DISASTER RECOVERY PLANNING: FROM THEORY TO ACTION

2025 Rochester Security Summit

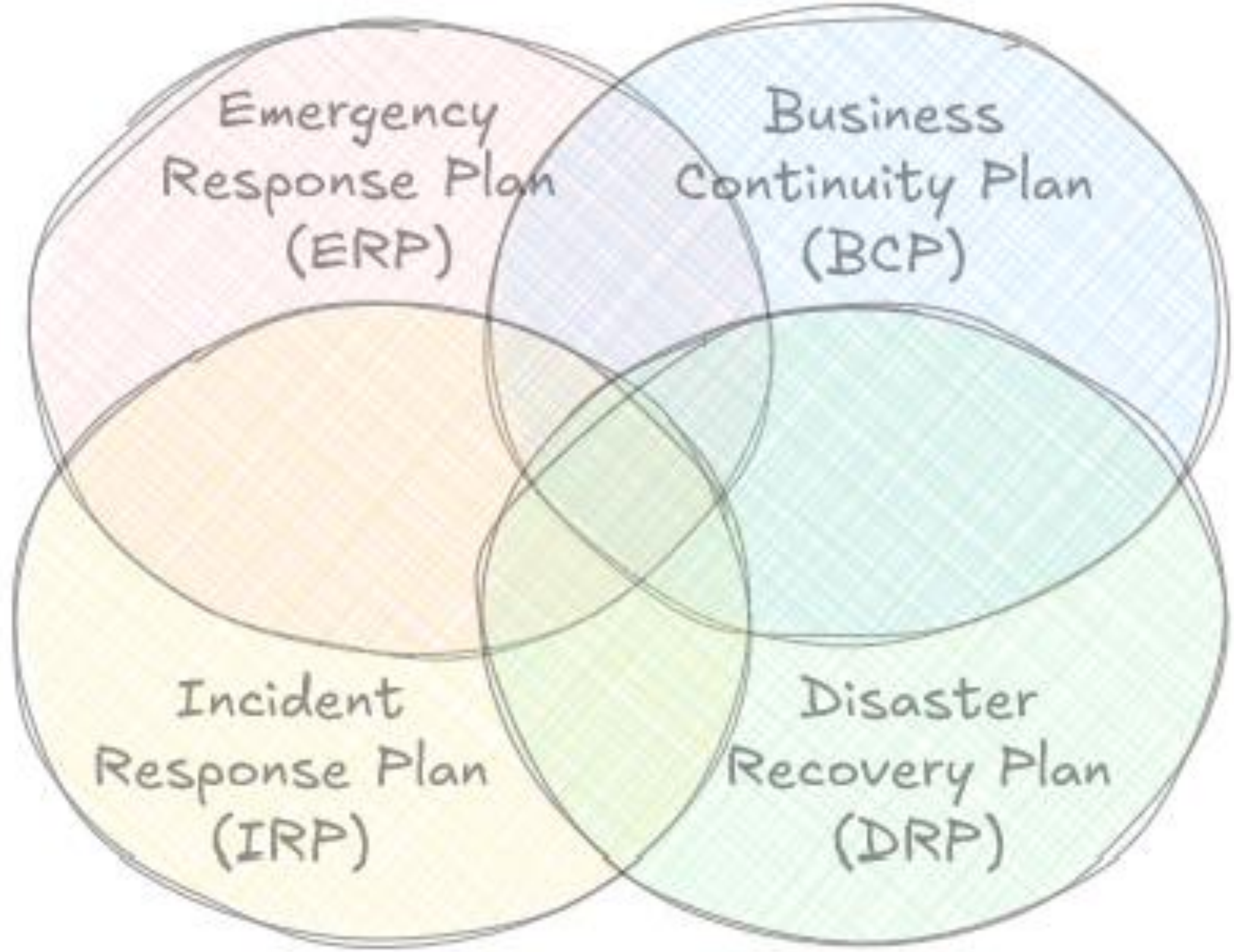
Jason Taylor

Learning Objectives / Quests

- I will be able to explain the differences between a DRP, IRP, and BCP

- I will be able to follow the steps to create a DRP:
  a) Identify Attack Surface and Priorities
  b) Develop Contingencies and Document them in a DRP
  c) Distribute, Test, and Maintain the DRP

Contingency Planning Confusion


Emergency Response Plan (ERP)
Business Continuity Plan (BCP)
Incident Response Plan (IRP)
Disaster Recovery Plan (DRP)

What is Disaster Recovery?

