KORNERSTONE
a TRAINOCATE company

Training. Makes a differece.

# Certified Cloud Security Professional, CCSP®

## Introduction

# Cloud Computing Security
# **Introduction**

# About (ISC)2 CCSP

- Certified Cloud Security Professional
- Jointly developed by (ISC)2 and Cloud Security Alliance (CSA)

- to ensure that cloud security professionals have the required knowledge, skills, and abilities in *cloud security design, *implementation, *architecture, *operations, controls, and *compliance with regulatory frameworks.

- applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge.

- a standalone credential that complements and builds upon existing credentials and educational programs, including

(ISC)²'s CISSP and CSA's CCSK.

# CCSP Domains

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance

# CCSP – Experience Requirements

- Minimum 5 years of cumulative paid full-time information technology experience;
- of which 3 years must be in information security and 1 year in one of the 6 domains of the CCSP.
- CSA's CCSK can be substituted for 1 year of experience in one of the 6 domains of CCSP.
- (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement.
- If not have the required experience above, may first become an Associate of (ISC)² by successfully passing the CCSP; then have 6 years to earn the 5 years required experience.

Accreditation

CCSP under ANSI review for compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024

# CCSP Examination Information

| | |
|---|---|
| **Length of exam** | 4 hours |
| **Number of questions** | 125 |
| **Question format** | Multiple choice |
| **Passing grade** | 700 out of 1000 points |
| **Exam availability** | English |
| **Testing center** | Pearson VUE Testing Center |

- Endorsement of certificate attainment
- Maintain 90 CPEs per year

# CCSP Exam Domain Weights

| Domains | Weight |
|---|---|
| 1. Architectural Concepts & Design Requirements | 19% |
| 2. Cloud Data Security | 20% |
| 3. Cloud Platform & Infrastructure Security | 19% |
| 4. Cloud Application Security | 15% |
| 5. Operations | 15% |
| 6. Legal & Compliance | 12% |

# 1. Architectural Concepts and Design Requirements

- Cloud computing concepts and definitions based on the ISO-17788 standard;
- security concepts and principles relevant to secure cloud computing.

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services

# 2. Cloud Data Security

- Concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability in cloud environments.

- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

# 3. Cloud Platform and Infrastructure Security

- Knowledge of the cloud infrastructure components, both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.

- Comprehend Cloud Infrastructure Components
- Analyze Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

# 4. Cloud Application Security

- Processes involved with cloud software assurance and validation; and the use of verified secure software.

- Recognize the need for Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Software Development Life-Cycle (SDLC) Process
- Apply the Secure Software Development Life-Cycle
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

# 5. Operations

- Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it;
- requirements of cloud architecture to running and managing that infrastructure;
- definition of controls over hardware, media, and the operators with access privileges as well as the
- auditing and monitoring are the mechanisms, tools and facilities.

# 5. Operations (cont'd)

- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct Risk Assessment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

# 6. Legal & Compliance

- Addresses ethical behavior and compliance with regulatory frameworks.
- Includes investigative measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics);
- privacy issues and audit process and methodologies;
- implications of cloud environments in relation to enterprise risk management.
- Understand Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues, Including Jurisdictional Variation
- Understand Audit Process, Methodologies, and Required Adaptions for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
- Execute Vendor Management

# Cloud Security - Introduction

- A macro-view (high-level) management and policy concept

- Due to
  - Outsourcing model of cloud computing
  - Lack of visibility, thus lack of control
  - Lack of ability to demonstrate compliance
  - Need to deal with different laws in different locations and domains, eg. Data sovereignty vs offsite DR/BC service.

# Cloud Computing – NIST Definition

- NIST SP-800-145 (Sep-2011)

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models.

# NIST Cloud Definition

**5 Essential Characteristics:**

- On-demand self-service.
- Broad network access.
- Resource pooling.
- Rapid elasticity.
- Measured service

# NIST Cloud Definition

- **Essential Characteristics:**

**1. <u>On-demand self-service</u>.**

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

**<u>2. Broad network access.</u>**

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

# NIST Cloud Definition

- **Essential Characteristics:**

**3. Resource pooling.**

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

# NIST Cloud Definition

**Essential Characteristics:**

**4. Rapid elasticity**.

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

**5. Measured service.**

Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

# NIST – Cloud – Service Models

**Currently 3 Official**

1. IAAS
2. PAAS
3. SAAS

# NIST – Cloud – Service Models

1. **Infrastructure as a Service (IaaS).**

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

**2. Platform as a Service (PaaS).**

- The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming

# NIST- Cloud – Service Models

**3. Software as a Service (SaaS).**

- The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

# NIST – Cloud – Deployment Models

- Public Cloud – basic concept model
- Private Cloud (own assets)
- Hybrid Cloud (mix private & public clouds)
- Community Cloud (less often referred to)

# NIST – Cloud – Deployment Models

**1. Public cloud.**

• The cloud infrastructure is provisioned for open use by the general public.

•It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

**2. Private cloud.**

•The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).

