Study Guide

Information Security Principles for CCSP®

# Checklist of Exam Objectives: Areas to Study

|  |  |
| --- | --- |
| **Terminal** | **3.1 Comprehend cloud infrastructure and platform components** |
| Enabling | Physical environment |
| Enabling | Network and communications |
| Enabling | Compute |
| Enabling | Virtualization |
| Enabling | Storage |
| Enabling | Management plane |
| **Terminal** | **3.2 Design a secure data center** |
| Enabling | Logical design (e.g., tenant partitioning, access control) |
| Enabling | Physical design (e.g., location, buy or build) |
| Enabling | Environmental design (e.g., Heating, Ventilation, and Air Conditioning (HVAC), multi-vendor pathway connectivity) |
| Enabling | Design resilient |
| **Terminal** | **3.3 Analyze risks associated with cloud infrastructure and platforms** |
| Enabling | Risk assessment (e.g., identification, analysis) |
| Enabling | Cloud vulnerabilities, threats and attacks |
| Enabling | Risk mitigation strategies |
| **Terminal** | **3.4 Plan and implementation of security controls** |
| Enabling | Physical and environmental protection (e.g., on-premises) |
| Enabling | System, storage and communication protection |
| Enabling | Identification, authentication and authorization in cloud environments |
| Enabling | Audit mechanisms (e.g., log collection, correlation, packet capture) |
| **Terminal** | **3.5 Plan business continuity (BC) and disaster recovery (DR)** |
| Enabling | Business continuity (BC) / disaster recovery (DR) strategy |
| Enabling | Business requirements (e.g.,RecoveryTimeObjective(RTO),RecoveryPointObjective(RPO), recovery service level) |
| Enabling | Creation, implementation and testing of plan |

# Important Terminology & Exam Essentials: What you need to know

**Availability class Protection:** specified in the ISO/IEC 22237 series that specifies redundant and resilient designs to prevent or mitigate outages in a data center.

**Business continuity and disaster recovery (BCDR):**

The capability of an organization to continue delivery of products and services within acceptable time frames at a predefined capacity relating to a disruption along with the ability of the information and communication technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption.

**Business continuity management system (BCMS):**

Combination of activities, roles, and processes involving leadership, recovery

teams, legal and regulatory requirements, risk analysis, and other elements that

programmatically support BCDR.

**Cloud computing interoperability:**

The goal of interoperability is to provide seamless service consumption and management between standalone services and cloud service providers.

**Cloud computing**

**Portability:**

The goal of portability is to enable cloud service customers to move their data or

applications between standalone services and cloud service providers.

**Cloud orchestration:**

End-to-end automation workflow, or process, that coordinates multiple lower-level

automation to deliver a resource or set of resources “as a service.”

**Control plane:** Control of network functionality and programmability is directly made to

devices at this layer. OpenFlow was the original framework/protocol specified to

interface with devices through southbound interfaces.

**Cyber kill chain**:

Lockheed Martin developed a cyber kill chain methodology that helps to sort out

correlation from causation. An attack is broken up into six steps. If the defender

disrupts any of the first six steps of the cyber kill chain, they can prevent the

successful carriage of the attack.

**Data plane**: The network switches and routers located at this plane are associated with the

infrastructure. The process of forwarding data is accomplished at this plane, so it can

also be referred to as a forwarding plane.

**Disaster recovery as a service (DRaaS):**

Service provided to on-premises data centers to recover to/from the cloud.

**East-west traffic**: Network traffic that traverses systems within a data center.

**Hyperconverged**

**Infrastructure:**

The cross-sectional control of major services consumed in a data center includes

compute, storage, and network systems.

**Hypervisor (Type 1):**

Commonly known as a bare-metal, embedded, or native hypervisor. Works directly on the hardware of the host and can monitor operating systems that run above the hypervisor. The hypervisor is small, as its main task is sharing and managing hardware resources between

different guest operating systems.

**Hypervisor (Type 2):**

Installed after a traditional operating system and supports other guest operating systems running above it as virtual machines. Completely dependent on the host operating system for its operations.

**IP Flow Information Export Protocol (IPFIX):**

Standard protocol RFC 7011 that is used to determine the nature of network traffic. Traffic on a data network can be seen as consisting of flows passing through network elements. For administrative or other purposes, it is often interesting, useful, or even necessary to have access to information about these flows that pass through the network elements.

**Limits:**

A maximum resource allocation per VM. This ceiling may be fixed or expandable, allowing for the acquisition of more compute resources through a “borrowing” scheme from the CSP.

**Management plane:**

Controls the entire infrastructure; parts of it will be exposed to customers independent of network location. It is a prime resource to protect.

**Micro segmentation:**

Identification of network traffic flows (see east-west/north-south) that lead to creating

granular policy schemes to isolate access for and based upon specific workloads.

**Network-attached storage (NAS):**

A file-level computer data storage server connected to a computer network provides data access to a heterogeneous group of clients.

**Network function virtualization (NFV):**

Alternately referred to as virtual network function. The objective of NFV is to decouple functions, such as firewall management, intrusion detection, network address translation, and name service resolution, away from specific hardware implementation and move them into

software solutions. NFV’s focus is to optimize distinct network services.

**North-south traffic:**

Network traffic that travels to and from the internet to a data center.