- **Disaster** = any event that results in widespread and/or long-term IT service outage and may require operating at an alternative location

- **Goal** = reduce operational loss by rebuilding, restoring, and recovering as quickly as possible

- **DR** = disaster recovery
- **DRP** = disaster recovery plan
- **DRT** = disaster recovery team

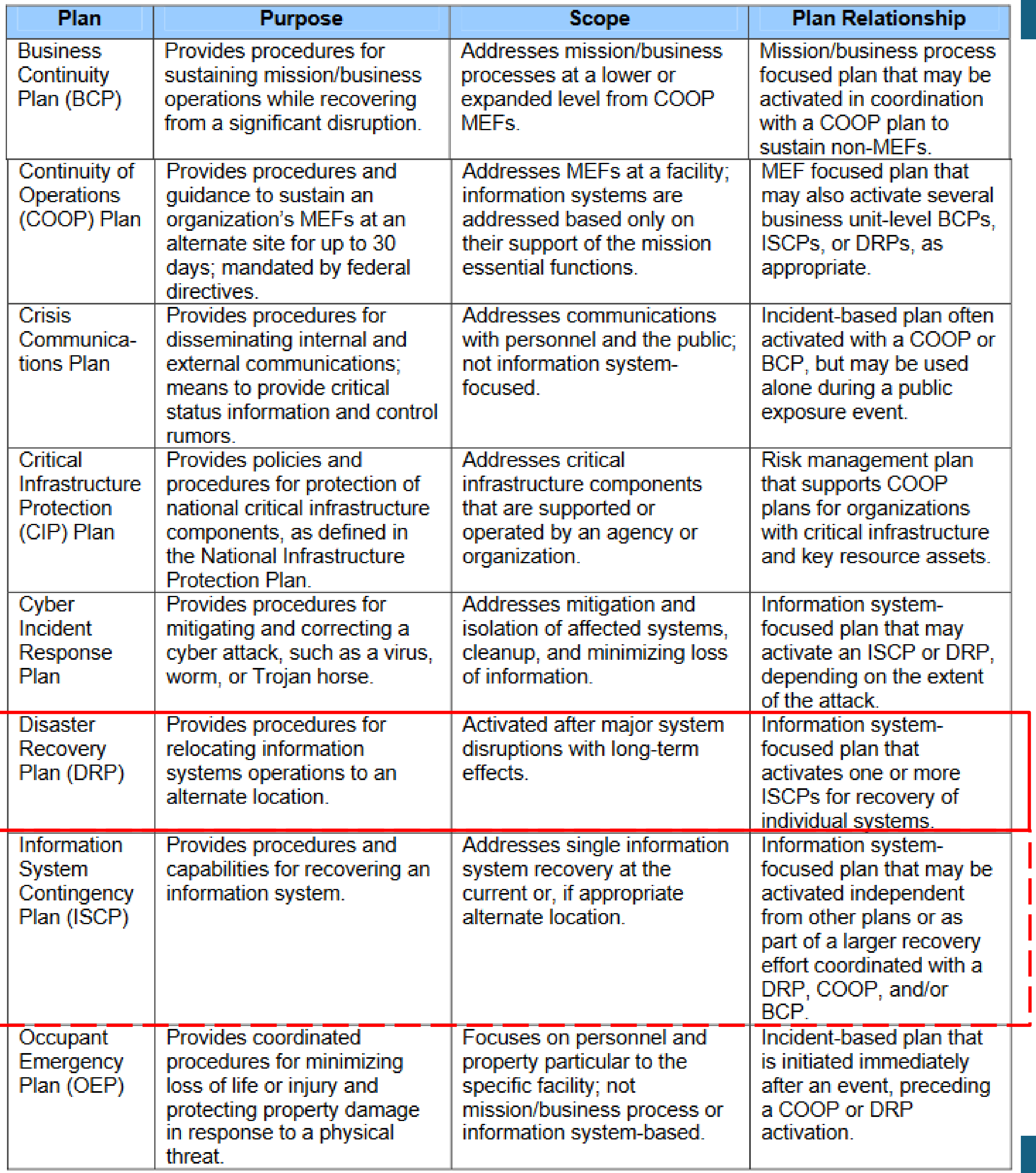
What Causes a Disaster?

- Physical damage to IT systems
  - E.g., fire, flood, or construction that severs upstream fiber
- Severe cyber attack
  - E.g., ransomware
- Hardware/software failure
  - E.g., CrowdStrike Falcon sensor update and BSOD on Windows on 2024-07-19
- Human error
  - E.g., Cloudflare 1.1.1.1 outage on 2025-07-14

