releases information in violation of policy or law is known as a:

###### Covert

###### Overt

###### Phishing

###### Logic Bomb

###### The organization is conducting a risk assessment that determines the risk of using a cloud provider for sensitive data storage. What should the organization do to protect their data?

###### Labelling

###### Replication

###### Service Level Agreements (SLAs)

###### Enforce access control

###### The organization is conducting a risk assessment that determines the risk of using a cloud provider for sensitive data storage. Which cloud solution would likely be most secure?

###### Community

###### Public

###### Hybrid

###### Private

###### A dispute between organizations or individuals is probably addressed through which type of law?

###### Criminal

###### Regulatory

###### Civil or tort

###### Customary

###### The measure of acceptable data loss following an incident is known as?

###### RTO

###### MTD

###### RPO

###### BIA

###### 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.