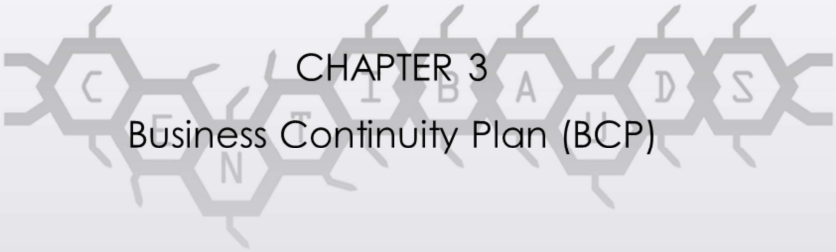
CISSP

Aitizaz Uddin Syed (M.Engg, CISSP, CISSP-ISSAP, CCSP, CRISC, GICSP, TOGAF)

Domain 1
Security and Risk Management

Domain 7
Security Operations



CHAPTER 3

Business Continuity Plan (BCP)

Differences between BCP and Disaster Recovery Planning (DRP)

- BCP tends towards strategic governance and processes (commercial)
- DRP tends towards the tactical, operational and technical aspect such as backup, remote site, and fault tolerance
- DR can be regarded as subset of BCP
- BCP focuses on resilience and system tolerance avoiding disruption while DRP achieves returning business as usual to previous stable state
- In both cases availability is the key

Four stages of BCP

1) Project Scope and planning [Business Organization Analysis, BCP team selection, Resource requirement (Financial and Human), External dependencies]

2) Business Impact Assessment [Prioritize Assets, Quantitative/Qualitative risk assessment, Re-organize based on priority]

3) Continuity Planning [Strategy Development, Provision & Process]

4) Plan Approval and Implementation

1) Project Scope and planning

1.1) Business Organization Analysis (BOA): Chalk out a list of all critical organization entities.

- Operational Department
- Critical support services
- Corporate security
- Senior Executives

1.2) Team Selection

- Every business unit representatives
- IT subject matter expert
- Cyber security team member
- Physical security team representatives
- Legal and regulatory matter expert
- Representative of HR
- Public Relation team representative
- Senior management representative

Assignment of a BCM is utmost importance at this stage

1) Project Scope and planning

1.3) Resources Requirement

1.3.1) Human resource:

-Considerable resources consumption in the planning and development of BCP plan

-Testing, Training, and Maintenance of BCP

-Implementation of BCP

1.3.2) Financial resources

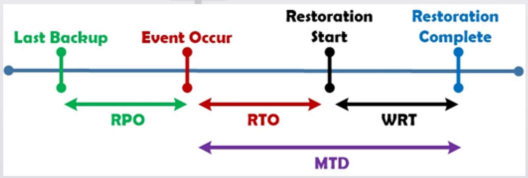
- Capital for human resources to perform and manage above stated activities of BCP
- Capital on technical/human resources redundancy (Additional repetitive cost)

1.4) External Dependencies

- Vendors: Vendors dependency is imminent to supply resources. Assess vendors based on SLA, SLR, MoU
- Legal and Regulatory matters: Fulfil legal and regulatory obligations

2) Business Impact Assessment (BIA)

- 2.1) Whatever identified assets are defined in BOA write them down and calculate the following terms for them:
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO) [Unit of time in DATA]
  - Mean Tolerable Downtime (MTD)
  - Work Recovery Time (WRT)



2) Business Impact Assessment (BIA) (Contd..)

- 2.2) Risk Identification and Threats
  - List down possible types of man made and/or natural risks
- 2.3) Likelihood Assessment
  - Calculate the ARO
- 2.4) Impact Assessment
  - Calculate SLE, ALE, EF. In qualitative assessment, consider experts opinion
- 2.5) Chalk down all the ALEs in the light of BIA parameters

3) Continuity Planning

3) Continuity Planning

- 3.1) Strategy Development: Based on the budget and various other factors, specify which of the ALE, RPO, and/or MTD will be covered