NIST SP 800-34: Contingency Planning Guide for Federal Information Systems

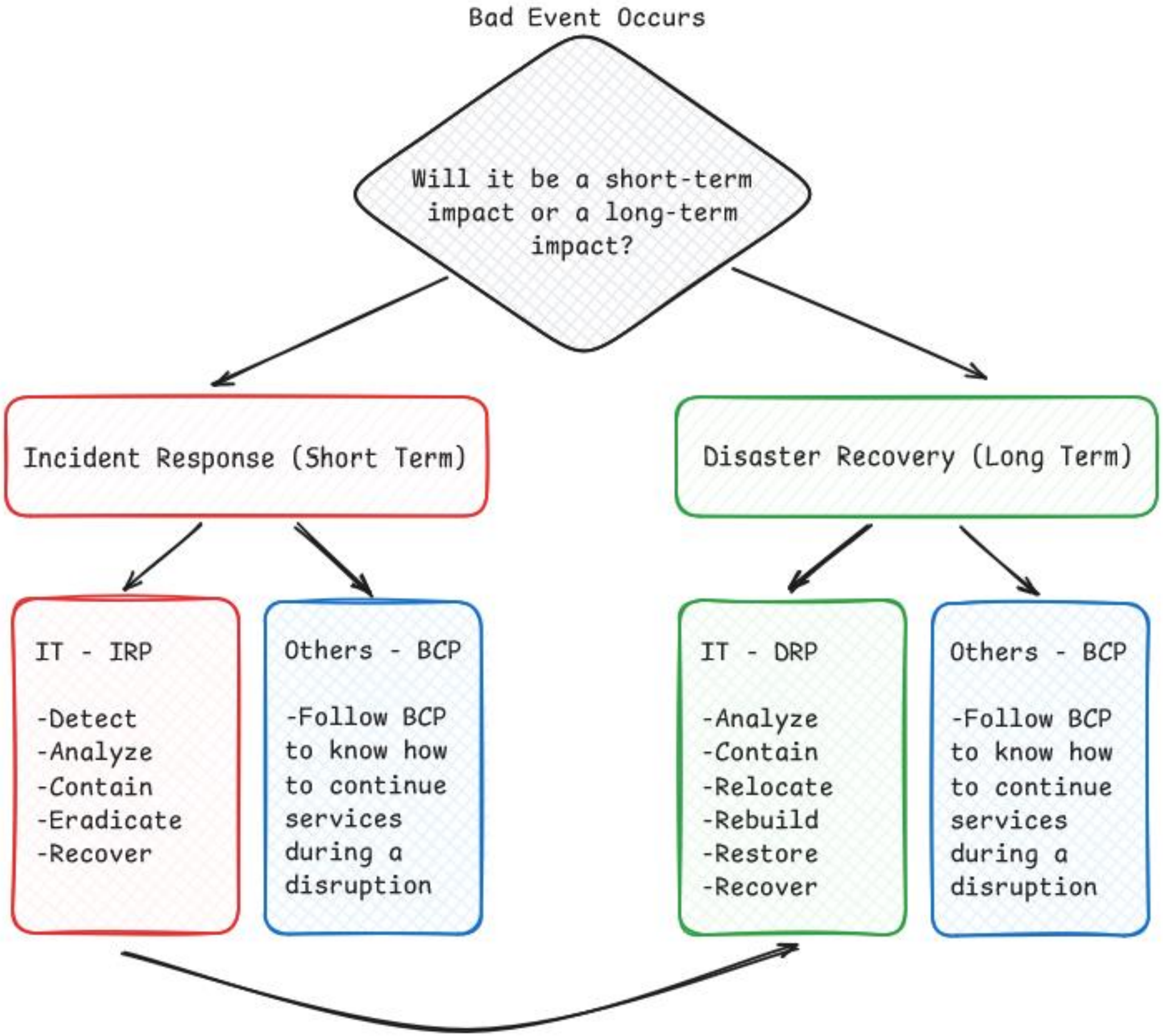
DRP

ISCP



Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

DR vs. IR vs. BC


Bad Event Occurs
Will it be a short-term impact or a long-term impact?
Incident Response (Short Term)
Disaster Recovery (Long Term)
IT - IRP
-Detect
-Analyze
-Contain
-Eradicate
-Recover
Others - BCP
-Follow BCP to know how to continue services during a disruption
IT - DRP
-Analyze
-Contain
-Relocate
-Rebuild
-Restore
-Recover
Others - BCP
-Follow BCP to know how to continue services during a disruption

Quest #1 - Complete!

- **Objective**: I will be able to explain the differences between a DRP, IRP, and BCP

