CCSP Study Notes - September 2021

--

Purpose: Collect only the most important pieces of information that have a high or very high likelihood of appearing on my CCSP exam.

Take down notes that are most likely to help me achieve a higher score on the final CCSP exam.

DOMAIN 1: Cloud Concepts, Architecture and Design (17%)

Cloud Characteristics

The **five** essential cloud characteristics:
Remember - "MR. BRO"

1. **M**easured service
2. **R**apid Elasticity
3. **B**road network access
4. **R**esource Pooling
5. **O**n-Demand self-service
6. An additional 6th characteristic is also **Multitenancy**.

Cloud Reference Architecture

Four cloud deployment models:

1. Public cloud
2. Private cloud
3. Community
4. Hybrid cloud

Three service categories (and associated benefits):

1. Infrastructure as a Service (IaaS)
    a. Cost efficiency
    b. Availability and reliability
    c. Scalability
2. **Platform as a Service (PaaS) - Focus on PaaS and examples of real-world use**
    a. Cost efficiency
    b. Flexibility
    c. Simplicity
    d. Ease of access
3. Software as a Service (SaaS)
    a. Cost efficiency
    b. Licensing
    c. Standardization

Security Concerns based on Cloud Service Category

IaaS

- Colocation and multitenancy
- Virtual machine (VM) attacks
- Hypervisor attacks
- Network security
- Denial of service (DoS) attacks

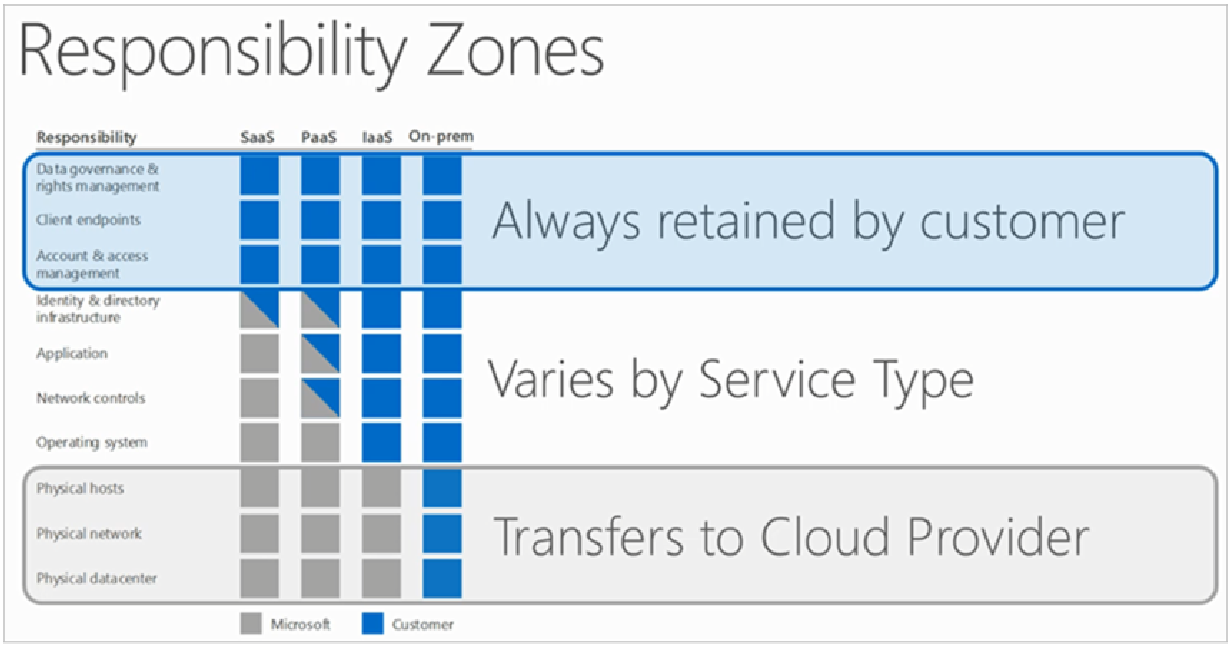
PaaS

- Resource isolation
- User permissions
- User access management
- Malware, trojans, backdoors and threats

SaaS

- Data comingling
- Data access policies
- Web application security

Shared responsibility model.
Know where the responsibilities ultimately lie between the cloud service provider (CSP) and the cloud customer for each of the three (3) cloud service categories.