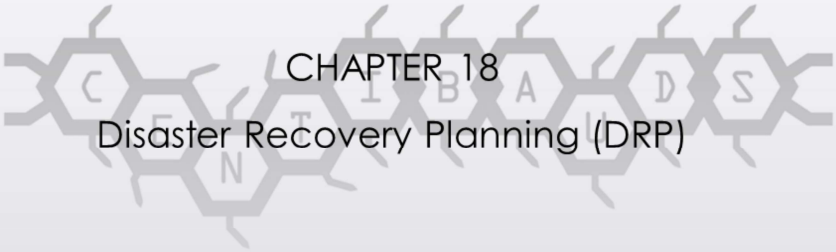
  Target the Risk Appetite and Risk Tolerance approved ALE, RPO and/or MTD

- 3.2) Provisions and Process: Budget and efforts are directed towards risk mitigation and devise procedures
  - 3.2.1) First focus on people ensure protection of lives
  - 3.2.2) Ensure facility protection so the team can continue the BCP
  - 3.2.3) Infrastructure hardening, redundancy and physical ramifications

4) Approval and Implement

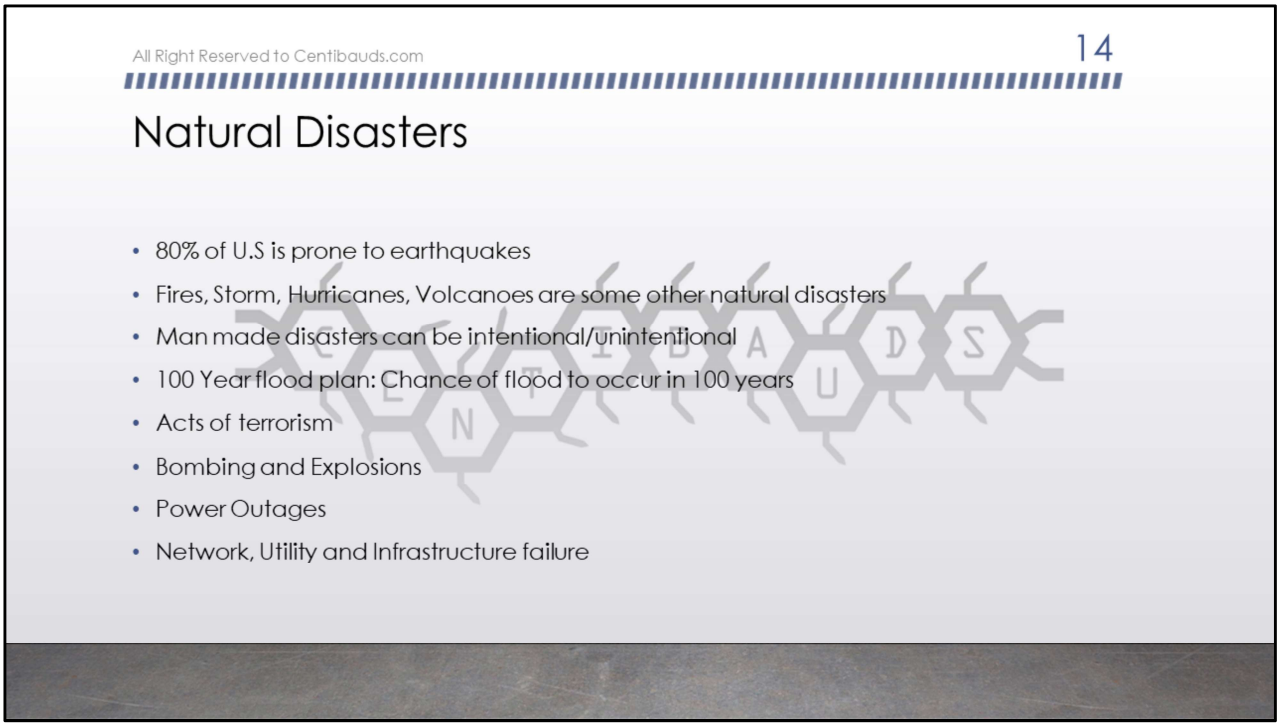
- Get sign-off and approval from top management
  - Implement to the state from where BCP will initiate
  - Educate, Train, and Prepare resources and organization