- **Reward**: Mantle of Intelligence – Intelligence +1

Steps to Create a DRP

1 – Identify Attack Surface and Priorities

1.1 Conduct a Risk Assessment

1.2 Conduct a Business Impact Analysis (BIA)

1.3 Define Recovery Objectives

1.4 Map your infrastructure

2 – Develop Contingencies and Document them in a DRP

2.1 Select a Disaster Handling Lifecycle

2.2 Define roles and responsibilities for the disaster recovery team

2.3 Documents backup schedules

2.4 (Optional) identify alternative site capabilities and procedures

2.5 Document specific recovery steps for different systems (i.e., ISCPs)

3 - Distribute, Test, and Maintain the DRP

3.1 Train Stakeholders

3.2 Test the Plan

3.3 Update and Maintain the Plan

Step 1: Identify Attack Surface and Priorities

1.1 Conduct a Risk Assessment

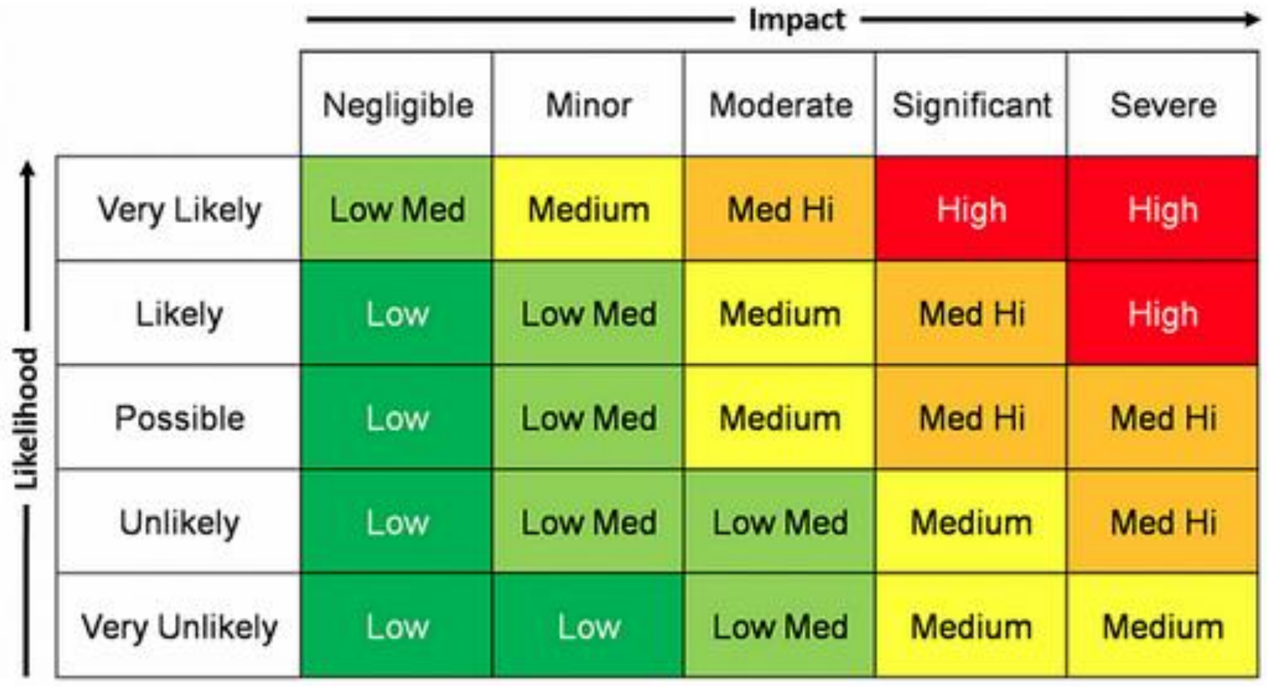
1.2 Conduct a Business Impact Analysis

1.3 Define Recovery Objectives

1.4 Map Your Infrastructure

1.1 - Conduct a Risk Assessment

- Risks help you define what could cause a disaster
- Risk = likelihood **X** impact of a threat
  1. Identify threats
  2. Identify likelihoods
  3. Identify impacts
  4. Document risks



Impact

Likelihood

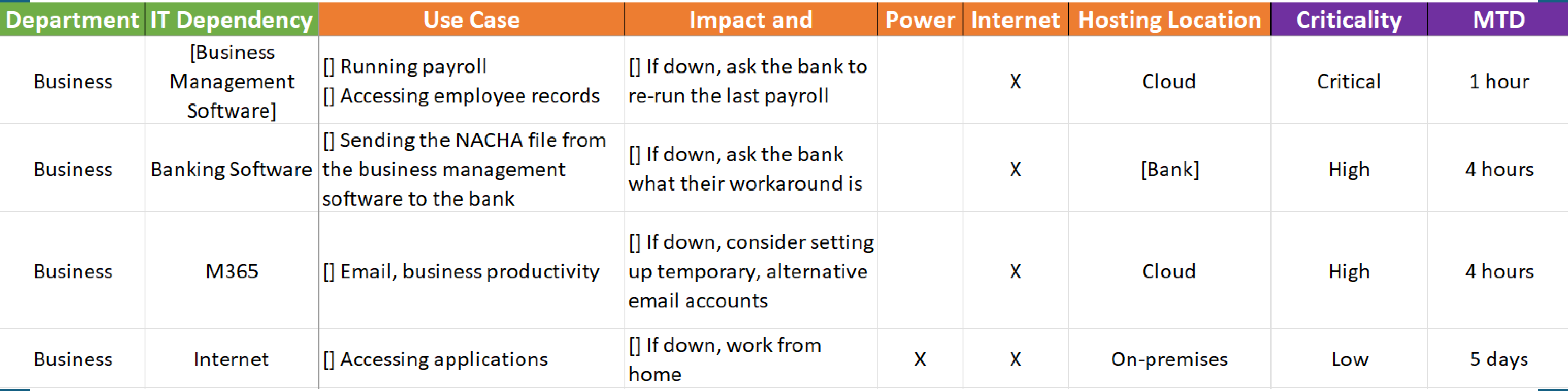
	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

