Understanding Incidents and Disasters

Understanding Incidents and Disasters

Incidents

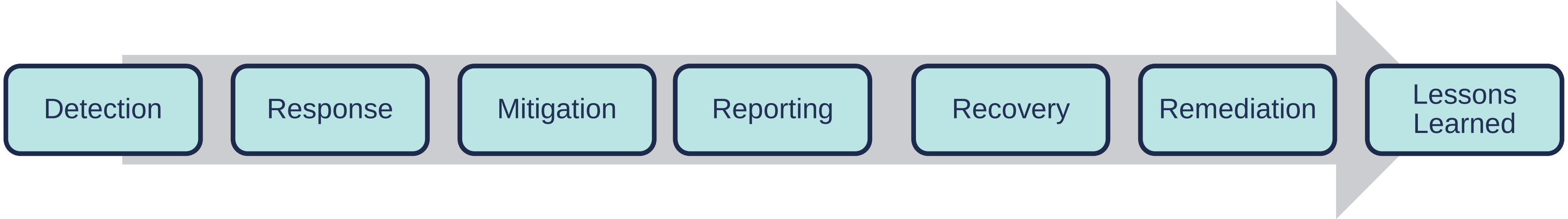
- An incident is any event that negatively impacts an organization.
- **Example:**
  - An employee's laptop is infected with a virus causing that one employee not to be able to work

Disasters

- Disasters are incidents that have a significant negative impact on the organization.
- **Example:**
  - A monsoon floods the entire data center causing significant downtime to the entire company.

Incident Response

7-Step Incident Response Process



1. **Detection**: The initial detection that an incident has occurred, such as an alert from an IPS or IDS.
2. **Response**: The initial response from the incident response team.
3. **Mitigation (Containment)**: The damage is contained so it doesn't spread to others.
4. **Reporting**: After the initial response and containment, reporting to appropriate stakeholders begins.
5. **Recovery**: The goal of recovery is to return systems back to their last known-good state.
6. **Remediation**: The root cause of the incident is addressed, ensuring it doesn't affect other systems in the future.
7. **Lessons Learned**: Reports and discussions on how we can improve our incident response process in the future.

Disaster Recovery and Business Continuity

Disaster Recovery and Business Continuity

Disaster Recovery Plan (DRP)

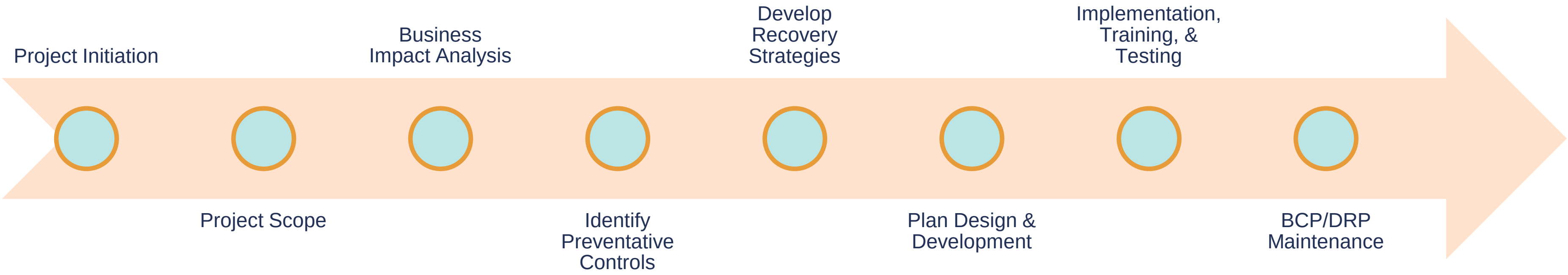
- A short-term plan designed to recover an organization from a disaster.
- Disaster recovery is the tactical response to a disaster, focusing on IT.
- Its end goal is to recover and protect an organization's IT infrastructure when a disaster occurs.

Business Continuity Plan (BCP)

- A long-term plan designed to ensure the continuity of operations after a disaster has occurred and the DRP is in effect.
- Ensures that the organization can operate throughout and after a disaster has occurred.
- Focuses on all critical business processes, not just IT.

INSTRUCTOR
ALTON

Developing a BCP and DRP


Project Initiation
Project Scope
Business Impact Analysis
Identify Preventative Controls
Develop Recovery Strategies
Plan Design & Development
Implementation, Training, & Testing
BCP/DRP Maintenance

Important BIA Metrics

Metric	Details
Maximum Tolerable Downtime (MTD)	The overall time an organization can survive without a given system running and operational.
Recovery Time Objective (RTO)	The maximum time allowed to recover IT systems. • RTO cannot be > MTD
Work Recovery Time (WRT)	The amount of time it takes to fully recover an IT system. • WRT cannot be > RTO.

INSTRUCTOR
ALTON

Common Recovery Options

Metric	Details
Redundant Sites	A live, running offsite production environment duplicate that has the capabilities to seamlessly take over IT operations without any downtime or loss of data in the event of a disaster.
Hot Sites	An off-premises location where a company's work can resume during a disaster. Has all the equipment necessary for a business to resume regular activities, typically in less than an hour, with critical applications and data mirrored in real-time.
Warm Sites	Similar to a hot site, but takes longer to get up and running. A warm site may include some of the hardware and software in place, but can take 1 to 3 days to fully configure and get up and running.
Cold Sites	This is the least expensive option of the four listed on this slide; moreover, it takes the longest to get up and running. It's typically an offsite location with none of the IT hardware or software in place.

BCP / DRP Testing

- A BCP/DRP is useless unless it is effectively tested on a regular basis. Common types of testing methodologies include:
    - Checklist
    - Structured Walkthrough / Tabletop Exercise
    - Simulated Test
    - Parallel Processing
    - Partial or Complete Disruption