Domain 7
Security Operations

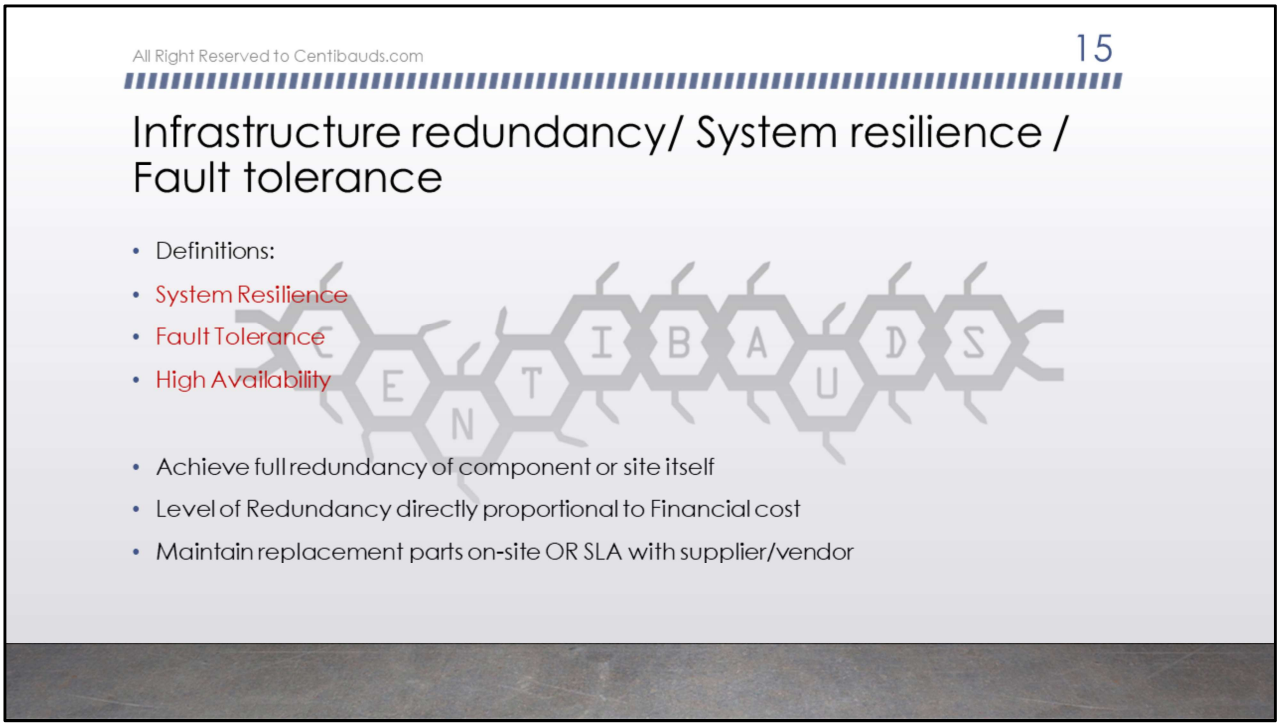


CHAPTER 18

Disaster Recovery Planning (DRP)



-Terrorism Objective is to inject fear and target most critical asset i.e. Human Lives
-Bombing: Man-made error or intentional causing drastic impact
-Power Outage: Addresses by UPS for short term until long term solution of generator starts. Also alternate power sources and redundancy is the key



-System Resilience is ability of a system to maintain an acceptable level of service at occurrence of an adverse event
-Fault Tolerance is ability of system to suffer a fault but maintain its operational practices
-High Availability is redundancy technology that make the secondary unit operational immediately

Redundant Array of Independent Disks (RAID)

- Example of system resilience and fault tolerance

- RAID-0 Striping 2 disk
- RAID-1 Mirroring 2 disks
- RAID-5 Striping with Parity at least 3 disks
- RAID-6 Same as RAID-5 but with distributed dual parity on 4 disks
- RAID-10 Striping + Mirroring

- Hardware based RAID more efficient unlike software based
- Parity recovery are time consuming

Fault tolerance controls

- Line interactive UPS giving backup of 5 to 30 minutes until system shuts down or generator turns on
- Redundancy via Failover clusters and load balancers
- Multiple servers behind Load Balancers