1.2 - Conduct a Business Impact Analysis

- BIA = analysis of business functions and their IT dependencies
    1. Identify business functions
    2. Identify business function dependencies on IT
    3. Identify maximum tolerable downtime of IT dependencies
    4. Identify criticality of IT dependencies
- Stakeholders are *every* department
- Business functions may have temporal differences
- BIA becomes a BCP if you describe how to continue delivering services (i.e., “workarounds”) during a disruption to a dependency

BIA Example

- Department = Business Office
- Critical Function = Biweekly Payroll

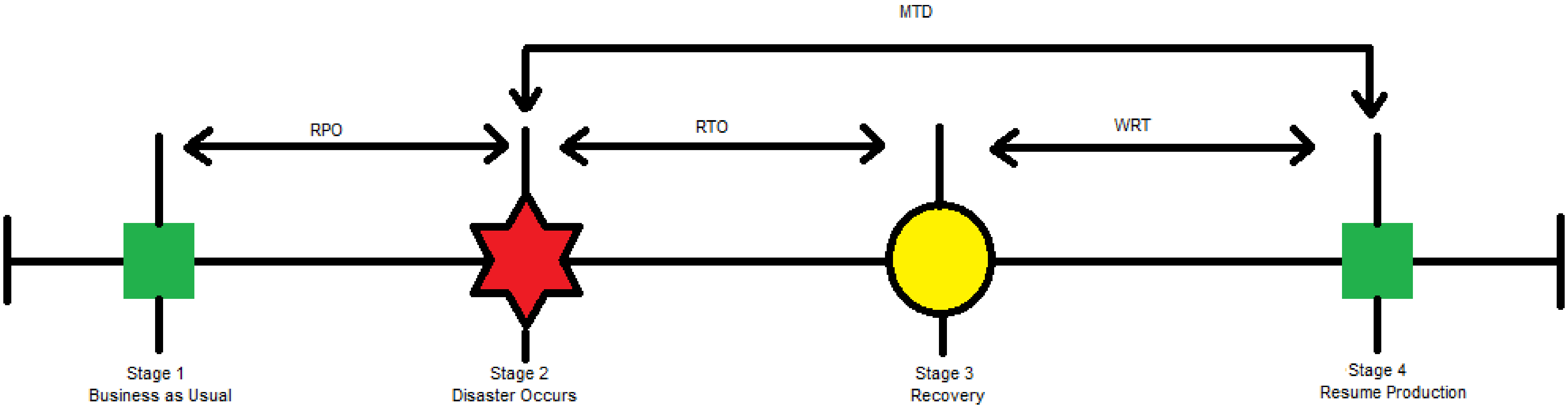


Department	IT Dependency	Use Case	Impact and	Power	Internet	Hosting Location	Criticality	MTD
Business	[Business Management Software]	[] Running payroll [] Accessing employee records	[] If down, ask the bank to re-run the last payroll		X	Cloud	Critical	1 hour
Business	Banking Software	[] Sending the NACHA file from the business management software to the bank	[] If down, ask the bank what their workaround is		X	[Bank]	High	4 hours
Business	M365	[] Email, business productivity	[] If down, consider setting up temporary, alternative email accounts		X	Cloud	High	4 hours
Business	Internet	[] Accessing applications	[] If down, work from home	X	X	On-premises	Low	5 days

