– if an organization has an RPO of four hours,

Topic no 41: High Availability & Redundancy Case Study

- Mid-sized enterprise
- 3000 total staff
- 2000 IT users
- 30 IT team
- One DC, one secondary (regional) data center (warm site & backup site), and one DR site 99. uptime designed.

IT setup:

- Oracle ERP system
- Share point portal for workflow automation
- Head office in Karachi
- Primary DC in Karachi (hosted with 3rd party)
- DR site in Lahore (hosted with 3rd party)
- Secondary DC in ISB

Primary DC:

High Availability

- Fully redundant (HA) design for network, systems, and storage
- Cisco HA (active-standby)
- Oracle cluster technology for servers and DBs (active-active)

DataBase.

Data Center

Secondary DC (ISB):

- All network, systems, and storage backups maintained here (also mirrored in DR)
- Regional servers (AD, file servers, etc)
- Test & staging environment here (segregated from main DC)
- Office working space

DR site IMP. DR → Disaster Recovery.

- Bare minimum HA (as DR site) for network, systems, and storage
- Mirror of all backups from secondary site maintained here
- Office working space
- Some additional computing capacity (minimum for unforeseen events)
- All critical systems and devices maintained in active mode (hot) for immediate DR failover
- Data maintained as per org RTO/RPO for immediate utility
- Monthly DR testing/drill

Backup strategy:

- Primary backup at secondary DR site MCQs.
- Mirror at DR site
- For critical systems: monthly full backup, daily incremental backup
- For critical network devices: weekly full backup; backups based on change

Topic no 42: Backup Strategies

- **Backup considerations:**
  - What to backup?
  - Backup location?
  - Freq of backup? Frequency.
  - Backup operator?
  - Backup checker (verification)?
  - Backup test & security methods?
  - Technology & tools used for backup?

- **What to backup?**
  - Network configuration files
  - OS backups (Operating System)
  - Database & application data
  - Other critical data
- **Backup location?**
  - Onsite for faster recovery
  - Offsite for DR purposes
  - Intermediate site (secondary site) as a middle-ground

depends on 4 factors.

- **Backup frequency?**
  - Depends entirely on criticality of data (1), nature of the information being backed up (2) (how frequently does info change?), storage space available (3), and overall backup plan (4).

- **Backup operator and checker?**
  - Backups should ideally be automated (1)
  - Operator should ensure that backups have taken place (2)
  - Verifier should sign-off (3) that check has been made
- **Backup testing & security considerations:**
  - Backup testing should be performed on a periodic (1) basis and greater than the frequency of the drill (2) (e.g. DR drill once a QTR, & testing once a month)
  - Encryption & compression

↓MCQs.

- **Backup tools and technology:**
  1. Consider NAS, SAN, SCSI/IDE/SATA drives
  2. Various tools and technology to perform full, differential, and incremental backups
  3. Encryption
  4. Access control
  5. Alerts & reporting

Short + Long + MCQs.

	Tool	Function	Complexity level	Examples
1)	Enterprise Antivirus	System antivirus and malware protection	Low	Sophos, Avast, Kaspersky, Symantec, McAfee
2)	MS AD (GP)	Pushing out security policies through AD GPO	Low	Pushing out windows password settings
3)	VM	Vulnerability scanning	Medium	OpenVAS, Nessus, Qualys
4)	Log Management	Logs collection & analysis	Medium	OSSEC
5)	Network & Performance Management	NOC	Low	CACTI, ORION
6)	Automated Backups	Backups	Medium	Veritas
7)	Windows Updates	Windows Updates & Configs	Low	WSUS, SCCM, SCM
8)	Asset Management	Dtect, Track, Manage Assets	Medium	Asset Explorer, PulseWay
9)	Trouble Ticket System	TT Workflow	Medium	BMC Track-IT, SysAid
10)	SIEM	Event Management	High	OSSEC, Splunk, Q-Radar
11)	DLP	Data Loss Prevention	High	Symantec,
12	Encryption Software	Encryption	High	TrueCrypt

Topic no 46: What Does "Box Security" Mean?

