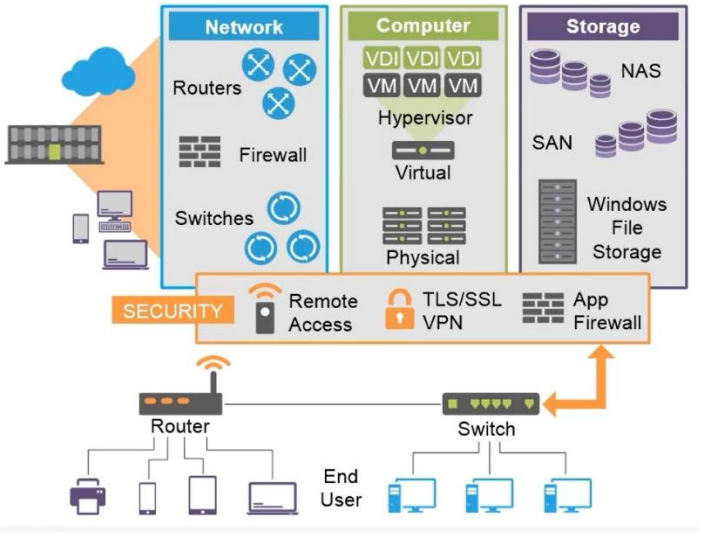
Cloud Infrastructure:

Physical Architecture

- Data centre:
    - Computers
    - Networks
    - Storage Devices
    - Management plane
    - 

- Cont.
    - Multiple data centres:
        - Storage decides can be geographically dispersed
        - CSP deploy replication and failover data centres

Network & Communications

- Network fabric
    - Combination of network components that offer network services
    - Could be wired or wireless
    - Examples:
        - Internet: ISP, Public Wi-Fi, VPN
        - CSP Networks: Wired, Virtual
- Cloud datacentre:
    - Network Architecture
        - Servers
        - Access switches
        - Firewalls
        - Routers
    - Support Devices
        - Load Balancers
        - Intrusion detection devices
    - Management Plane
        - Software Defined Networking (SDN): Software control of network config
            - Used in data centres
            - Moves traffic control from individual device firmware to a centralised and user-managed console (often web interface)
        - Network Function Virtualisation (NFV)

                - Used my service providers (instead of private orgs in their own datacentres)
                - Software control of specific network functionality (e.g. routing)
                - Virtualisation & management of network equipment
                - SDH (Synchronous Digital Hierarchy) could become a component of NFV
        - Virtual Networks
            - Hypervisor
                - Managing Virtual Machines and Virtual Networks

Compute

- Host computers
    - Physical hardware
    - Host computers are the physical hardware devices that host the CSP Virtual Servers (instances)
    - Deployed to support computing capability through virtual machines creation on Hypervisors
        - CPU must support virtualisation
        - Hypervisor selection
        - Memory, storage
        - Host hardware manufacturer data not provided

Virtualisation

- VMS run Hypervisor software
- Host CPU must support VT-x on Intel, AMD-V on AMD processors
- Divides Host Computer resources across VMs
- VMs:
    - Run own OS
    - Can use Virtual Hard Disks
    - Can use physical storage
    - Has assoc config file
    - Utilised segment of host memory
    - Share host I/O and network resources
    - Can run on Virtual Networks (VLANs)

Storage

- Storage associated with VM (temporary)
- Persistent storage (host app data & DB tables. Can be linked with VM instance)
- Archive storage
- Individual CSPs will provide different things
- Storage usually associated with a storage account
- Services:
    - Backup
    - Identity and Access Management (IAM)
    - Disaster Recovery
    - Deduplication

Cloud Risk Management

Cloud Risk Assessment

1. Understand applicable Industry Standards and Guidelines
2. ID & categorise assets
3. Understand risks associated with the cloud platform
4. Investigate and analyse attack surface areas
5. Map data data assets to compliance and security controls
6. Map security requirements against CSP capabilities
7. Define security responsibilities
8. Integrate security mechanisms into the SLA
9. Create and adopt policy and implement solutions
10. Monitor and audit

- Areas of focus:
    - Loss of governance
    - Responsibility ambiguity
    - Isolation failure
    - Vendor lock in
    - Handling of security incidents
    - Visibility
    - Disaster recovery and business continuity
    - Management interface vulnerability
    - Data protection
    - Malicious behaviour at the CSP
    - Insecure or incomplete data deletion

Cloud Infra Risk

- Platform category=specific risks and intra-platform dependency
- Multi-tenancy
- Determine what data assets will be hosted on the cloud service
- Map data and services to security mechanisms
- Define responsibility for protection of data assets and systems
- Service and data availability
- Monitor operations

Threats and Attacks

Security Impact

- Trust boundaries are less clear
- Data asset and application isolation is logical
- Major network backbone is internet
- Application exposure is increased, API vulnerabilities
- Governance of data assets and applications is altered, new disciplines must be implemented and deployed via policy

