Ch.12 summary By @MHazazi

Emergency Preparedness

- **Disaster**
  - Any event that results in damage or destruction, loss of life, or drastic change to the environment
  - The cause can be environmental, operational, accidental, or willful
- **Resilient organization**
  - Quickly adapt and recover from known or unknown change to the environment
- Business disruption has an economic and societal ripple effect
- Emergency preparedness is a civic duty and regulatory requirement

Business Continuity Risk Management

- **Continuity planning**
  - Business practice of ensuring the execution of essential functions
  - Component of organizational risk management
  - Risk management for continuity of operations requires the organizations to:
    - Identify the threats that can disrupt operations
    - Determine the risk
    - Assess the impact on the company
- **Business continuity threat**
  - potential danger to the organization
  - Threats can be business specific, local, regional, national, or even global
- **Business continuity threat assessment objective**
  - Identify viable threats and predict the likelihood of occurrence
  - Threat modeling takes into account historical and predictive geographic, technological, physical, environmental, industry, and third-party factors
- **Business continuity Risk assessment**
  - Evaluates the sufficiency of controls to prevent a threat from occurring or to minimize its impact

What Is a Business Impact Assessment

- **Business Impact Analysis (BIA)**
  - Identify essential services/processes and recovery timeframes
  - multistep collaborative activity involves business process owners, stakeholders, and corporate officers

- **A BIA incorporates three metrics**:
  - **Maximum tolerable downtime (MTD)**
    Total length of time an essential business function can be unavailable without causing significant harm to the business.
  - **Recovery time objective (RTO)**
    Maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business processes.
  - **Recovery point objective (RPO)** The acceptable data loss
    point in time, where data can be recovered prior to a disruption or system outage

Business Continuity Plan

- **Business continuity plan (BCP) or continuity of operations plan (COOP)**
  - The objective is to ensure the organization has the capability to respond and recover from a disaster.
- **Component:**
  - **Response plans**
    initial response and near-term response, plan activation, notification, communication, evacuation, relocation, coordination with public authorities, and security
  - **Contingency plans**
    immediate, near-term, and short-term alternate workforce and business processes
  - **Recovery plans**
    immediate, near-term, and short-term recovery of information systems, infrastructure, and facilities
  - **Resumption plans**
    guide the organization back to normalcy.
- **Business continuity management involves the entire organization**
  - Board of Directors
    provides oversight and guidance, authorizes the related policy, and is legally accountable for the actions of the organization
  - Executive management
    provides leadership
  - Business Continuity Team (BCT)
    make decisions related to disaster preparation, response, and recovery

Disaster Response Plans

- **Addresses what should be done immediately following a significant incident**
  - Defines who has the authority to declare a disaster
  - Defines who has the authority to contact external entities
  - Defines evacuation procedures
  - Defines emergency communication & notification procedures

- **Upon declaration of a disaster, all BCT members should report to a designated command and control center**

- **Occupant emergency Plan (OEP)**
  - Describes evacuation and shelter-in-place procedures in the event of a threat or incident to the health and safety of personnel

- **Relocation strategies**
  - **Hot site**
    - Fully operational location with redundant equipment.
    - The data has been streamed to the site on a real-time basis or close to real time
  - **Warm site**
    - Configured to support operations including communications capabilities, peripheral devices, power, and HVAC.
    - Spare computers may be located there that then would need to be configured in the event of a disaster
    - Date must be restored
  - **Cold site**
    - Available alternative location
    - Equipped with power, HVAC, and secure access
  - **Mobile site**
    - Self-contained unit
    - Equipped with the required hardware, software, and peripherals
    - Data needs to be restored

Operational Contingency Plans

- Addresses how an organization's essential business processes will be delivered during the recovery process
- Developed at the departmental level
- Responsibility of the business process owner
- The documentation should follow the same form as the SOPs

The Disaster Recovery Phase

- **Recovery strategies**
  - The path to bringing the company back to a normal business environment
  - A plan should be in place that breaks down each category of the overall recovery effort to simplify the daunting recovery process:
    - Mainframe
    - Network
    - Communications
    - Infrastructure
    - Facilities

- **Recovery procedures**
  - All procedures should be designed, tested, documented, and approved *prior* to when the disaster strikes
  - Procedures should be written as if the person who will be following them is not intimately familiar with the information system or component
  - Procedures should explain what needs to be done, when, where, and how
  - The key is to respond fast using predefined steps
  - Recovery procedures should be reviewed annually

The Resumption Phase

- The objective is to transition to normal operations

- **Two major activities**
- **Validation** = Verifying recovered systems are operating correctly
- **Deactivation** = official notification that organization is no longer operating in emergency or disaster mode

Plan Testing and Maintenance

- Proactive testing of the plan is essential
- Until tested, the plan is theoretical at best
- **The tests should prove that the procedures and the plan are:**
  - Relevant
  - Operable under adverse conditions
  - Accurate
- Tests are used to discover errors and inadequacies
- **Three standard testing methodologies:**
  - **Tabletop exercise**
    - Structured review
    - Simulation
  - **Functional exercises**
  - **Full-scale testing**

- **Business continuity plan audit**
  - Evaluation of how the business continuity program in its entirety is being managed
  - Auditors must be independent

Plan Maintenance

- Business environments are dynamic:
  The plan should be reviewed and edited regularly to match the changes that occur in the company and/or the industry in which the company is involved

- The plan cannot be reviewed without the risk assessment being reviewed as well

- Responsibility for maintaining the plan should be assigned to a specific role such as the ISO