•It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- *(new "hybrid private cloud"?! Eg AWS offering)*

# NIST - Cloud – Deployment Models

**3. Hybrid cloud.**

•The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

**4. Community cloud.**

•The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
*(funny thing this was how the internet started long ago)*

•It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

# Cloud Services Activity

1. _____ Automatic updates and patch management
2. _____ Globally distributed development teams are able to work together on software development projects
3. _____ Reduced energy and cooling costs
4. _____ Standardization and compatibility
5. _____ Operating system can be changed and upgraded frequently

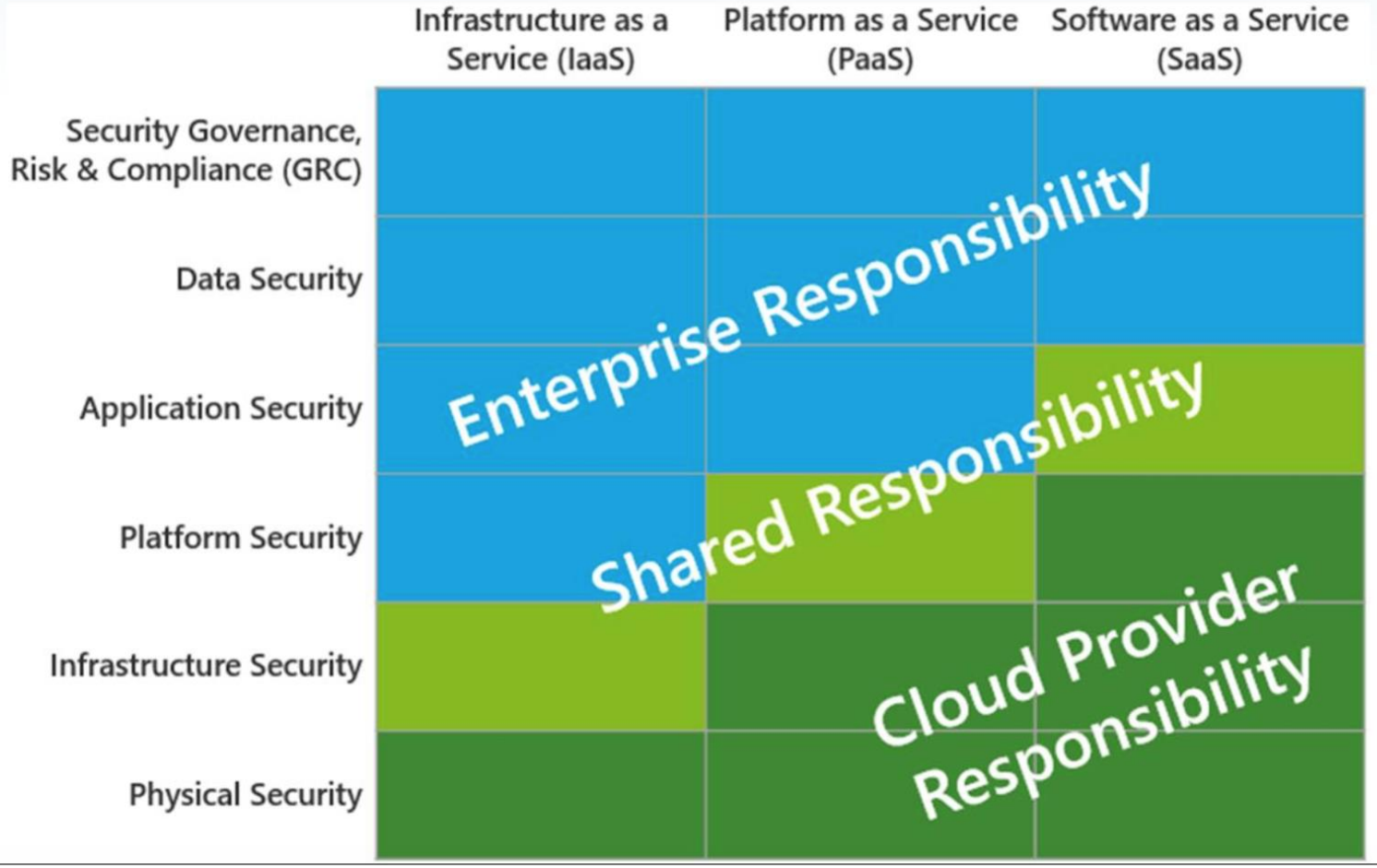
a. SaaS
b. PaaS
c. IaaS

# Storage Types Review Activity

a. IaaS
b. PaaS
c. SaaS

1. _____ Self-service models for accessing, monitoring, and managing remote data center infrastructures
2. _____ Many applications can be run directly from a web browser without any downloads or installations required, although some require small plugins
3. _____ Provides developers with a framework they can build upon to develop or customize applications
4. _____ Uses volume storage and object storage as storage types
5. _____ With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, and networking
6. _____ Uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the client's' side

# Responsibility Depending on the Type of Cloud Service



# Security properties (C-I-A) - per ISO-17788 (from ISO-27000)

- **3.1.1 availability**: Property of being accessible and usable upon demand by an authorized entity.
- **3.1.2 confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **3.1.3 information security**: Preservation of **confidentiality** (3.1.2), **integrity** (3.1.4) and **availability** (3.1.1) of information.
- NOTE: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
- **3.1.4 integrity**: Property of accuracy and completeness.