1.3 - Define Recovery Objectives

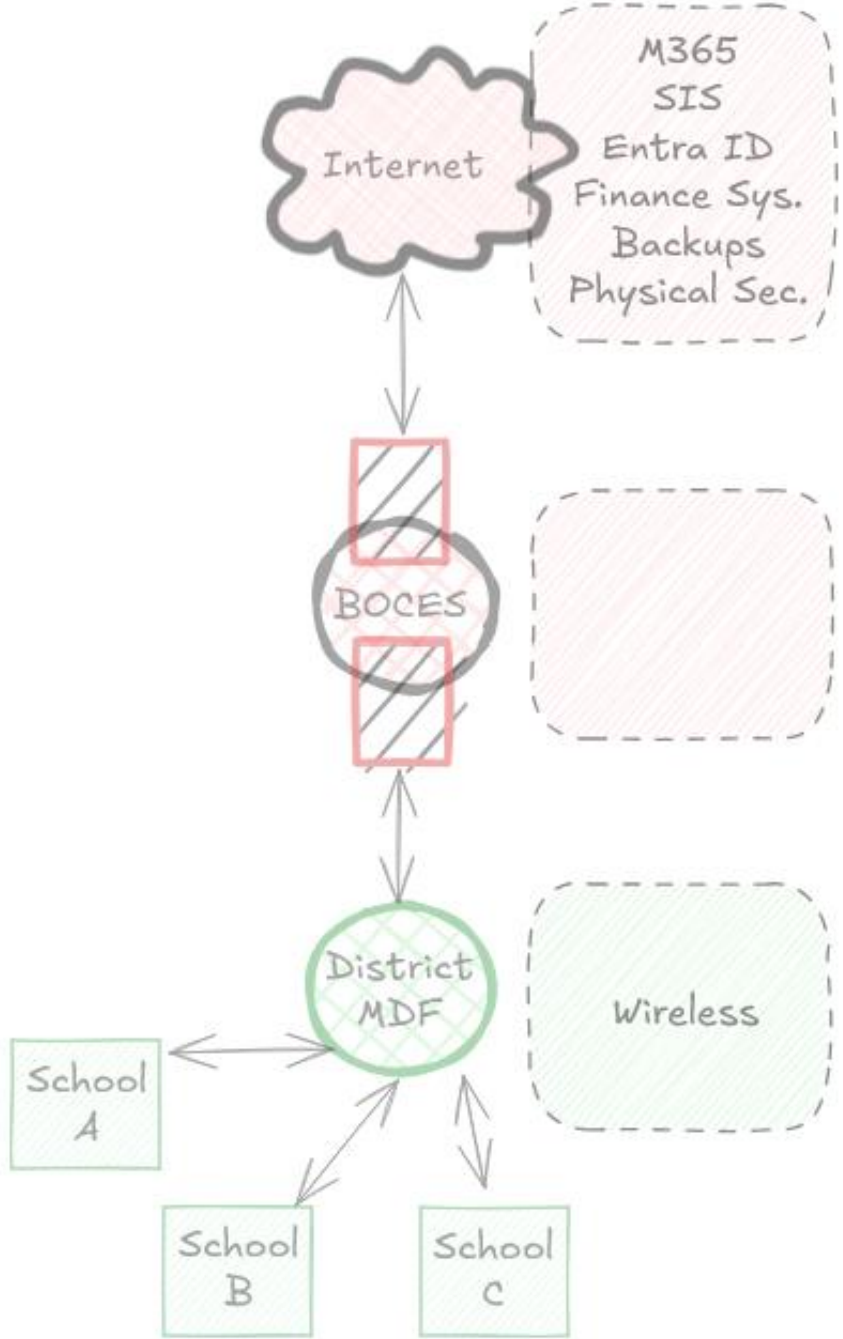
- RPO = how much data loss can you tolerate (as measured in time)?
- RTO = how long would it take to restore a system?
- WRT = how long would it take for users to start using a restored system?
- MTD = how long can you tolerate an outage?

RPO, RTO, WRT, and MTD



1.4 - Map Your Infrastructure

- What does a disaster look like you to?
- How is your network architected?
- What are your critical hardware/software assets?
- Where are they hosted?
- Where can you “break the chain,” and what would the impact be?

