KORNERSTONE
a TRAINOCATE company

Training. Makes a differece.

Certified Cloud Security Professional, CCSP®

D3 - Cloud Platform & Infrastructure Security

Domain 3 – Cloud Platform and Infrastructure Security

Goal of this domain

- Provide you with knowledge regarding:
  - Both the physical and the virtual components of the cloud infrastructure
  - Risk-management analysis, including tools and techniques for maintaining a secure cloud infrastructure

Goal of this domain

- Provide you with knowledge regarding:
  - How to prepare and maintain business continuity and disaster recovery (BCDR) plans, including techniques and concepts for identifying critical systems and lost data recovery.

Domain Objectives

- Describe both the physical and the virtual infrastructure components as the pertain to a cloud environment
- Define the process for analyzing risk in a cloud infrastructure
- Develop a plan for mitigating risk in a cloud infrastructure based on the risk assessment plan, including countermeasure strategies

Domain Objectives

- Describe disaster recovery (DR) and business continuity management for cloud systems with regard to the environment, business requirements, risk management, and developing and implementing the plan

Introduction

- A typical cloud infrastructure consists of:
  - Physical Data Center Infrastructure
  - Compute Nodes
  - Storage
  - Networking Hardware
  - Virtualization Software
  - Management Software

Introduction

- Physical Environment:
  - High volume of expensive hardware
  - High power densities
  - Enormous and immediate impact of downtime
  - Multiple levels of service, summarized as:
    - Power
    - Pipe
    - Ping

Introduction

- Physical Environment:
  - “Power” and “pipe” limit the density of servers
  - Power densities is expressed in kW / rack
  - 100W / rack were once the norm
  - 10kW or more / rack is common nowadays
  - Require advanced cooling engineering

Introduction

- Physical Environment:
  - Network connectivity / external connectivity
  - Data center providers (colocation) can provide floor space, rack space, and cages (lockable floor space) on any level of aggregation

Introduction

- Physical Environment:
  - Low tolerance for failure
  - Should be evaluated for geographic and political risks (seismic activity, floods, availability of power, and accessibility)

Introduction

- Data Center Design:
  - Revolves around the redundancy in the design
  - Anything that can break down should be replicated
  - No single point of failure should remain

Introduction

- Data Center Design:
  - Backup power
  - Multiple independent cooling units
  - Multiple power lines to individual racks and servers
  - Multiple power distribution units (PDUs)
  - Multiple entrances to the building

Introduction

- Data Center Design:
  - Multiple external entry points for power and network, and so on
  - Geographic distribution of the data centers

Network and Communications in the Cloud

- Purpose of the network:
  - Provide for and control communication between computers; i.e. servers and clients

Network and Communications in the Cloud

- According to National Institute of Standards and Technology (NIST), the following terms are defined:
  - Cloud service consumer: Person or organization that maintains a business relationship with and uses service from the cloud service providers (CSPs)

Network and Communications in the Cloud

- According to National Institute of Standards and Technology (NIST), the following terms are defined:
  - CSP: Person, organizations, or entity responsible for making a service available to service consumers
  - Cloud carrier: The intermediary that provides connectivity and transport of cloud services between CSPs and the cloud service consumers

Network and Communications in the Cloud

- Network Functionality includes:
  - Address allocation
  - Access control
  - Bandwidth allocation
  - Rate limiting
  - Filtering
  - Routing

Network and Communications in the Cloud

- Software-Defined Networking (SDN):
  - Its objective is to provide a clearly defined and separate network control plane to manage network traffic that is separated from the forwarding plane
  - Allows for network control to become directly programmable and distinct from forwarding, allowing for dynamic adjustment of traffic flows

Network and Communications in the Cloud

- Software-Defined Networking (SDN):
  - This is done by *decoupling* or *disassociating* the system that makes decisions about where traffic is sent (the SDN controller, or control plane) from the underlying systems that forward traffic to the selected destination (the data plane)

https://en.wikipedia.org/wiki/Software-defined_networking

Network and Communications in the Cloud

- Hardware Security Module (HSM):
  - A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing
  - HSMs may possess controls that provide tamper evidence such as logging and alerting and tamper resistance such as deleting keys upon tamper detection

https://en.wikipedia.org/wiki/Hardware_security_module

The Compute Parameters of a Cloud Server

- Compute parameters of a cloud server:
  - The number of CPUs
  - The amount of RAM memory

The Compute Parameters of a Cloud Server

- Virtualization:
  - The foundational technology that underlies and makes cloud computing possible
  - Based on the use of powerful host computers to provide a shared resource pool that can be managed to maximize the number of guest operating systems (OS) running on each host

https://en.wikipedia.org/wiki/Virtualization

The Compute Parameters of a Cloud Server

- Virtualization:
  - The key drivers and business cases for using virtualization:
    - Sharing underlying resources to enable a more efficient and agile use of hardware
    - Easier management through reduced personnel resourcing and maintenance

The Compute Parameters of a Cloud Server

- Scalability:
  - The ability to run multiple isolated guest OSs (virtual machines, or VMs) and their associated applications on a single host

The Compute Parameters of a Cloud Server

- The Hypervisor or Virtual Machine Monitor (VMM):
  - A computer software, firmware, or hardware, that creates and runs virtual machines
  - A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine

The Compute Parameters of a Cloud Server

- The Hypervisor or VMM:
  - The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems
  - Multiple instances of a variety of operating systems may share the virtualized hardware resources