Responsibility Zones

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	🟦	🟦	🟦	🟦
Client endpoints	🟦	🟦	🟦	🟦
Account & access management	🟦	🟦	🟦	🟦
Identity & directory infrastructure	▨/🟦	▨/🟦	🟦	🟦
Application	▨	▨/🟦	🟦	🟦
Network controls	▨	▨/🟦	🟦	🟦
Operating system	▨	▨	🟦	🟦
Physical hosts	▨	▨	▨	🟦
Physical network	▨	▨	▨	🟦
Physical datacenter	▨	▨	▨	🟦

▨ Microsoft 🟦 Customer

Infrastructure: The core cloud components. Compute (CPU), network, memory (RAM), storage. Infrastructure is the foundation that everything else is built on. The moving parts.
Metastructure: Set of protocols and mechanisms that connects the infra layer to the applications and data being used. It ties together the technologies and enables management and configuration of cloud computing.
Infostructure: The data and information. Content in a database, file storage, etc.
Applistructure: Includes the apps that are deployed in the cloud and the underlying services used to build them.

The Three (3) Data States

1. Data at rest
2. Data in transit
3. Data in use

Reporting and Compliance

Service Organisation Controls (SOC)
3 types of reports.

1. **SOC 1** - Focuses strictly on an organisation's financial statements. Generally required or used by organisations that perform payroll or credit card processing.

2. **SOC 2** - Tightly controlled. Usually contains sensitive information relating to information security controls, etc.
    a. **Type 1 Report** = Point in time assessment of the implemented controls
    b. **Type 2 Report** = Period of time (~6 months) assessment on the effectiveness of the controls implemented.

    Based on AICPA's 5 key trust principles:
    1. Security
    2. Availability
    3. Processing Integrity
    4. Confidentiality
    5. Privacy
3. **SOC 3** - Loosely controlled. Used for general public consumption.

System/Subsystem product certifications

Common Criteria (CC)

- Protection profiles
- Evaluation Assurance Levels (EALs) - 7 levels

FIPS 140-2 / 140-3

- Federal Information Processing Standard (FIPS)
- Contains 4 levels of product security rating (1 lowest to 4 highest)

DOMAIN 2: Cloud Data Security (19%)

Cloud Secure Data Lifecycle: C-S-U-S-A-D

- Create
- Store
- Use
- Share
- Archive
- Destroy

Common Storage Types:

Types of cloud storage. Remember "FOB"...

- File Storage (NAS)
    - Protocol: CIFS and NFS
- Object storage
    - Protocol: REST and SOAP over HTTP
- Block storage
    - Protocol: SCSI, Fibre Channel, SATA

Object Storage

A key issue relating to Object storage that all Cloud Service Providers need to be aware of is:

Data consistency can only be achieved after change propagation to all replica instances occurs

Explanation: An object storage system typically comes with minimal features. It gives the ability to store, copy, retrieve and delete files and also gives authority to control which user can perform these actions. If you want to be able to search or have an object metadata central repository for other apps to draw on, you have to do it by yourself. Many storage systems such as Amazon S3 provide REST APIs to let programmers work with objects and containers. However, what Cloud Service Providers need to know about object storage systems is that they can only achieve data consistency in the end. Whenever a file is updated, you have to wait for the change to be propagated to all replicas before requests can return the latest version. This is why object storage is unsuitable for data that constantly changes. But it can be a good solution for stagnant data like audio and video files, archives, backups and machine images.