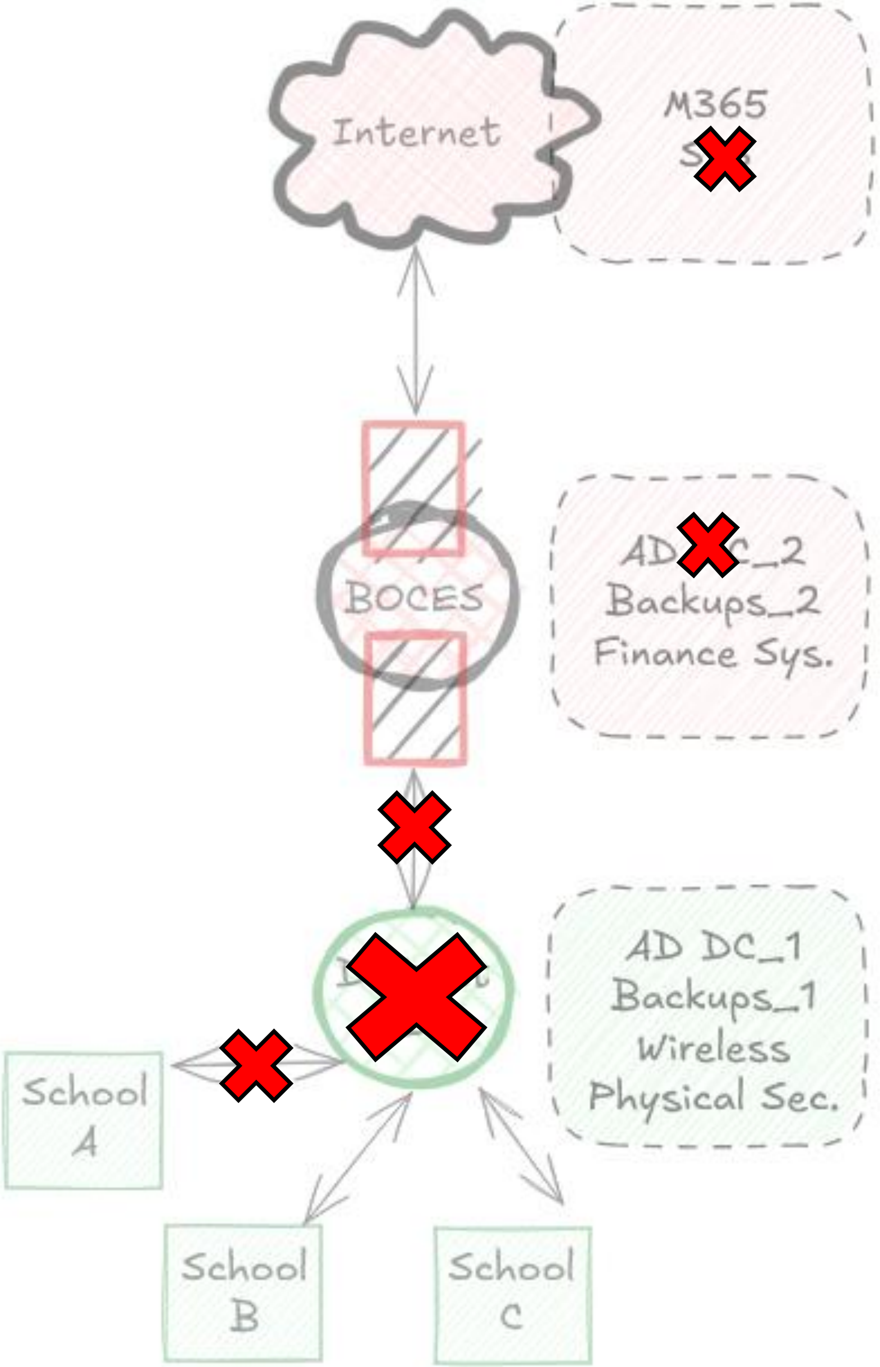


Example 1

- Traditional “hub and spoke”

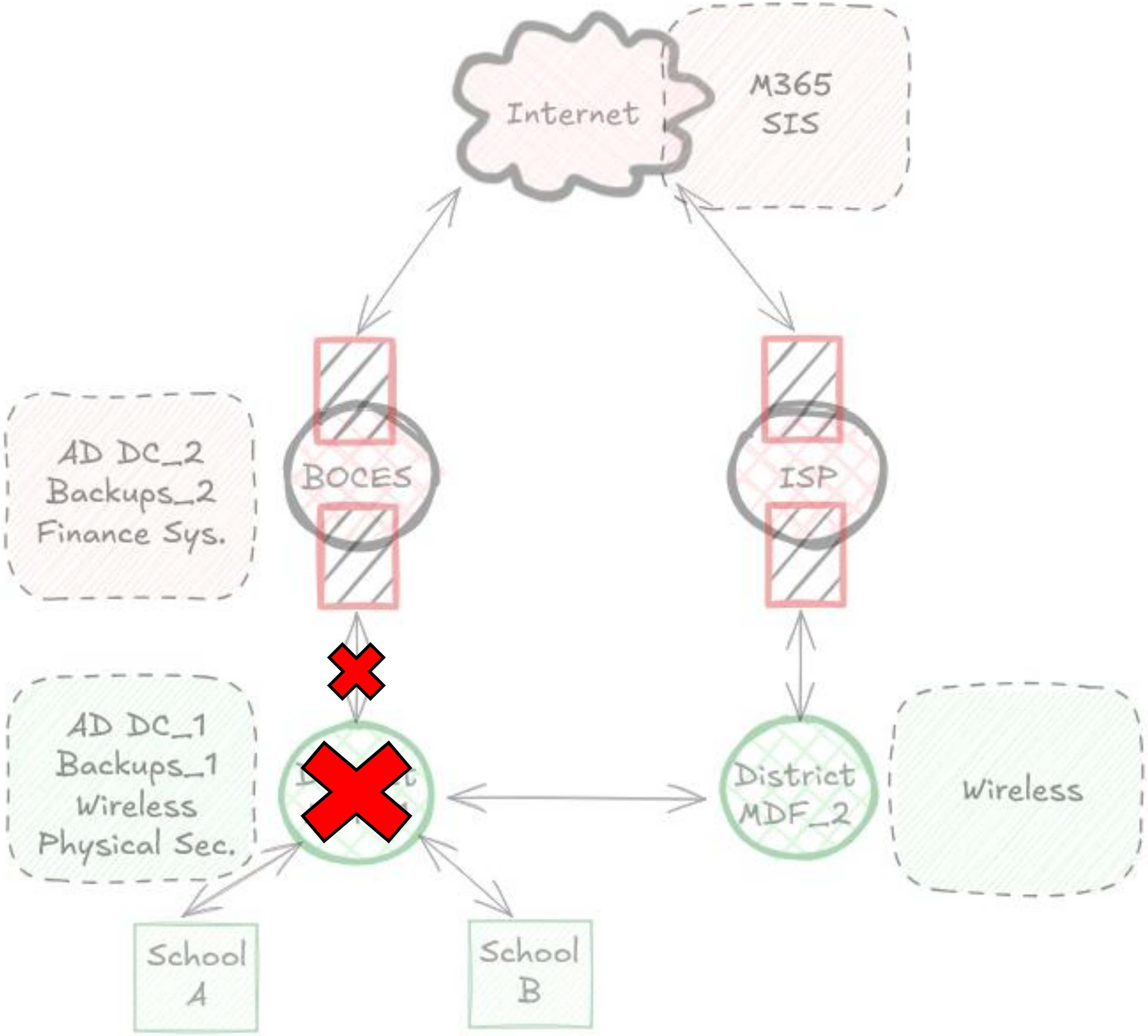
- LAN/WAN Fault Tolerance
  - North-South = none
  - East-West = none