The Compute Parameters of a Cloud Server

- The Hypervisor or VMM: (continue)
  - This contrasts with operating-system-level virtualization, where all instances (usually called containers) must share a single kernel, though the guest operating systems can differ in user space
  - The are two types of hypervisors

https://en.wikipedia.org/wiki/Hypervisor

The Compute Parameters of a Cloud Server

- Type 1 hypervisor:
  - Commonly known as a bare metal, embedded, or native hypervisor
  - Works directly on the hardware of the host and can monitor OSs that run above it
  - Is small because its main task is sharing and manging hardware resources between different guest OSs

The Compute Parameters of a Cloud Server

- Type 2 hypervisor:
  - Is installed on top of the host's OS and supports other guest OSs running above it as VMs
  - Is completely dependent on the host OS for its operations

The Compute Parameters of a Cloud Server

- Hypervisor risks and challenges:
  - Security flaws in the hypervisor can lead to malicious software targeting individual VMs running on it or other components in the infrastructure

https://news.cgtn.com/news/3d59544e32417a4d/share_p.html?t=1489821757800

The Compute Parameters of a Cloud Server

- Hypervisor risks and challenges: (continue)
  - A flawed hypervisor can facilitate inter-VM attacks (also known as VM hopping) when isolation between VMs or trust levels have not been configured appropriately; that is, one tenant's VM can peek into the data of another tenant's VM on the same underlying host

http://www.vmware.com/security/advisories/VMSA-2017-0006.html

The Compute Parameters of a Cloud Server

- Hypervisor risks and challenges: (continue)
  - Network traffic between VMs is not necessarily visible to physical network security controls, which means additional security controls may be necessary
  - Resource availability for VMs can be flawed. Individual VMs can be starved of resources

The Compute Parameters of a Cloud Server (continued)

- Hypervisor risks and challenges: (continue)
  - VMs and their disk images are simply files residing somewhere. A stopped VM is potentially accessible on a file system by third parties if no controls are applied. Inspection of this file can circumvent any controls that the gust OS applies

Storage Issues in the Cloud

- Persistent mass storage in cloud computing typically consists od spinning hard disk drives or solid-state drives (SSDs)
- Disk drives are often grouped to provide redundancy. The typical approach is Redundant Array of Inxpensive Disks (RAID)

Storage Issues in the Cloud

- The storage volumes have no file system. The file system structure is applied by the OS on the VM instance to which they are provisioned

Storage Issues in the Cloud

- Object Storage
  - CSP provides a file system-like scheme to its customers
  - Traditionally called object storage, where objects (files) are stored with additional metadata (content type, redundancy required, creation date, and so on)

Storage Issues in the Cloud

- Object Storage (continue)
  - Objects are accessible through APIs and potentially through a web interface
  - Object storage systems store files in a flat organization of containers (bucket in Amazon S3) and use unique ID (keys in S3) to retrieve them

Storage Issues in the Cloud

- Object Storage (continue)
  - Data consistency is achieved only eventually with object storage systems
  - Unsuitable for frequently change data
  - Good solution for data that does not change much; e.g. backups, archives, video and audio files, and VM images

Management Plane

- Object Storage (continue)
  - Allows administrator to remotely manage hosts, as opposed to having to visit each server physically to turn it on or install software on it
  - Key functionally is to create, start, and stop VM instances and provision them with the proper virtual resources; e.g. CPU, memory, storage, and network connectivity

Management Plane

- Object Storage (continue)
  - Typically runs on its own set of servers and has dedicated connectivity to the physical machines under management
  - Integrates authentication, access control, and logging and monitoring of resources used

Management of Cloud Computing Risks

- Cloud computing represents outsourcing, and it becomes part of the IT supply chain
- Cloud risk management should therefore be linked to corporate governance and enterprise risk management

Management of Cloud Computing Risks

- Corporate governance is a broad area describing the relationship between the shareholders and other stakeholders in the organization vs the senior management of the corporation
- Enterprise risk management is the set of process and structure to systematically manage all risks to the enterprise

Management of Cloud Computing Risks

- Risk Assessment and Analysis
  - Policy and Organization Risks
  - General Risks
  - Virtualization Risks
  - Cloud-Specific Risks
  - Legal Risks
  - Non-Cloud-Specific Risks

Management of Cloud Computing Risks

- Policy and Organization Risks (3rd party risk)
  - Provider lock-in
  - Loss of governance
  - Compliance Risks
  - Provider exit

Management of Cloud Computing Risks

- General Risks
  - The consolidation of IT infrastructure leads to consolidation risks, where a single point of failure can have a bigger impact
  - A large-scale platform requires the CSP to bring to bear more technical skills to mange and maintain the infrastructure
  - Control over technical risks shifts toward the provider

Management of Cloud Computing Risks

- Virtualization Risks
  - Guest breakout: Guest OS can access the hypervisor or other guests; presumably facilitated by a hypervisor flaw
  - Snapshot and image security
  - Sprawl: when you lose control of the amount of content on your image store

Management of Cloud Computing Risks

- Cloud-Specific Risks
  - Management plane breach: The most important risk is a management plane breach
  - Resource exhaustion
    - Denial-of-service (DoS) attacks, where a common network or other resource is saturated, leading to starvation of users
    - Traffic analysis
    - Manipulation or interception of data in transit

Management of Cloud Computing Risks

- Cloud-Specific Risks (continue)
  - Isolation control failure
  - Insecure or incomplete data deletion
  - Control conflict risk
  - Software-related risks: The ultimate accountability for compliance still falls into the customer

Management of Cloud Computing Risks

- Legal Risks
  - Data protection: Cloud customers may have legal requirements about the way that they protect data – in particular PII. The controls and actions of the CSP may not be sufficient
  - Jurisdiction: CSPs may have data storage locations in multiple jurisdictions, which can affect other risks and their controls