Storage Types by Cloud Service Category

IaaS:

- Volume (Same as Block):
    - Uses a file system; NTFS, FAT32...etc
- Object:
    - Generally accessed through an API or web interface, without being attached to an operating system.
    - Stores object data and metadata.
    - Examples include Azure Blob storage, AWS S3 buckets.

PaaS:

- Structured:
    - Highly organised, and normalised.

    - Commonly used for relational databases (SQL).
- Unstructured:
    - Not easily organised or formatted.
    - Data types can be things like audio files, images, videos...etc.

SaaS:

- Information storage and management:
    - Involves customers entering data into the application via a web interface.
    - Application stores data and manages that data in a back-end database.
    - Application generated data.
- Content and file storage:
    - The customer uploads data through the web application.
    - Files are stored using mechanisms that users can access.

Encryption and key management

Encryption architecture has three basic components:

1. The data being secured
2. The encryption engine that performs all encryption operations
3. The encryption keys used to secure the data

Database Encryption

Database encryption comes with the following options, each of which is explained.

Transparent Encryption: A large number of database management systems have the ability to encrypt the complete database or even some portions of it. In transparent encryption, the encryption engine resides in the database and is transparent to the application. The Keys reside within the instances while their management and processing may be offloaded to an external Key Management System. This type of encryption is effective in protecting from database and application-level attacks, media theft and backup system intrusion.

File Level Encryption: The database server resides on volume storage. The database folder or volume is encrypted, and the encryption engine and keys reside on instances attached to the volume. It protects against lost backups, external attacks and media theft.

Application Level Encryption: The encryption engine resides in the application using the database. It protects against a wide array of threats that include application-level attacks, compromised databases and administrative accounts.

Data Classification

Sensitive Data Types

Three main categories of highly regulated sensitive data

1. Protected Health Information (PHI)
2. Personally Identifiable Information (PII)
3. Cardholder data

Information Rights Management (IRM)

- Data security technology.

- Combines data encryption with granular identity and authorisation management.
- Allows you to control and manage access to data as it moves across various locations.
- Important and effective tool for cloud environments.
- IRM protects data regardless of location.

Event Sources and Identity Attribution

SaaS event sources

Data Protection - IRM and DRM

Information Rights Management (IRM)

Data De-identification

Masking

- Substitution
  - Mimics the look of real data
  - Replaces real data with unrelated values
  - Can be random or algorithmic (two-way substitution using a reversible algorithm)
- Scrambling
  - Jumbles the data characters into a random order
- Deletion or Nulling
  - When used, data appears blank or empty to anyone who isn't authorised to view it

Two primary methods/strategies for data masking are:

1. Static data masking
2. Dynamic data masking

Tokenisation

Data Discovery

Labels
Metadata
Content

DOMAIN 3: Cloud Platform and Infrastructure Security (17%)

Comprehending Cloud Infrastructure Components

Cloud infra is comprised of

- Physical environment
- Networking resources
- Compute resources
- Virtualisation capabilities
- Storage resources
- Management plane

Network and communications

Some key concepts:

- Routing
- Filtering
- Rate limiting
- Address allocation
- Bandwidth allocation

Software-Defined Networking (SDN)

Consistent and holistic management across various applications and technologies.

- Abstracts network control from network forwarding capabilities (like routing).

[DATA LAYER] <-> [CONTROL LAYER] <-> [INFRASTRUCTURE LAYER]
Applications SDN controller Network devices

Compute

- CPU = Compute
- RAM = Processing / Memory

Virtual Machines (VMs)

Emulate the functionality of physical machines.

- CSP provides support for VMs
- Cloud Consumer is **responsible** for managing VM instances and data within VMs.

Containers

Containers package only the necessary code, config, and resources needed to run a particular application.