- "Box Security" refers to a prevalent approach in the industry, especially in larger organizations in which the solution for every security challenge is in the form of a "box" or device
- **Box for :**
  - Email security
  - Web security
  - FW
  - IPS
  - APT attack prevention
  - DDOS prevention
  - Network DLP
  - Network Forensics
  - Others
- Security is a combination of people, process, and technology
- Industry observation: most of the devices are not used to full capability or capacity after purchase
- Case in point: SIEM solution or DB security solution
- "Box security" is not the silver bullet MCQs.
- Although many devices and boxes are required, they do not ensure a good security posture
- This approach is unfortunately promoted by many vendors who have equipment to sell
- Consider organizational maturity & readiness

Other challenges with "box security" approach:

- Shortage of staff (IT & security)
- Training and skill required to operate the sophisticated devices and features

- Device objectives, and high-level-design (HLD) should be planned prior to commissioning
- Min operational baseline and configuration should be documented in SOP
- Device feature set and configuration audits should be conducted on a periodic basis (annual)

Topic no 47: Best Approach: IT Enterprise Security

- The 4-layer security transformation model is the only way to effectively and practically address secur posture
- 4-layer security transformation model is tried & tested for geographies where the overall secur awareness & posture is weak

1. **Security hardening:** address security configuration of all IT assets which security "boxes" won't do f you
2. **Vulnerability management:** scanning to inspect patching of IT assets (essential)

– Security engineering

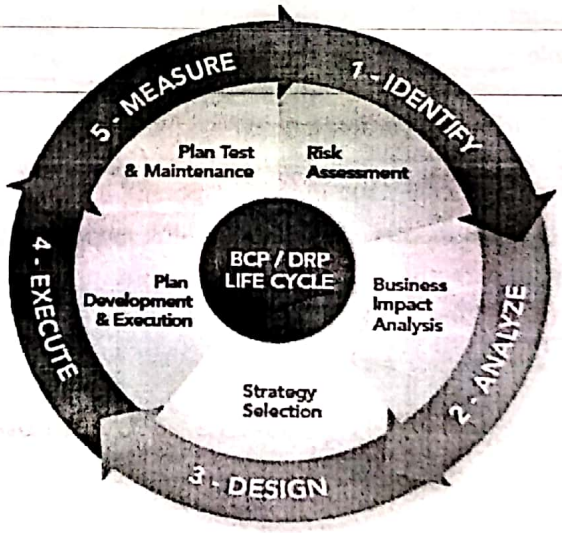
– Security governance

3. **Security engineering:** this is where more serious investments may be made once layers 1 & 2 ha been completed satisfactorily (or are being addressed).

4. **Security governance**: ensure the proper utilization (as intended), ROI, and audits of purchased devic & solutions. Also ensure configs are as per design, and SOPs.

Topic no 48: What Is Disaster Recovery (DR)?

- **What is a disaster?**
  - Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business
- **What is disaster recovery (DR)?**
  - DR is an area of security that allows an organization to maintain or quickly resume mission-critical (IT) functions following a disaster
- **What could cause the invocation of a DR fail over to DR site?**
  - (1) Natural disasters such as flood, earthquake, lightning, storm
  - (2) Disaster caused by human actions such as riot, fire, terrorist act, etc
- **What is the difference between DR and business continuity (BC)?** IMP
  - DR is an IT function, whereas business continuity addresses keeping all essential aspects of a business functioning despite disruptive events (DR is a part of BC) MCQs.



DR.

- **Three step process:**
  - Failover to the DR site (DR invocation)
  - Restoration of the services/facilities on primary site
  - Recovery (switchover back to primary site)
- **What is a DR plan?**
  - (1) A documented, (2) structured approach to dealing with unplanned incidents

- **DR plan checklist:**

- Scope of the activity
- Gathering relevant network infrastructure documents
- Identifying the most serious threats and vulnerabilities, and the most critical assets
- Identifying current DR strategies
- Identifying emergency response team
- Management review & approval of DR plan
- Testing the plan (drill)
- Updating the plan
- Implementing a DR plan audit

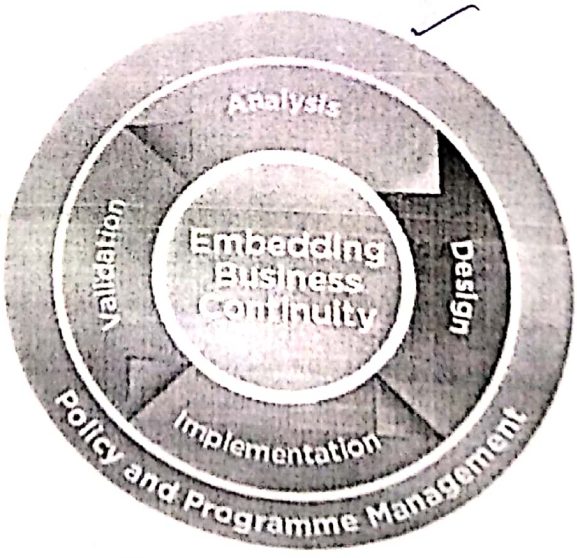
Topic no 49: What is Business Continuity (BC)?