Management of Cloud Computing Risks

- Legal Risks
  - Law enforcement
  - Licensing

Management of Cloud Computing Risks

- Non-Cloud-Specific Risks
  - Natural disasters
  - Unauthorized facility access
  - Social engineering
  - Network attacks on the consumer and provider
  - Default passwords
  - Other malicious or non-malicious actions

Management of Cloud Computing Risks

- Cloud Attack Vectors
  - Guest breakout
  - Identity compromise, either technical or social; e.g. through employees of the provider
  - API compromise, such as by leaking API credentials
  - Attacks on the provider's infrastructure and facilities

Management of Cloud Computing Risks

- Cloud Attack Vectors (continue)
  - Attacks on the connecting infrastructure (cloud carrier)

Countermeasure Strategies across the Cloud

- Highly recommended to implement multiple layers of defense against any risk
- For a control that directly addresses a risk, there should be an additional control to catch the failure of the first control. These controls are referred to as compensating controls

Countermeasure Strategies across the Cloud

- Four criteria of compensating control
  - Have the intent and rigor of the original requirement
  - Provide a similar level of defense as the original requirement
  - Be above and beyond other requirements
  - Be commensurate with the additional risk imposed by not adhering to th requirement

Countermeasure Strategies across the Cloud

- Continuous Uptime
  - It implies that every component is redundant. This serves two purposes:
    - It makes the infrastructure resilient against component failure
    - It allows individual components to be updated without affecting the cloud infrastructure uptime

Countermeasure Strategies across the Cloud

- Automation of Controls
  - Controls should be automated as much as possible, thus ensuring their immediate and comprehensive implementation. E.g. integrate software into the build process of VM images that detects malware, encrypts data, configures log files, and registers new machines into configuration management database

Countermeasure Strategies across the Cloud

- Access Controls
  - Depending on the service and deployment models, the responsibility and actual execution of the control can lie with the cloud service consumer, with the CSP, or both
  - Cloud services should deploy a user-centric approach for effective access control, in which every user request is bundled with the user identity

Countermeasure Strategies across the Cloud

- Examples of access controls
  - Building access
  - Computer floor access
  - Cage or rack access
  - Access to physical servers (hosts)
  - Hypervisor access (API or management plane)
  - Guest OS access (VMs)
  - Developer access

Countermeasure Strategies across the Cloud

- Examples of access controls (continue)
  - Customer access
  - Database access rights
  - Vendor access
  - Remote access
  - Application and software access to data (SaaS)

Physical and Environmental Protections

- It consist of the data center, its buildings, and surroundings
- Facilities and its staff are most relevant, not just for the security of the IT assets but because they are the focus of a lot of security controls on other components

Physical and Environmental Protections

- Infrastructure outside the data center that needs protecting:
  - Network and communication facilities
  - Endpoints such as PCs, laptops, mobile phones, and other smart devices

NIST's SP800-14 and SP800-123

Physical and Environmental Protections

- Key Regulations applicable to CSP facility:
  - Health care Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Scurity Standard (PCI DSS)
  - North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

Physical and Environmental Protections

- Examples of Controls:
  - Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas
  - Physical access to information assets and functions by users and support personnel shall be restricted

Physical and Environmental Protections

- Examples of Controls: (continue)
  - Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems

Physical and Environmental Protections

- Protecting Data Center Facilities:
  - Require multiple layers of access controls
  - Controls are implemented that deter, detect, delay, and deny unauthorized access between different security zones
  - Key resources and assets should be made redundant, preferably in independent ways such as multiple electricity feeds, network cables, cooling systems, and UPSs

Physical and Environmental Protections

- Protecting Data Center Facilities: (continue)
  - On the computer floor, redundancy continues in power and network cabling to racks
  - Data center and facility staff represent a risk
    - Extensive background checks and screening
    - Adequate and continuous training in security awareness and incident response capability

System and Communication Protections

- All these components run software that needs to be properly configured, maintained and analysed for risk.
- When these components have security functions, such as virus scanners and network intrusion detection systems (IDSs) and network intrusion prevention systems (IPSs), these need to be virtualization aware

System and Communication Protections

- Here is a non-exhaustive list of services:
  - Hypervisor
  - Storage controllers
  - Volume management
  - IP address management (DHCP)
  - Security group management
  - VM image service

System and Communication Protections

- Here is a non-exhaustive list of services: (continue)
  - Identity service
  - Message queue
  - Management database
  - Guest OS protection

System and Communication Protections

- Automation of Configuration
  - Manually configuring all the infrastructure components in a system can be a tedious, expensive, error-prone, and insecure process
  - Automation of configuration and deployment is essential to make sure that components implement all relevant controls

System and Communication Protections

- Automation of Configuration (continue)
  - Automations also allows for a more granular proliferation of controls

- Case Studies
  - AWS outage 2017
  - AWS S3 outage root cause
  - Lesson learned

Responsibilities of Protecting the Cloud System

- Implementation of controls requires cooperation and a clear demarcation of responsibility between CSP and the cloud service customer
- It is important to understand where responsibility is placed and what level of responsibility the organization is expected to undertake regarding the use of cloud services

Following the Data Lifecycle

- Following the data across its lifecycle is an important approach in ensuring sufficient coverage of controls
- Data lifecycle is in three broad categories:
  - Data at Rest (DAR)
  - Data in Motion (DIM)
  - Data in Use (DIU)

Following the Data Lifecycle

- Data at Rest (DAR):
  - In storage, the primary control against unauthorized access is encryption, which helps to ensure confidentiality
  - Availability and integrity are controlled through the use of redundant storage across multiple locations

Following the Data Lifecycle

- Data in Motion (DIM):
  - Network get segregated into multiple zone physically and logically through technology such as VLANs; can result in traffic separation acts as a control to improve DIM confidentiality and integrity
  - A countermeasure against availability and capacity risks caused by resource contention