- Good for **portability**
- Easy to 'lift and shift' because containers are abstracted from the underlying operating system (OS) of the host machine.
- Containers don't run an entire OS - instead, they use the **kernel** of the VM or OS they are hosted on.
- Rapid scalability.

Reservations, Limits, and Shares

- Reservation = minimum resource allocation
- Limit = maximum resource utilisation / opposite of reservation
    - Best used within a development environment (not production) as development environments will want to keep costs to a minimum.
- Share = method to resolve **resource contention**
    - Share values are used to allocate resources to all tenants assigned a share value
    - Tenants with higher share value receive a larger portion of resources available

Virtualisation

Benefits of virtualisation:

1. Increases scalability
2. Allows faster resource provisioning
3. Reduces downtime
4. Avoids vendor lock-in
    a. Virtualisation abstracts software from hardware, meaning virtualised resources are more **portable**. Virtualisation makes moving between CSPs easier.
5. Saves time (and money) - centrally managed, reduced equipment

Hypervisor abstracts software from hardware. Allows each guest OS to share the host's hardware resources.

Remember the two types of hypervisors - **type 1** and **type 2**.
Type 1 = Bare metal, physical host
Type 2 = Software hypervisor. Sits on the host OS. Greater attack surface.

Virtualisation challenges:

- Hypervisor security
- VM security
- Network security
- Resource utilisation

Management Plane

Cloud vulnerabilities, threats, and attacks

- Management plane compromise
- Incomplete data deletion and sanitisation
- Insecure multitenancy
- Resource exhaustion
- Network, OS, and application vulnerabilities

DOMAIN 4: Cloud Application Security (17%)

Secure Software Development Lifecycle (SDLC)

- Planning
- Define
- Design
- Develop
- Testing
- Deploy and maintain

OWASP Top 10

CSA Treacherous Twelve and Egregious Eleven

Two common software development methodologies

1. Waterfall - rigid, linear.
2. Agile - Flexible. High level of collaboration. Cyclical.

OWASP Top 10 - Web application vulnerabilities
CSA Egregious Eleven - Top Cloud Threats

Threat Modelling

Two common threat modelling (TM) methodologies;

1. STRIDE
2. PASTA - Process for Attack Simulation and Threat Analysis
   a. Define Objectives
   b. Define technical scope
   c. Perform app decomposition
   d. Complete threat analysis
   e. Conduct vuln analysis
   f. Model attacks
   g. Conduct risk and impact analysis
3. DREAD - Focuses on coming up with a quantitative value for assessing risks and threats.
   a. Damage Potential
   b. Reproducibility
   c. Exploitability
   d. Affected Users
   e. Discoverability

Risk_DREAD = (Damage + Reproducibility + Explotability + Affected Users + Discoverability) / 5

Apply Cloud Software Assurance and Validation

Functional Testing

- White box testing; complete knowledge of application, code known
- Black box testing; opposite to white, unknown details of the system

Security Testing Methodologies

- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Vulnerability scanning
  - Cloud service category (IaaS, PaaS, SaaS) will impact your responsibility for vuln scanning and what components can be scanned by you, the cloud customer vs. the CSP.
- Penetration testing

Using Verified Secure Software

Application Virtualisation and Orchestration

Designing Appropriate Identity and Access Management (IAM) Solutions

DOMAIN 5: Cloud Security Operations (17%)

Virtualisation and Trusted Platform Module (TPM)

ISO/IEC standard for Trusted Platform Module - **ISO 11889**.
The standard for architectural and security information related to TPMs.

TPM's provide the following functions:

- Platform integrity
- Drive encryption
- Password protection - Passwords can be stored using a TPM.

TPMs are generally certified using FIPS-140-2 certification to verify the level of protection the specific TPM can provide.

Virtual TPM (vTPM) is provided by the **hypervisor** of a virtualisation host. Virtual TPMs provide the same level of security as physical TPMs to virtual machines and guest operating systems.

vTPMs rely on the hypervisor to provide an isolated environment.