- **What is business continuity?**

  - Business Continuity (BC) is the capability of the org to continue delivery of products or se at acceptable predefined levels following a disruptive incident *(Source: ISO 22301:2012)*

- **What is business continuity management?**

- Holistic management process that identifies potential threats to an organization and the impa business operations those threats, if realized, might cause, and which provides a framework for bui org resilience with an effective response that safeguards interests of key stakeholders, reputation and value-creating activities. *(Source: ISO 22301:2012)*

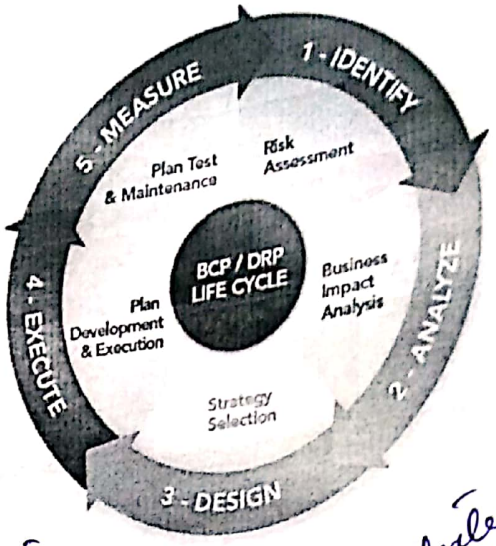


The BCM Lifecycle
- Improving organizational resilience

- **What is a BC plan?** Imp.
  - A document that consists of critical information an organization needs to continue operating during an unplanned event
  - The BCP should state essential functions of the business, identify which systems and processes must be sustained, & detail how to maintain them.
  - It should take into account any possible business disruption

Topic no 50: DR In Enterprise Architecture – Part 1

- **DR considerations:**
  - DR plan
  - RTO & RPO
- **DR plan:** MCQS + Short.
  - A disaster recovery policy statement, plan overview and main goals of the plan
  - Key personnel and DR team contact information
  - Description of emergency response actions immediately following an incident.
  - A diagram of the entire network and recovery site. MCQ's.
  - Directions for how to reach the recovery site,
  - A list of software and systems that will be used in the recovery.
  - Sample templates for a variety of technology recoveries, including technical documentation from vendors.
  - Summary of insurance coverage.
  - Proposed actions for dealing with financial and legal issues.
  - Ready-to-use forms to help complete the plan.



Recovery Time Object - Both all repeated.

- **RTO:**
  - Max amount of time, following a disaster, for an org to recover files from backup storage resume normal operations; max amount of downtime an org can handle.
  - If an organization has an RTO of two hours, it cannot be down for longer than that
- **RPO:** Recovery Point Object.
  - RPO is the max age of files that an organization must recover from backup storage for n operations to resume after a disaster; determines the minimum frequency of backups.
  - For example, if an organization has an RPO of four hours, the system must back up at least four hours

Topic no 51: DR In Enterprise Architecture – Part 2

- DR considerations:
  - DR facility
  - DR drills & testing
  - DR testing checklist
  - BC plan alignment
- **DR facility:**
  - Location
  - Media circuits and backup circuits
  - Power and environment

- IT data center design
- Based on DR plan
- Operations & maintenance

- **DR drills & testing:**
  - Frequency and execution of DR drills as per IT policy of the org
  - Min twice a year and preferable quarterly for critical business reqmts
  - Backup testing

- **DR testing checklist:**
  - Secure management approval and funding for the test.
  - Provide detailed information about the test.
  - Make sure the entire test team is available on the planned test date.
  - Ensure your test does not conflict with other scheduled tests or activities.
  - Confirm test scripts are correct.
  - Verify that the test environment is ready.
  - Schedule a dry run of the test.
  - Be ready to halt the test if needed.
  - Have a scribe take notes.
  - Complete an after-action report about what worked and what failed.
  - Use the test results to update DR plan

- **BC plan alignment:**
  - DR is under IT ownership, whereas BC is under business operations ownership
  - DR is part of overall BC
  - Both plans must integrate and align seamlessly

Topic no 52: Role Of An IT Asset In Enterprise Security

- **What is an IT asset?** MCQs.
  - An IT asset is any resource such as hardware, software, information, human resource, or facility owned or utilized by the organization for IT processing