Following the Data Lifecycle

- Data in Motion (DIM): (continue)
  - Traffic separation is often mandated from a compliance perspective
  - Encryption is also a control to consider, and it provides for data confidentiality

Following the Data Lifecycle

- Data in Motion (DIM): (continue)
  - Network components are a potential area for controls:
    - Firewall acting as the gatekeeper on the single perimeter is an outdated thought process in cloud architectures
    - Control is possible between demarcated network zones
      - Data loss prevention (DLP)
      - Data activity monitoring, and egress filtering

Following the Data Lifecycle

- Data in Use (DIU):
  - Requires granular access control for data at risk
  - APIs should be protected through the use of digital signatures and encryption
  - Access rights should be restricted to the roles of the consumer

Virtualization Systems Controls

- Virtualization components (compute, storage, and network), all governed by the management plane; they are a prime source of cloud-specific risks and compensating controls

Virtualization Systems Controls

- Management plane is a prime resource to protect:
  - Highest risk components with respect to software vulnerabilities because it affect tenant isolation
  - GUI, CLI, and APIs all need to have stringent and role-based access controls (RBACs) applied

Virtualization Systems Controls

- Management plane is a prime resource to protect: (Continue)
  - Logging all relevant actions
    - Machine image changes, configuration changes, and management access logging
  - Isolate the management network with respect to other networks (storage, tenant, and so on); might need to be a separate physical network to meet regulatory and compliance requirements

Virtualization Systems Controls

- Insufficient controls implemented by virtualization components could be compensated by employing trust zones to segregate the physical infrastructure
  - Address confidentiality risks and control availability and capacity risks
  - Often required by certain regulations

Managing Identification, Authentication, and Authorization

- Anything (users, devices, code, organizations, and agents) in cloud computing that needs to be trusted has an identity
- Distinguishing characteristic of an identity in cloud computing is that it can be federated across multiple collaborating parties

Managing Identification, Authentication, and Authorization

- It implies a split between “identity providers” and “relying parties”, who rely on identities to be issued by the providers
- This leads to a model whereby:
  - An identity provider can service multiple relying parties
  - A relying party can federate multiple identity providers

Managing Identification, Authentication, and Authorization

- In the public cloud world, identity providers are increasingly adopting OpenID and OAuth as standard protocols
- In a corporate environment, corporate identity repositories can be used; e.g. Microsoft Active Directory and LDAP

Managing Identification, Authentication, and Authorization

- Relevant standard protocols in the corporate world are:
  - Security Assertion Markup Language (SAML)
  - WS-Federation

Managing Identification, Authentication, and Authorization

- Managing Authentication
  - Authentication is the process of establishing with adequate certainty the identity of an entity
  - Authentication is a function of the identity provider that is done through factors such as passwords, key generators, and biometrics
  - Multifactor authentication is often advised for high-risk roles such as administrative functions

Managing Identification, Authentication, and Authorization

- Managing Authorization
  - Authorization is the process of granting access to resources
  - Authorization can be based on identities, attributes of identities such as roles, and contextual information such as location and time of day

Managing Identification, Authentication, and Authorization

- Managing Authorization (continue)
  - Authorization is enforced near the relevant resource, at the policy enforcement point
  - In a federated identity model, this is typically at the relying party

Managing Identification, Authentication, and Authorization

- Accounting for Resources
  - Accounting measures the resources a user consumes during access. E.g. amount of system time or the amount of data a user has send or received during a session
  - Its carried out by logging session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities

Managing Identification, Authentication, and Authorization

- Managing Identity and Access Management
  - Identity management is the entire process of registering, provisioning, and de-provising identities for all relevant entities and their attributes, while making that information available to the proper audit

Managing Identification, Authentication, and Authorization

- Managing Identity and Access Management (continue)
  - Access management includes managing the identities' access rights
  - Access management is where the real decisions are made
  - It is more important to control access rights than it is to control the number of identities

Managing Identification, Authentication, and Authorization

- Making Access Decisions
  - Can a device be allowed to receive an IP address on the local network?
  - Can a webserver communicate with a particular database server?
  - Can a user access a certain application, a function within an application, or data within an application?

Managing Identification, Authentication, and Authorization

- Making Access Decisions (continue)
  - Can an application access data from another application?
- These access right might be very detailed, down to the individual row of a database

Managing Identification, Authentication, and Authorization

- Making Access Decisions (continue)
  - Access decisions can be enforced at various points with various technologies
  - These are called policy enforcement points (PEPs)
  - The individual policies are controlled at the policy decision point (PDP) and communicated via standard protocols

Managing Identification, Authentication, and Authorization

- Entitlement Process
  - The entitlement process starts with business and security requirements and translates these into a set of rules
  - This rule represents a risk decision; it's a balance between enabling users to be productive while reducing abuse potential

Managing Identification, Authentication, and Authorization

- Entitlement Process (continue)
  - This rule refers to a number of attributes of entities (user account, user role, user device, and device network connection)
  - These rules are then translated into component authorization decisions to be enforced at the PEPs

Managing Identification, Authentication, and Authorization

- The Access Control Decision-Making Process

Risk Audit Mechanisms

- The purpose of a risk audit is to provide reasonable assurance that adequate risk controls exist and are operationally effective
- Reasons for conducting audits:
  - Regulatory or compliance related
  - (internal) audits are employed as part of a quality system
  - Demonstration of quality

Risk Audit Mechanisms

- The Cloud Security Alliance Cloud Controls Matrix
  - In the cloud computing world, it serves as a framework to enable cooperation between cloud service consumers and CSPs on demonstrating adequate risk management