# Cloud Computing – definition per ISO-17788

**3.2.5 cloud computing**:

•Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

•NOTE : Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

# Some more cloud definitions - per ISO-17788

- **3.2.1 application capabilities type**: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can use the **cloud service provider's** (3.2.15) applications.
- **3.2.2 cloud application portability**: Ability to migrate an application from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).
- **3.2.3 cloud auditor**: **Cloud service partner** (3.2.14) with the responsibility to conduct an audit of the provision and use of **cloud services** (3.2.8).
- **3.2.4 cloud capabilities type**: Classification of the functionality provided by a **cloud service** (3.2.8) to the **cloud service customer** (3.2.11), based on resources used.
- NOTE The **cloud capabilities types** are **application capabilities type** (3.2.1), **infrastructure capabilities type** (3.2.25) and **platform capabilities type** (3.2.31).

# Some more cloud definitions per ISO-17788

- **3.2.6 cloud data portability**: **Data portability** (3.2.21) from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).
- **3.2.7 cloud deployment model**: Way in which **cloud computing** (3.2.5) can be organized based on the control and sharing of physical or virtual resources.
- NOTE The **cloud deployment models** include **community cloud** (3.2.19), **hybrid cloud** (3.2.23), **private cloud** (3.2.32) and **public cloud** (3.2.33).
- **3.2.8 cloud service**: One or more capabilities offered via **cloud computing** (3.2.5) invoked using a defined interface.

# Some more cloud definitions per ISO-17788

- **3.2.9 cloud service broker**: **Cloud service partner** (3.2.14) that negotiates relationships between **cloud service customers** (3.2.11) and **cloud service providers** (3.2.15).
- **3.2.10 cloud service category**: Group of **cloud services** (3.2.8) that possess some common set of qualities.
- NOTE A **cloud service category** can include capabilities from one or more **cloud capabilities types** (3.2.4).
- **3.2.11 cloud service customer**: **Party** (3.1.6) which is in a business relationship for the purpose of using **cloud services** (3.2.8).
- NOTE: A business relationship does not necessarily imply financial agreements.

# Cloud – more ISO-17788 definitions

- The **cloud service customer** (3.2.11) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The **cloud service customer** (3.2.11) may also have limited ability to control certain networking components (e.g., host firewalls).
- **3.2.25 infrastructure capabilities type**: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can provision and use processing, storage or networking resources.
- **3.2.26 measured service**: Metered delivery of **cloud services** (3.2.8) such that usage can be monitored, controlled, reported and billed.
- **3.2.27 multi-tenancy**: Allocation of physical or virtual resources such that multiple **tenants** (3.2.37) and their computations and data are isolated from and inaccessible to one another.

# Cloud – more ISO-17788 definitions

- **3.2.29 on-demand self-service**: Feature where a **cloud service customer** (3.2.11) can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider** (3.2.15).
- **3.2.30 Platform as a Service (PaaS)**: **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is a **platform capabilities type** (3.2.31).
- **3.2.31 platform capabilities type**: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the **cloud service provider** (3.2.15).

# Cloud – more ISO-17788 definitions

- **3.2.32 private cloud**: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are used exclusively by a single **cloud service customer** (3.2.11) and resources are controlled by that **cloud service customer** (3.2.11).
- **3.2.33 public cloud**: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are potentially available to any **cloud service customer** (3.2.11) and resources are controlled by the **cloud service provider** (3.2.15).
- **3.2.34 resource pooling**: Aggregation of a **cloud service provider's** (3.2.15) physical or virtual resources to serve one or more **cloud service customers** (3.2.11).

# Cloud – more ISO-17788 definitions

- **3.2.35 reversibility**: Process for **cloud service customers** (3.2.11) to retrieve their **cloud service customer data** (3.2.12) and application artefacts and for the **cloud service provider** (3.2.15) to delete all **cloud service customer data** (3.2.12) as well as contractually specified **cloud service derived data** (3.2.13) after an agreed period.
- **3.2.36 Software as a Service (SaaS)**: **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is an **application capabilities type** (3.2.1).
- **3.2.37 tenant**: One or more **cloud service users** (3.2.17) sharing access to a set of physical and virtual resources.

# Cloud Data Portability – per ISO-17788

**3.2.21 data portability**:

•Ability to easily transfer data from one system to another without being required to re-enter data.

•NOTES:

- It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system.
- But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools.
- On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy".

# Cloud – Definitions Per ISO-17788

## SLA – Service Level Agreement (per ISO-20000)

- Documented agreement between the service provider and customer that identifies services and service targets.
- NOTES:

1. A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.
2. A service level agreement can be included in a contract or another type of documented agreement.

# Cloud : NIST-800 vs ISO-17788

## NIST

- On demand self-service
- Broad network access
- Resource pooling
- Rapid Elasticity
- Measured service

## ISO 17788

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity and scalability
- Measured service
- Multi-tenancy

# Cloud Eco-system Players