Datacenter (DC) types

	Energy	Cooling	Data Source (ISP link)	Alternate Power, Cooling, ISP lines	Redundancy	Compute sources
Tier 1	Single source	Single Unit	Single Source	No	No	Plain compute servers
Tier 2	Power grid +UPS (5 mins backup)+24 hour petrol filled generator	Alternate Units	Single Source/ Multiple Source	No	Yes	Redundant servers within same cluster
Tier 3	Redundant power sources	Alternate Units	Multiple Sources	Yes, from different facility entrances	Yes	Redundant Clusters
Tier 4	Redundant power sources	Alternate Units	Multiple Sources	Yes, from different facility entrances	Yes	Redundant Clusters

-Tier1 just few plain compute sources
-Tier 2. Can be power grid and 24 hour petrol filled generator with UPS giving few minutes backup. starts to give power. Cooling units are alternate. But power cabling and cold air channel is the same. Same goes for data
-Tier 3 Same characteristics as Tier 2 but the entrance of cabling and channels paths for cooling into the facility is different. This specialized to prevent fire related emergencies. It gives privilege to perform maintenance on one part of the DC while the 2nd part continues the services
-Tier 4 is end to end redundancy from multiple systems to achieve level of fault tolerance. It is optimization over Tier 3 by making system sustain and tolerate fault but maintain its operational services.

Trusted recovery

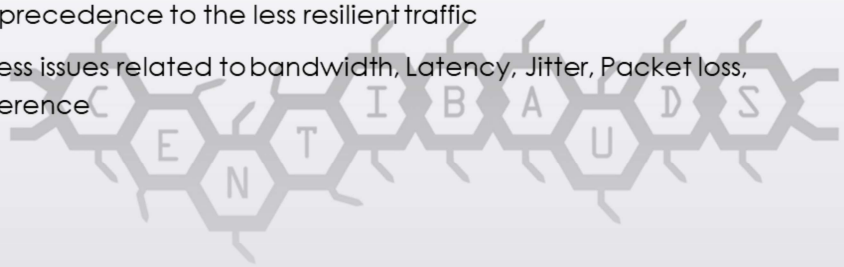
- Recovery can be manual or automated
- fail-open OR fail-secure
- Cases of fail-open and fail-secure
- When considering fail-secure state, consider the following:
  - Failure preparation in the form of fault tolerance, system resilience, and reliable backup solution
  - System recovery to recover in the previous secure state

Fail-Secure state recovery as per Common criteria

- Manual recovery: System recovers to secure state on Administrator intervention
- Automated recovery: System recovers to secure state upon no intervention
- Automated recovery without Undue Loss: System recovery with assurance that no loss is incurred in any entity such as data
- Functional recovery: Recovery is done in 2 options. It attempts recovery of the functions OR roll back changes and return to secure state

Quality of Service

- Give precedence to the less resilient traffic
- Address issues related to bandwidth, Latency, Jitter, Packet loss, Interference



Recovery Strategy

- Have organization individuals aware of their roles and contribution in case disaster hits
- Automated process
- Effective insurance plan
- Crisis Management
- Situation is dire in the event of disaster
- Cool and predetermined minds dominate
- Constant awareness, practice and training can facilitate readiness
- Evacuation training is must
- Every resource should inform LEA

Work Group Recovery and Alternate Facilities

- Work Group Recovery:
  - Set up section of same site or alternate site for the team that are engaged in recovery functions
  - The environmental should be functional and supportive
  - Provide sufficient provisions and stable supply of resources
- Alternate Facilities
  - Cold Site: Empty facility with electrical capability No compute, No Data or/and ISP circuit; is up in 2-3 days
  - Warm Site: Facility equipped with compute and ISP circuit but no data. Data is suppose to be replicated from the backup storage site; take up to 12 hours
  - Hot Site: Facility fully operational and is in standby mode; Data is on-site of the last backup but new backup may or may not be there
  - Mobile Site
- Hardware Replacement: SLA, On-site spares, Outsource