Storage Controllers

Controller-based encryption. Storage controllers are able to encrypt data at the controller level before the data is sent to the disk.

iSCSI protocol is often used to provide virtualised network-based storage.
iSCSI is IP-based storage that enables the use of SCSI over TCP/IP.
Supports CHAP, Kerberos for authentication and IPsec for encrypted comms.

Virtualisation Management Tools

KVM
Console-based access
Remote Access (RDP)

Unsorted Notes

Follow up: Risks to the organisation when returning to normal operations too soon. Is this mentioned anywhere in the CCSP material?

Given explanation: “If you return to normal or what you think should be normal too soon there is a risk of being right back where you started, there are risks from potentially not validating that everything is restored properly, think transaction ledgers and possible double posting or missing posts.”

Cloud Responsibility Matrix (CRM) - try and get one of these from the internet.
Shared Responsibility Model - find good, detailed examples of this in diagram format.

Map out all cloud security controls for each phase of the secure data lifecycle (CSUSAD).

eDiscovery in cloud environments - who is responsible for collecting data?

- The cloud customer AND the cloud provider. Both are responsible.
- The degree or extent to which each party is responsible will vary depending on the cloud service category and deployment model.

Authentication / Authorisation Mechanisms:

SAML:

OAuth:

- Used to provide an authorisation mechanism from one service to another.
- The current version is OAuth 2.0 - **not backwards compatible** with OAuth v1.1.
- Valet key example - only provides access to the car for a set amount of time and allows the valet to perform a limited set of actions.
- Access delegation.
- Uses tokens to provide access permissions for services.
- Trustable (cannot be tampered with)
- Token uses JSON Web Token format (JWT)

Software-Defined Networking (SDN)
Attributes of SDN include the following:

- The network control plane is separated from the forwarding plane.
- Can be run on general-purpose/commodity hardware.
- Presents as a logical switch to the applications running above.
- Can be accessed/administered via API's that can configure, manage and secure network resources.
- Northbound interface (NBI) usually handles traffic between the SDN controllers and the SDN Applications.
- Southbound interfaces (SBI) main function is to enable communication between the SDN controller and the network nodes (both physical and virtual switches and routers).

Cloud Risk Management:
You can never outsource the ownership of risk in the public cloud, only some of the *risk management* can be outsourced to the cloud provider. As the cloud customer/consumer - you will ALWAYS retain full accountability for risk management in the cloud.

Types of risk management available in the cloud:

1. Manage
2. Accept
3. Transfer
4. Avoid

Data Discovery Approaches: - Data Analysis ***IN PROGRESS***

- Real-time Analytics
- Agile Analytics / Business Intelligence
- Big Data
- Observe polyglotism

Insight into the "uses of data"

- Any ACTION being taken on data would be considered a form of **processing**.
- A PASSIVE action such as "viewing" data is not a form of processing as the data is simply being shown and not USED/ACTED upon (processed).

IMPORTANT ISO/IEC STANDARDS

ISO/IEC 27001:2013 = Global standard for the implementation of an enterprise-wide ISMS
ISO/IEC 27002 = Best practice guidelines on HOW to implement ISO 27001
ISO/IEC 27017 = Security guidelines, controls for cloud
ISO/IEC 27018 = Privacy of PII in cloud environments
ISO/IEC 27036 = Supply Chain Security
ISO/IEC 27050 = Digital Forensics
ISO/IEC 11889:2009 = Information Technology - Trusted Platform Module
ISO/IEC 15408 = Common Criteria

IMPORTANT NIST STANDARDS

NIST 800-37
NIST 800-53 - Security and Privacy Controls for U.S Federal Information Systems (FedRAMP)
NIST 800-145 - Cloud Computing Terms and Components

