IT Auditing

Lecture - 8

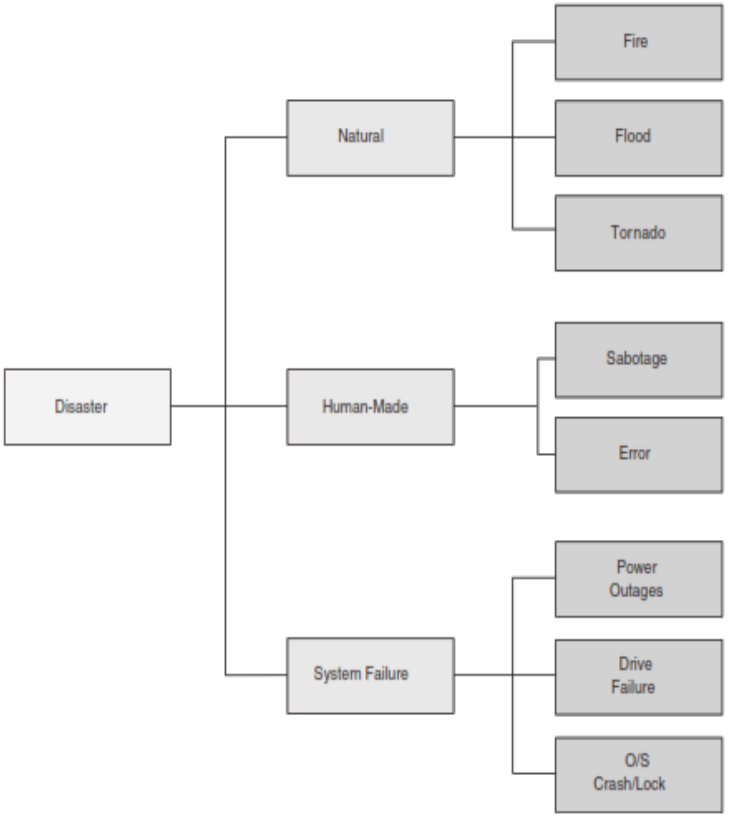
Ms. Saleem Adeeba
Temporary Assistant Lecturer
Dept. of Computing & Information Systems
Sabaragamuwa University of Sri Lanka
0720928486
adeesa@foc.sab.ac.lk

3. Disaster recovery planning

- Disasters such as earthquakes, floods, sabotage, and even power failures can be catastrophic to an organization’s computer center and information systems.

3. Disaster recovery planning

- Types of Disasters



3. Disaster recovery planning

a) Identify critical applications

b) Create a disaster recovery team

c) Provide site backup

d) Specify backup and off-site storage procedures

3. Disaster recovery planning

a) Identify critical applications

- The first essential element of a DRP is to identify the firm's critical applications and associated data files.
- Recovery efforts must concentrate on restoring those applications that are critical to the short-term survival of the organization.
- The task of identifying critical items and prioritizing applications requires the active participation of user departments, accountants, and auditors.
- Too often, this task is incorrectly viewed as a technical computer issue and therefore delegated to IT professionals.

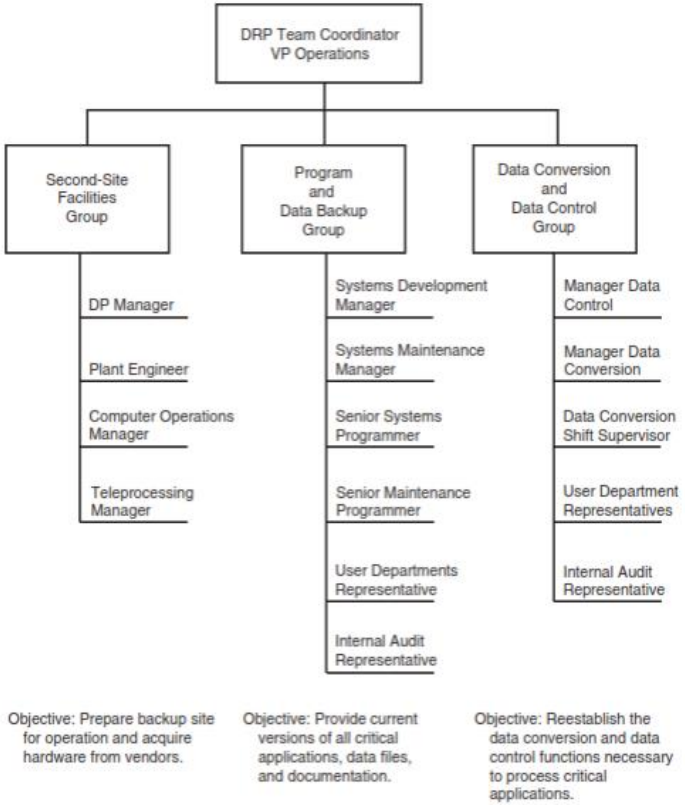
3. Disaster recovery planning

b) Create a disaster recovery team

- Recovering from a disaster depends on timely corrective action.
- Delays in performing essential tasks prolongs the recovery period and diminishes the prospects for a successful recovery.
- To avoid serious omissions or duplication of effort during mplementation of the contingency plan, task responsibility must be clearly defined and communicated to the personnel involved.

3. Disaster recovery planning

b) Create a disaster recovery team



3. Disaster recovery planning

c) Provide site backup

- A necessary ingredient in a DRP is that it provides for duplicate data processing facilities following a disaster.

- Among the options available the most common are

i. mutual aid pact;
ii. empty shell or cold site;
iii. recovery operations center or hot site; and
iv. internally provided backup.

3. Disaster recovery planning

d) Specify backup and off-site storage procedures

- ❑ All data files, applications, documentation, and supplies needed to perform critical functions should bemautomatically backed up and stored at a secure off-sitelocation.

- ❑ Data processing personnel should routinely perform backup and storage procedures to obtain and secure these critical resources.

3. Disaster recovery planning

d) Specify backup and off-site storage procedures

- ❑ – Some of the examples are;

i. Operating System Backup.
ii. Application Backup.
iii. Backup Data Files.
iv. Backup Documentation.
v. Backup Supplies and Source Documents.

3. Disaster recovery planning

- ❑ Audit Objective

- ✓ The auditor should verify that management’s disaster recovery plan is adequate and feasible for dealing with a catastrophe that could deprive the organization of its computing resources.

3. Disaster recovery planning

- Audit Procedures

- In verifying that management's DRP is a realistic solution for dealing with a catastrophe, the following tests may be performed.

i. Site Backup.
ii. Critical Application List.
iii. Software Backup.
iv. Data Backup.
v. Backup Supplies, Documents, and Documentation.
vi. Disaster Recovery Team.

Next Lecture

- Outsourcing the IT function
- Chapter 3: Security Part I: Auditing Operating Systems and Networks