Risk Audit Mechanisms

- The Cloud Security Alliance Cloud Controls Matrix (continue)
  - An essential component of audits is evidence that controls are actually operational
  - This evidence includes management structures, configurations, configuration files and policies, activity reports, log files, and so on.
  - Gathering evidence can be a costly effort

Risk Audit Mechanisms

- Cloud Computing Audit Characteristics
  - Cloud infrastructure is often located at a hosting facility, which is a dependency; issues at that facility can affect the cloud infrastructure
  - Individual tenants may not be in a position to physically inspect and audit data centers

Risk Audit Mechanisms

- Cloud Computing Audit Characteristics (Continue)
  - Cloud computing can improve transparency and assurance if the essential cloud characteristics are being exploited properly
  - The use of contractual agreements such as hosting agreements and service-level agreements (SLA) distributes responsibility and risk among both CSPs and cloud consumers

Risk Audit Mechanisms

- Using a VM
  - Service automation can be instrumental in automatically generating evidence. E.g., a VM image can be built according to a specified configuration. This configuration baseline and th logs of the build process then provide evidence that all instances of this VM will implement adequate controls

Risk Audit Mechanisms

- Using a VM (continue)
  - Controls that can be built in a VM image include an automated vulnerability scan on system start, an automatic registration in a configuration management database, and an asset management system.

Risk Audit Mechanisms

- Using a VM (continue)
  - The configuration might imply any number of management and control agents, such as VM-level firewalls, DLP agents, and automated log file generation.
  - All this can lead to the automatic generation of evidence

Risk Audit Mechanisms

- Using a VM (continue)
  - Cloud computing's automation and self-service provisioning can be progressed to lead demonstrated on a continuous and near real-time basis

Understanding the Cloud Environment related to BCDR

- The business continuity plan (BCP) allows a business to plan what it needs to do to ensure that its key products and services continue to be delivered in case of a disaster
- The disaster recovery plan (DRP) allows a business to plan what needs to be done immediately after a disaster to recover from the event

Understanding the Cloud Environment related to BCDR

- Different scenarios in which you might want to consider BCDR:
  - On-Premises, Cloud as BCDR
  - Cloud Service Consumer, Primary Provider BCDR
  - Cloud Service Consumer, Alternative Provider BCDR

Understanding the Cloud Environment related to BCDR

- On- Premises, Cloud as BCDR:
  - Existing on-premises infrastructure
  - Consider the provider of alternative facilities should a disaster strike the on-premises infrastructure
  - The “traditional” failover conversation that IT has been engaged in since before the advent of cloud

Understanding the Cloud Environment related to BCDR

- On- Premises, Cloud as BCDR: (continue)
  - The only difference is that the cloud is now being introduced as the endpoint for failover services and BCDR activities

Understanding the Cloud Environment related to BCDR

- Cloud Service Consumer , Primary Provider BCDR:
  - The infrastructure under consideration is already at a CSP
  - The risk being considered is potential failure of part of the CSP's infrastructure
  - The business continuity strategy then focuses on restoration of service or failover to another part of the sam CSP infrastructure

Understanding the Cloud Environment related to BCDR

- Cloud Service Consumer , Alternative Provider BCDR:
  - Somewhat like the 2nd scenario, but instead of restoration of service to the same provider, the service has to be restored to a different provider
  - This address the risk of complete CSP failure
  - DR almost by definition requires replication. The key difference between these scenarios is where the replication happens

Understanding the Cloud Environment related to BCDR

- BCDR Planning Factors
  - Information relevant in BCDR planning includes the following:
    - The important assets: data and processing
    - The current locations of these assets
    - The networks between the assets and the sites of their processing
    - Actual and potential location of workforce and business partners in relation to the disaster event

Understanding the Cloud Environment related to BCDR

- Relevant Cloud Infrastructure
  - Cloud Infrastructure has a number of characteristics that can be distinct advantages in realizing BCDR:
    - Rapid elasticity and on-demand self-service lead to flexible infrastructure that can be quickly deployed to execute an actual DR without hitting unexpected ceilings
    - Broad network connectivity, which reduces operational risk

Understanding the Cloud Environment related to BCDR

- Relevant Cloud Infrastructure (continue)
  - Cloud Infrastructure has a number of characteristics that can be distinct advantages in realizing BCDR: (continue)
    - Cloud infrastructure providers have resilient infrastructure, and an external BCDR provider has the potential for being experienced and capable because the provider's technical and people resources are being shared across a number of tenants

Understanding the Cloud Environment related to BCDR

- Relevant Cloud Infrastructure (continue)
  - Cloud Infrastructure has a number of characteristics that can be distinct advantages in realizing BCDR: (continue)
    - Pay-per-use can mean that the total BCDR strategy can be a lot cheaper than alternative solutions. During normal operation, the BCDR solution is likely to have a low cost

Understanding the Business Requirements related to BCDR

- Vocabulary Review:
  - The **recovery point objective** (PRO) helps determine how much information must be recovered and restored. Or ask yourself, “how much data can the company afford to lose?”
  - The **recovery time objective** (RTO) is a time measure of how fast you need each systm to be up and running in the event of a disaster or critical failure

Understanding the Business Requirements related to BCDR

- Vocabulary Review: (continue)
  - The **recovery service level** (RSL) is a percentage measurement (0 – 100%) of how much computing power is necessary based on the percentage of the production system needed during a diaster

Understanding the Business Requirements related to BCDR

- Business requirements that are specific to BCDR:
  - BCDR protects against the risk of data not being available and the risk that the business processes that it supports are not functional, leading to adverse consequences for the organization

Understanding the Business Requirements related to BCDR

- Business requirements that are specific to BCDR: (continue)
  - A modern, cloud-centric view of BCDR is that, it is not an activity to be performed after the application and system architecture are developed. Instead, it should lead to requirements that are to be used as inputs to the design and selection of the information systm

Understanding the Business Requirements related to BCDR

- Questions to be answered before development of cloud BCDR:
  - Is the data sufficiently valuable for additional BCDR strategies?
  - What is the required PRO; i.e., what data loss would be tolerable?
  - What is the required RTO; i.e., what unavailability of business functionality is tolerable?