Backup method

- Time and data loss RPO matters here
- Electronic Vault: Once in a while replication and backup (12 hrs); Keep into consideration time required to complete vault process and restoration
- Remote Journaling: Considerably frequent replication and backup (2-3 mins)
- Remote Mirroring: Immediate replication (seconds)
- Backup method, size, type, and strategy directly influenced by criticality and budget
- Always take backup when network is least utilized
- Full backup on weekend, Incremental weekly
- Review backup once in a while V V V important. restore it to see it works

Types of Backup

- Full backup: Full replication Reset archive bit
- Differential Backup: Difference from previous full backup Retains Archive BIT (ON)
- Incremental Backup: Difference from any previous Turns Archive Bit (OFF)

Sample Question on backup types

- A File server follows this backup schedule:
  - Sunday: Full backup
  - Monday to Saturday: Incremental backups

Which backup files are needed to recover the complete data?

- A File server follows this backup schedule:
  - Sunday: Full backup
  - Monday to Saturday: Differential backups

Which backup files are needed to recover the complete data?

Some controls that are considered in DR

- Tape Management: Tower of Hanoi, Six cartridge, GSM etc. are various schedulers.
  - Disk-to-Disk backup for exact replica of drives (Most effective but costly)
  - A tape managed properly can be reused 1000 times
- Murphy Law suggests that there is always change soon after backup; to counter that use technologies of clustering, mirroring, and RAID
- Software Escrow Management: 3rd party holds the key and support code in case application needs reset
- Service Bureau: Rental support and assistance in DR situation
- Mutual Assistance Agreement (MAA) OR Reciprocal Agreement susceptible to confidentiality breach

RAID is done in backups/ Disk management in archiving

Some controls that are considered in DR (contd..)

- Database are the most critical asset
- Should have constant availability at all times with no room for loosing data
- Cloud Computing:
  - Outsource IAAS to cloud
  - Cloud bursting

Disaster Recovery Plan Development

- Iterative process with creation of multiple documents
- Organization size defines list of documents created
- DR Plan is extremely confidential document
- Documentation of DR:
  - Executive summary (High level plan)
  - Department specific
  - Technical guides for IT and backup managing team
  - Checklist for individuals
  - Full copy of DR plan

Full copy of DR plan document

- Emergency Response
- Where to collect DR package containing keys, flash light, maps, documents, contacts and checklist
- Checklist is created to perform certain action with most critical on top to least
- Actions like Alarm initiate, Evacuate, Call911, Medical Emergency participate, Initiate DRP
- Top to bottom call and bottom calls top to assure all are aware
- Holistically DR covers:
  Plan-> Activation Procedure -> Recovery Strategy -> Costing -> Tests -> Assigned members -> Resources -> Documents -> Restoration

Recovery VS Restoration

- Recovery: Just bring the services up at secondary site (Quick resolution)
- Restoration: Make it to previous stable state at primary site (Time consuming maybe months)

Training Awareness

- Sent time-to-time to review
- Table top exercise (Read Through, Structured Walk Through)
- Simulation Test and Gamification
- Parallel Test
- Full Interruption aware
- Full Interruption unaware

Communication and Documentation

- In disaster CEO is spokesperson for everyone
- Public Relation department will use quote of CEO and engage with
  - LEA
  - Media
- BCP documentation assures:
  - Written commitment
  - Historical record for guidance
  - Clear vision of roles and responsibilities to BCP

Communication and Documentation

- BCP Project Plan and MEMO (BOA and phase 1)
  - Audience are BCP team members for BCM
  - List all business assets, senior management approval and scope
  - Continuity Planning Goals from the team or top management
- Statement of Importance
  - Audience are all employees and stakeholders for CEO
  - Highlights the need of BCP/DR
  - Includes Statement of Organizational Responsibly

Communication and Documentation (Contd..)

- Statement of Priority
  - Audience are BCP team members for BCM
  - After BIA process, these statements sets the assets and operations in the order of importance
- Statement of Urgency and Timing
  - Audience are BCP team members for BCM
- Risk Assessment report
  - Audience are BCP team members for BCM
- Vital Records Program
  - Audience are BCP team members for BCM
  - Maintain records and events details of BCP process