**Object storage:**

Objects (files) are stored with additional metadata (content type, redundancy required, creation date, etc.). These objects are accessible through APIs and potentially through a web user interface.

**Open Virtualization Format (OVF):**

Syntactic standard of sending and receiving data between different vendor virtualization systems.

**Protect surface:**

The specific area (systems/resources) afforded protection through isolation and micro-segmentation.

**Protection classes:**

Consigned to spaces within a data center. As you arrive at the most central location, or the core, in the data center, you will find the systems that garner the greatest levels

of protection as they are the most critical and highly valued.

**Recovery point objective (RPO):**

Relates to the amount of data that is lost and unrecoverable due to the disruption. This is represented on the timeline as the amount of time between the last good backup and when the disruption event occurs.

**Recovery time objective (RTO):**

Per product, service, or activity, the acceptable amount of time from the point at which a disruption occurs until the product, service, or activity is recovered.

**Region:**

A geographic span containing multiple zones hosted by a cloud provider.

**Reservations:**

A guaranteed minimum resource allocation, which must be met by the host with physical compute resources in order to allow for a guest to power on and operate.

**Security group:**

VPC- and VM-associated access control list for allowance or denial of ingress and egress traffic flows.

**Shares:**

If resource contention takes place, share values are used to prioritize compute resource access for all guests assigned a certain ratio of shares.

**Software-Defined Network (SDN):**

###### Network capability that abstracts the functions of routers and switches to create data-centric control verses infrastructure-centric

**Trusted Platform Module (TPM):**

Isolated and separate compute and storage unit that enables trust in computing platforms by employing security and privacy techniques using cryptography.

**Virtual Private Cloud (VPC):**

A logically isolated section of a cloud (not a private cloud per se) where resources can

be launched in a virtual network that is customer-defined. The customer has complete control over their virtual networking environment, including selection of private IP address range,

creation of subnets, and configuration of route tables and network gateways.

**Volume storage:**

A virtual hard drive that can be attached to a virtual machine instance and be used to

host data within a file system. Storage is written to committed blocks of data. Volumes attached to IaaS instances behave just like a physical drive or an array does.

**Zero Trust Model:**

Removing the design belief that the network has any trusted space. Security is managed

at a protected surface, representing the most granular asset. Micro-segmentation of workloads is a tool of the model.

**Zone:**

One or more data centers hosted by a cloud provider.

# Self-Assessment Questions: Test your Understanding

###### What architecture is designed to abstract the functionality of routers and switches to move from infrastructure-centric management to data-centric management?

###### IT Infrastructure Library

###### Multi-Protocol Label Switching (MPLS)

###### Software Defined Network (SDN)

###### Border Gateway Protocol (BGP)

###### What type of storage is automatically attached to launched VM?

###### Volume

###### Object

###### Ephemeral

###### Long-term

###### How does zero trust mitigate common threats that spread within a network?

###### Through web application firewalls

###### Through trusted and untrusted zoning

###### Using always-on technology

###### Through micro-segmentation and explicit-allow

###### A cloud provider is experiencing an errant process on a physical computing system that is serving up launched instances on bare-metal. The problem begins to affect the minimum compute power guaranteed to each guest host. What settings will allow the guest to consume the most amount of computing resources that represent their SLA?

###### Limits

###### Reservations

###### Service Level Objections

###### Shares

###### A cloud service provider has experienced the outage of a data center. What configuration item allows the customer to still access their data without interruption?

###### Regions

###### Zones

###### Soft-ware defined network

###### Network Function Virtualization

###### What disaster recovery item would consider the amount of data loss hosted by a workload versus the recovery of the workload itself?

###### Maximum tolerable period of disruption

###### Recovery time objective

###### Recovery point objective

###### Maximum tolerable downtime.

###### What kind of testing induces failure on systems that are in a production environment thus giving you the greatest confidence of resiliency?

###### Chaos engineering

###### Component

###### Full

###### Parallel

1. What is another name for a Type II hypervisor?
   1. Bare-metal
   2. Hosted
   3. Non-OS
   4. Overlapping fragment
2. Which plane of a Software Defined Network (SDN) can you abstract the infrastructure into a business need?
   1. Data
   2. Control
   3. Management
   4. Application
3. What is a major risk to cloud computing?
   1. Extreme cost
   2. Shared responsibilities
   3. Insufficient due diligence
   4. Lack of transparency

# Answers to Self-Assessment Questions:

###### C – SDN abstracts the functionality of routers and switches to be data-centric.

1. A – Volume storage on a VM is as a disk in a server.

###### D- Micro-segmentation and explicit allowing to specific resources are major tenants of zero trust.

###### D – Shares allow a ratio of consumption based upon the contention of what is leftover from the CSPs compute pool.

###### B - Zones contain one or more data centers that have high-speed replicas.

###### C – The recovery point objective represents the amount of data the business can tolerate the loss of.

###### A – Chaos engineering induces failure in live productions systems to prove resilience.

###### B – A type II hypervisor can be hosted on a traditional OS as an application.

###### A – The data plane transitions a network from infrastructure-centric to data-centric by abstracting the infrastructure to forward data.

###### C – Insufficient due diligence with granularity of controls is a top risk of cloud computing.