Understanding the Business Requirements related to BCDR

- Questions to be answered before development of cloud BCDR: (continue)
  - What kinds of “disasters” are included in th analysis?
  - Does that include provider failure?
  - What is the necessary RSL for the systems covered by the plan?

Understanding the Business Requirements related to BCDR

- Both **RRO** and the **RTO** requirements could be zero. In practice, iteration from requirements is occurring for an optimal balance between loss prevention and its cost

Understanding the Business Requirements related to BCDR

- Geographically separating resources for the purpose of BCDR can result in a reduction of, say flooding or earthquake risk. Counter balancing this is the fact that every CSP is subject to local laws and regulations based on geographic location

Understanding the Business Requirements related to BCDR

- How BCDR can differ in a cloud environment from the traditional approaches that exist in noncloudy environments?
  - In a virtualized environment, the use of snapshots can offer a bare-metal restoration option that can be deployed extremely quickly

Understanding the BCDR Risks

- Categories of risks to consider in the context of BCDR:
  - Risks threatening the assets and support infrastructure that the BCDR plan is protecting against
  - Risks that threaten the successful execution of a BCDR plan invocation

Understanding the BCDR Risks

- BCDR Risks Requiring Protection:
  - Damage from natural causes, disasters and deliberate attacks
  - Wear and tear of equipment
  - Availability of qualified staff
  - Utility service outages; e.g. power failures
  - Failure of a provider to deliver services; e.g. bankruptcy, taken over, change of business plan

Understanding the BCDR Risks

- BCDR Strategy Risks:
  - BCDR strategy typically involves a redundant architecture, or failover tactic
  - BCDR strategies still have common failure modes; e.g. multizone architectures are still vulnerable to region failures
  - DR site is likely to be geographically remote from any primary sites. (Performance Issue)

Understanding the BCDR Risks

- BCDR Strategy Risks: (continue)
  - Regulatory compliance concerns if the DR site is in a different jurisdiction

Understanding the BCDR Risks

- Potential Concerns about the BCDR Scenarios
  - Existing on premise solution, using cloud as BCDR:
    - The functional and resource capabilities that need to be available for speedy DR
    - E.g. workloads on physical machines may need to be converted to work loads in a virtual environment

Understanding the BCDR Risks

- Potential Concerns about the BCDR Scenarios (continue)
  - Existing cloud service consumer, evaluating their cloud service provider's BCDR:
    - Re-evaluation of the provider's capabilities is necessary because the BCDR strategy is likely to require new resources and functionality
    - E.g. load-balancing functionality and available bandwidth between the redundant facilities of the CSP

Understanding the BCDR Risks

- Potential Concerns about the BCDR Scenarios (continue)
  - Existing cloud service consumer, evaluating alternative CSP as BCDR:
    - Similar to the selection of a new provider
    - The speediness with which the move to the new provider can be made should be a primary concern
    - Worthwhile to involve the business users as soon as possible so that they can make an assessment of the residual risks directly to the business

BCDR Strategies

- Common components to the previous three scenarios
  - Location
  - Data Replication
  - Functionally Replication
  - Event Anticipation
  - Failover Event
  - Return to Normal

BCDR Strategies

- Location
  - BCDR strategy address the loss of important assets, replication of those assets across multiple locations is more or less assumed
  - The relevant locations to be considered depend on the geographic scale of the calamity anticipated
    - Power or network failure
    - Flooding, fire, and earthquakes

BCDR Strategies

- Location (continue)
  - Switching to a different cloud service provider
    - Unique to the cloud model
    - Use of a memo of understanding, along with SLAs to regulate and guide a switch, should be thought out ahead of time and put in place prior to a switch taking place

BCDR Strategies

- Data Replication
  - It is about maintaining a more-or-less up-to-date copy of the data on a different location
  - It can be done on a number of technical levels and with different granularity
    - Block level, file level, and the database level
  - It can be in bulk, on the byte level, by file synchronization, database mirroring, daily copies

BCDR Strategies

- Data Replication (continue)
  - Each of these levels allows the mitigation of certain risks, but not all risks
    - Block-level data replication protects against physical data loss but not against database corruption
    - It does not necessarily permit recovery to a different software solution that requires different data formats

BCDR Strategies

- Data Replication (continue)
  - Backup and archive are traditionally used for snapshot functionality
    - Mitigate risks related to accidental file deletion and database corruption

BCDR Strategies

- Data Replication (continue)
  - Beyond replication, there exist an opportunity to rearchitect the application so that relevant data sets are moved to a different provider
    - Makes the data more resilient in case of power failure
    - Examples of components to split off include;
      - Database as a service (DBaaS)
      - Remote storage of log files

BCDR Strategies

- Functionality Replication
  - It is about re-creating the processing capacity on a different location
    - Could be as simple as selecting an additional deployment zone or as involved as performing an extensive rearchitecting
    - In SaaS case, this replication of functionality might even involve selecting a new provider with a different offering, implying a substantial impact on the users of the service

BCDR Strategies

- Planning, Preparing, and Provisioning
  - About the tooling, functionality, and processes that lead up to the actual DR failover response
  - The most important component is adequate monitoring, where more time is often available ahead of the required failover event
  - The sooner anomalies are detected, the easier it is to attain an RTO