Attack Vectors

- Physical damage
- Insider threat
- DoS, DDoS
- Impersonation

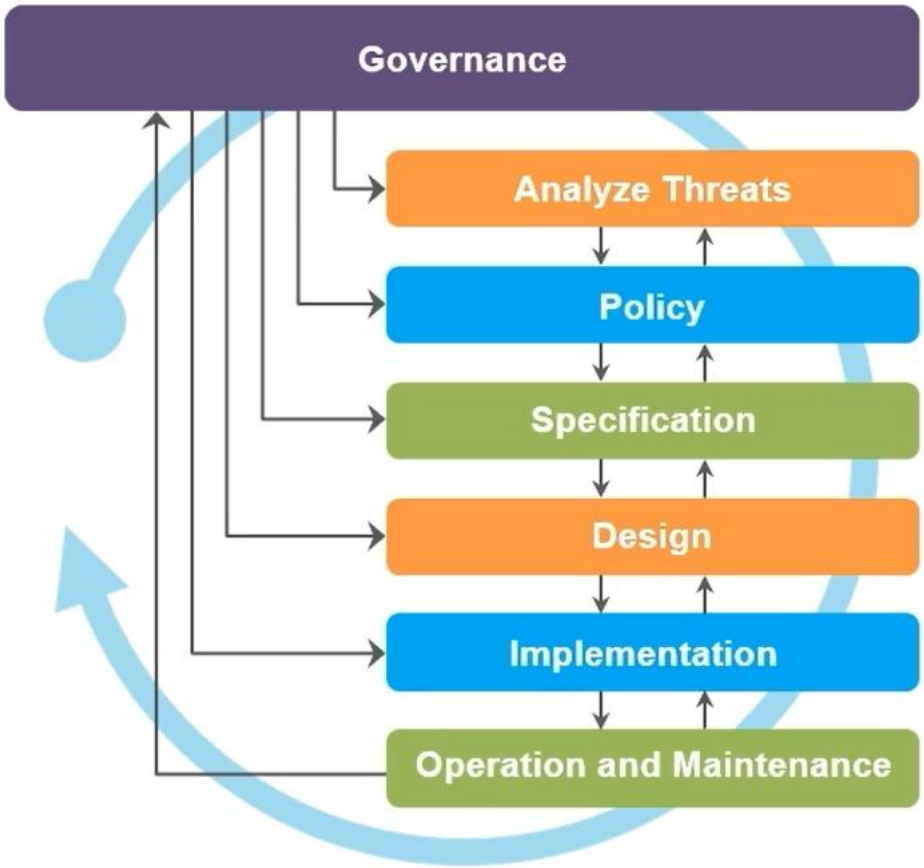
    - Masquerading
    - MitM
    - Replay
    - Authentication theft
    - Key extraction
- Malware

Virtualisation Vulnerabilities

- Virtual Infra
    - Virtual Server protection
    - Hypervisor and guest operation system hardening
    - Virtual Machine Sprawl (proliferation of easily established VMs)
    - VMware developing DLP tools
- Threats to Hypervisor:
    - VM Escape:
        - Rogue VM which managed to subvert access control functions
    - Breaking isolation
        - Breaks boundaries
    - Resource starvation
        - Misconfigured or malicious VMs may starve resources from other VMs by over-consuming
    - Privilege interfaces provided by hypervisor:

Defence and Threat Mitigation

- Risk assessment process



    -

Security Control

Data Centre Protection

- Utility redundancy
    - Electricity, water
    - Comms
    - Redundant air handling and cooling
- Structural design
    - Location
    - Raised floors
    - Physical firewalls
    - Floor to ceiling barriers
    - Minimise window and door access
    - Fire doors should be exit only
- Boundary Protection
- Site Access
- Data centre access
- Personal security

Security Control

- Protecting physical assets:
    - Protection:
        - Multifactor access + role-based acess
        - Deployment of secure KVM
        - Locked equipment racks
        - Monitoring
    - Hardware redundancy measures:
        - Component fault tolerance
        - Failover clusters
        - Centralised and offsite logging
- Visualisation areas of concern:
    - VM encryption
    - VM isolation
    - VM destruction
    - VM image tampering
    - VM migration and movement

Protecting Access

Identification, Authentication and Authorisation

- Cloud Security Issues
    - ID theft
    - Authorisation breaches
- ID Management
    - Password policy, credential protection
    - Check credentials to confirm user/device
- ID Management Systems:
    - Cloud Service Consumer credentials system
    - CSP credentials system
    - Integration of Consumer and Provider Identify Management systems

    - Federation (inter-company trust solution)
    - Single Sign On / Off (SSO)
    - Public / private key management mechanisms
- Managing authorised access:
    - Authorisation: Degree of access to data assets/applications
    - Management of shared data
    - Data asset classification is foundation for:
        - Data asset and application authorisation
        - Data asset and application security controls
        - Digital chain of custody
        - Digital rights management solutions
    - Roles and responsibilities
    - Documents Right management
        - Controlled at document level
        - ACL (Access control List) travels with the document
        - Application of default security authorisation for newly created assets
        - Security breaches on the cloud are more controlled since the CSP does not have access to data assets

Auditing