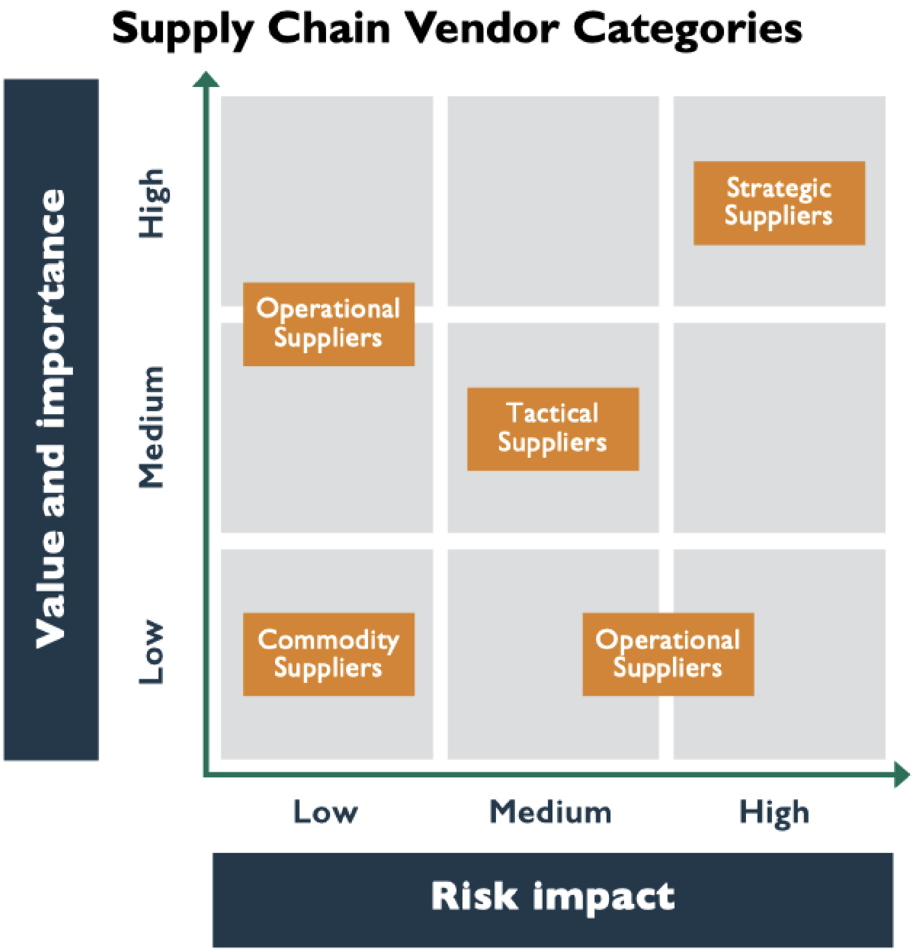
ITIL Components

5 RESTful Architectural Constraints

1. Client-server architecture
2. Uniform interface
3. Cacheable
4. Stateless
5.

Exam Focus Topics:

1. Federation/Federated identities - SSO/SAML/OAuth/LDAP.
2. Third-party vendors know the different types of vendors (Strategic/ Tactical/ Commodity/ Operational).
4. SDLC - What happens at each stage.
5. Concepts of Microsegmentation/Isolation.
6. Forensics in PaaS (where the responsibility of logging is shared).
7. ITIL concepts (problem management/ incident management/ Release and Deploy management)



CCSP Resource List

Books - OSGv2, AIO, CBKv3, Dummies, Cloud Guardians
Practice Exams - AIO, OSG, CCSP IOS Learnzapp
Videos - Mohamed Ahmed - Udemy, Prabh - Youtube, Lecteron, Mike Chapple - Linkedin
CSA Security Guidance, CCSP_Master_Notes_V2, CIRRUS-8000-ft, SecaaS, Alukos, Cromwell, Adam Notes, OWASP, Uptime institute tiers

https://cromwell-intl.com/cybersecurity/isc2-ccsp/

https://cromwell-intl.com/cybersecurity/isc2-ccsp/standards-and-regulations.html