BCDR Strategies

- Failover Capability
  - It requires some form of load balancer to redirect user service requests to the appropriate services
  - It can take the technical form of cluster managers, load balancer devices, or domain name system (DNS) manipulation

BCDR Strategies

- Return to Normal
  - It is where DR ends. In case of a temporary failover, the return to normal would be back to the original provider (or in-house infrastructure, as the case may be)
  - Alternatively, the original provider may no longer be a viable option, in which case the DR provider becomes the “new normal”

Creating the BCDR Plan

- When organizations are incorporating IT systems and cloud solutions on an ongoing basis, creating and re-evalusting BCDR plans should be a defined and documented process

Creating the BCDR Plan

- Scope of the BCDR Plan
  - The BCDR plan and its implementation are embedded in an information security strategy, which encompasses:
    - Clearly defined roles
    - Risk assessment
    - Classification
    - Policy
    - Awareness and training

Creating the BCDR Plan

- Gathering Requirements and Context
  - Requirements that are input for BCDR:
    - Identification of critical business process and their dependence on specific data and services
    - A list of risks and threats that can negatively affect any important business processes
    - Business strategy influences the acceptable RTO and PRO values

Creating the BCDR Plan

- Gathering Requirements and Context
  - Requirements that are input for BCDR:
    - Company internal policies and procedures
    - Applicable legal, statutory, or regulatory compliance obligations

Creating the BCDR Plan

- Analysis of the Plan
  - Purpose of the analysis phase:
    - Translate BCDR requirements into input to be used in the design phase
    - The most important inputs for the design phase are scope, requirements, budget, and performance objectives

Creating the BCDR Plan

- Analysis of the Plan (continue)
  - Business requirements and the threat model should be analysed for completeness and consistency and then translated into an identification of the assets at risks
  - With that, requirements on resources needs for mitigating those risks can be made.

Creating the BCDR Plan

- Analysis of the Plan (continue)
  - This includes the identification of all dependencies, including processes, applications, business partners, and third-party service providers

Creating the BCDR Plan

- Risk Assessment
  - BCDR solutions should be assessed for residual risks
  - All scenarios involve evaluation of the CSP's capability to deliver. The typical challenges include:
    - Elasticity of the cloud provider
      - Can the CSP provide all the resources if BCDR is involved?

Creating the BCDR Plan

- Risk Assessment (continue)
  - The typical challenges include: (continue)
    - Contractual issues
      - Will any new CSP address all contractual issues and \SLA requirements?
    - Available network bandwidth for timely replication of data
    - Available bandwidth between the impacted user base and the BCDR locations

Creating the BCDR Plan

- Risk Assessment (continue)
  - The typical challenges include: (continue)
    - Legal and licensing risks
      - There may be legal or licensing constraints that prohibit the data or functionality to be present in the backup location

Creating the BCDR Plan

- Plan Design
  - The objective is to establish and evaluate candidate architecture solutions
  - It should not just result in technical alternatives but also flesh out procedures and workflow
  - The BCDR solution should have a clear owner:
    - With a clear role and mandate in the organization
    - Who is accountable for the correct setup and maintenance of the BCDR capability

Creating the BCDR Plan

- Plan Design (continue)
  - BCDR-specific questions that should be addressed in the design phase:
    - How will the BCDR solution be invoked?
    - What is the manual or automated procedure for invoking the failover services?
    - How will the business use of the service be affected during the failover, if at all?
    - How will the BCDR be tested?

Creating the BCDR Plan

- Other Plan Considerations
  - Once the BCDR is ready, work will start on implementing the solution
  - On the primary platform, these activities include:
    - Implementation of functionality for enabling data replication on a regular or continuous schedule
    - Functionality to automatically monitor for any contingency that might arise a failover event

Creating the BCDR Plan

- Other Plan Considerations (continue)
  - On the DR platform, these activities include:
    - The required infrastructure and services need to be built up and brought into trial production mode
  - The DR platform tracks any relevant changes and functional updates that are being made on the primary platform
  - Include all DR-related infrastructure and services in the regular IT service management

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan
  - Test all parts of the plan to validate that it would work in a real event
  - Testing policy should include enterprise-wide testing strategies that establish expectations for individual business lines
  - Business lines include all internal and external supporting functions

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - The testing strategy should include:
    - Expectations for business lines and support functions to demonstrate the achievement of business continuity test objectives consistent with the business impact analysis (BIA) and risk assessment
    - A description of the depth and breadth of testing to be accomplished

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - The testing strategy should include: (continue)
    - The involvement of staff, technology, and facilities
    - Expectations for testing internal and external interdependencies
    - An evaluation of the reasonableness of assumptions used in developing the testing strategy

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - Testing strategies should include the testing scope and objectives:
    - Clearly define which functions, systems, or processes are going to be tested
    - What will constitute a successful test

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - The testing objectives should:
    - Ensure that the business continuity planning (BCP) process is accurate, relevant, and viable under adverse conditions

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - Testing should include applications and business functions that were identified during the BIA
  - The BIA determines the RPOs and RTOs, which then help determine the recovery strategy
  - Validation of the PROs and RTOs is important to ensure that they are attainable

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - At a minimum, the testing scope and objectives should do the following:
    - Ensure support for normal business operations
    - Gradually increase the complexity, level of participation, functions, and physical locations involved

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - At a minimum, the testing scope and objectives should do the following: (continue)
    - Demonstrate a variety of management and response proficiencies under simulated crisis conditions, progressively involving more resources and participants
    - Uncover inadequacies so that testing procedures can be revised

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - At a minimum, the testing scope and objectives should do the following: (continue)
    - Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services
    - Involve a sufficient volume of all types of transactions to ensure adequate capacity and functionality of the recovery facility

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - Test plans should clearly communicate the predefined test scope and objectives and give participants relevant information, such as:
    - A master test schedule that encompasses all test objectives
    - Specific descriptions of test objectives and methods
    - Roles and responsibilities for all test participants, including support staff

Creating the BCDR Plan

- Planning, Exercising, Assessing, and Maintaining the Plan (continue)
  - relevant information, such as: (continue)
    - Designation of test participants
    - Test decision makers and succession plans
    - Test locations
    - Test escalation conditions and test contact information

Creating the BCDR Plan

- Test Plan Review
  - Testing plan should be revised to account for:
    - Any changes to key personnel
    - Policies and procedures
    - Facilities and equipment
    - Outsourcing relationships
    - Vendors
    - Other components that affect a critical business function

Creating the BCDR Plan

- Testing methods include both business recovery and DR exercise
  - Business recovery exercises primarily focus on testing business line operations
  - DR exercises focus testing the continuity of technology components, including systems, networks, applications, and data

Creating the BCDR Plan

- A comprehensive test should involve processing a full day's work at peak volumes to ensure that equipment capacity is available and that RTOs and RPOs can be achieved
- The most common types of exercise are call exercises, walk-through exercises, simulated or actual exercises, and compact exercises

Creating the BCDR Plan

- Tabletop Exercise / Structured Walk-Through Test
  - A preliminary one in the overall testing process
  - May be used as an effective training tool
  - It is not a preferred testing method
  - Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP and that the plan accurately reflects the organization's ability to recover from a disaster

Creating the BCDR Plan

- Tabletop Exercise / Structured Walk-Through Test (continue)
  - This exercise / test is characterized by:
    - Attendance of business unit management representatives and employees who play a critical role in the BCP process
    - Discussion about each person's responsibilities as defined by the BCP

Creating the BCDR Plan

- Tabletop Exercise / Structured Walk-Through Test (continue)
  - This exercise / test is characterized by: (continue)
    - Individual and team training, which includes a walk-through of the step-by-step procedures outlined in the BCP
    - Clarification and highlighting of critical plan elements, as well as problems noted during testing

Creating the BCDR Plan

- Walk-Through Drill / Simulation Test
  - It is somewhat more involved than a tabletop exercise / structured walk-through test
  - The participants choose a specific event scenario and apply the BCP to it

Creating the BCDR Plan

- Walk-Through Drill / Simulation Test
  - A walk-through drill / simulation test includes:
    - Attendance by all operational and support personnel who are responsible for implementing the BCP procedures
    - Practice and validation of specific functional response capabilities
    - Focus on the demonstration of knowledge and skills, as well as team interaction and decision-making capabilities

Creating the BCDR Plan

- Walk-Through Drill / Simulation Test
  - A walk-through drill / simulation test includes:
    - Role playing with simulated response at alternate locations to act out critical steps, recognize difficulties, and resolve problems in a nonthreatening environment
    - Mobilization of all or some of the crisis management and response team to practice proper coordination without performing actual recovery processing

Creating the BCDR Plan

- Walk-Through Drill / Simulation Test
  - A walk-through drill / simulation test includes:
    - Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan

Creating the BCDR Plan

- Functional Drill / Parallel Test
  - It is the first type that involves the actual mobilization of personnel to other sites in an attempt to establish communications and perform actual recovery processing as set forth in the BCP
  - To determine whether critical systems can be recovered at the alternate processing site and if employees can actually deploy the procedures defined in the BCP

Creating the BCDR Plan

- Functional Drill / Parallel Test (continue)
  - It encompasses:
    - A full test of the BCP, which involves all employees
    - Demonstrate of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning
    - Testing medical response and warning procedures

Creating the BCDR Plan

- Functional Drill / Parallel Test (continue)
  - It encompasses: (continue)
    - Response(s) to alternate locations or facilities using actual communications capabilities
    - Mobilization of personnel and resources at varied geographical sites, including evacuation drills in which employees test the evacuation route and procedures for personnel accountability

Creating the BCDR Plan

- Functional Drill / Parallel Test (continue)
  - It encompasses: (continue)
    - Varying degrees of actual, as opposed to simulated, notification and resource mobilization in which parallel processing is performed and transactions are compared to production results

Creating the BCDR Plan

- Full-Interruption / Full-Scale Test
  - It is the most comprehensive type of test
  - A real-life emergency is simulated as closely as possible
  - Comprehensive planning should be a prerequisite to this type of test
  - Implements all or portions of its BCP by processing data and transactions using backup media at the recovery site

Creating the BCDR Plan

- Full-Interruption / Full-Scale Test
  - The test involves:
    - Enterprise-wide participation and interaction of internal and external management response teams with full involvement of external organizations
    - Validation of crisis response functions
    - Demonstration of knowledge and skills as well as management response and decision-making capability

Creating the BCDR Plan

- Full-Interruption / Full-Scale Test
  - The test involves: (continue)
    - On-the-scene execution of coordination and decision-making roles
    - Actual, as opposed to simulated, notifications, mobilization of resources and communication of decisions
    - Activities conducted at actual response locations or facilities

Creating the BCDR Plan

- Full-Interruption / Full-Scale Test
  - The test involves: (continue)
    - Actual processing of data using backup media
    - Exercise generally extending over a longer period of time to allow issues to fully evolve as they would in a crisis and to allow realistic role-playing of all the involved groups

Creating the BCDR Plan

- Full-Interruption / Full-Scale Test
  - After every exercise, the results need to be published and action items identified to address the issues that were uncovered
  - Action items should be tracked until they have been resolved, and where appropriate, the plan should be updated

Creating the BCDR Plan

- Testing and Acceptance to Production
  - Ideally, a test realizes a full switchover to the DR platform
  - IT should be recognized that this test does represent a risk to the production user population