- Applications Fault Tolerance
  - Minimal



Example 2

- Semi “hub and spoke”
- LAN/WAN Fault Tolerance
  - North-South = some
  - East-West = none
- Applications Fault Tolerance
  - Minimal

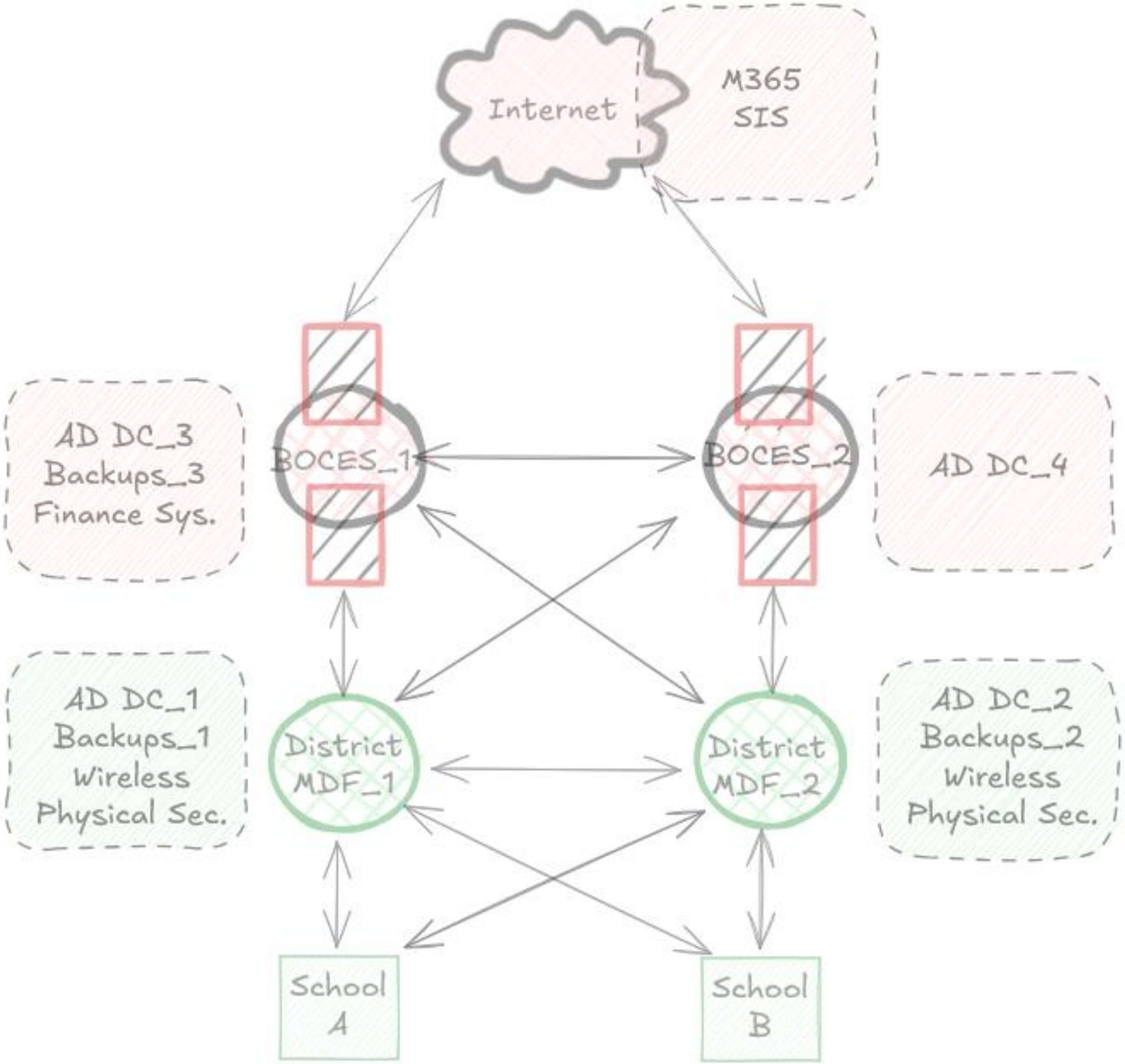


Example 3

- Mesh

- LAN/WAN Fault Tolerance
    - North-South = full
    - East-West = full

- Applications Fault Tolerance
    - Moderate/full



Quest #2 - Complete!

- **Objective**: I will be able to follow the steps to create a DRP:
  a) **Identify Attack Surface and Priorities**
  ~~b) Develop Contingencies and Document them in a DRP~~
  ~~c) Distribute, Test, and Maintain the DRP~~

- **Reward**: Staff of Wizardry – Intelligence +2

Step 2: Develop Contingencies and Document them in a DRP

- Include the essential elements of your risk assessment, BIA, recovery priorities, and your infrastructure map

2.1 Select a Disaster Handling Lifecycle

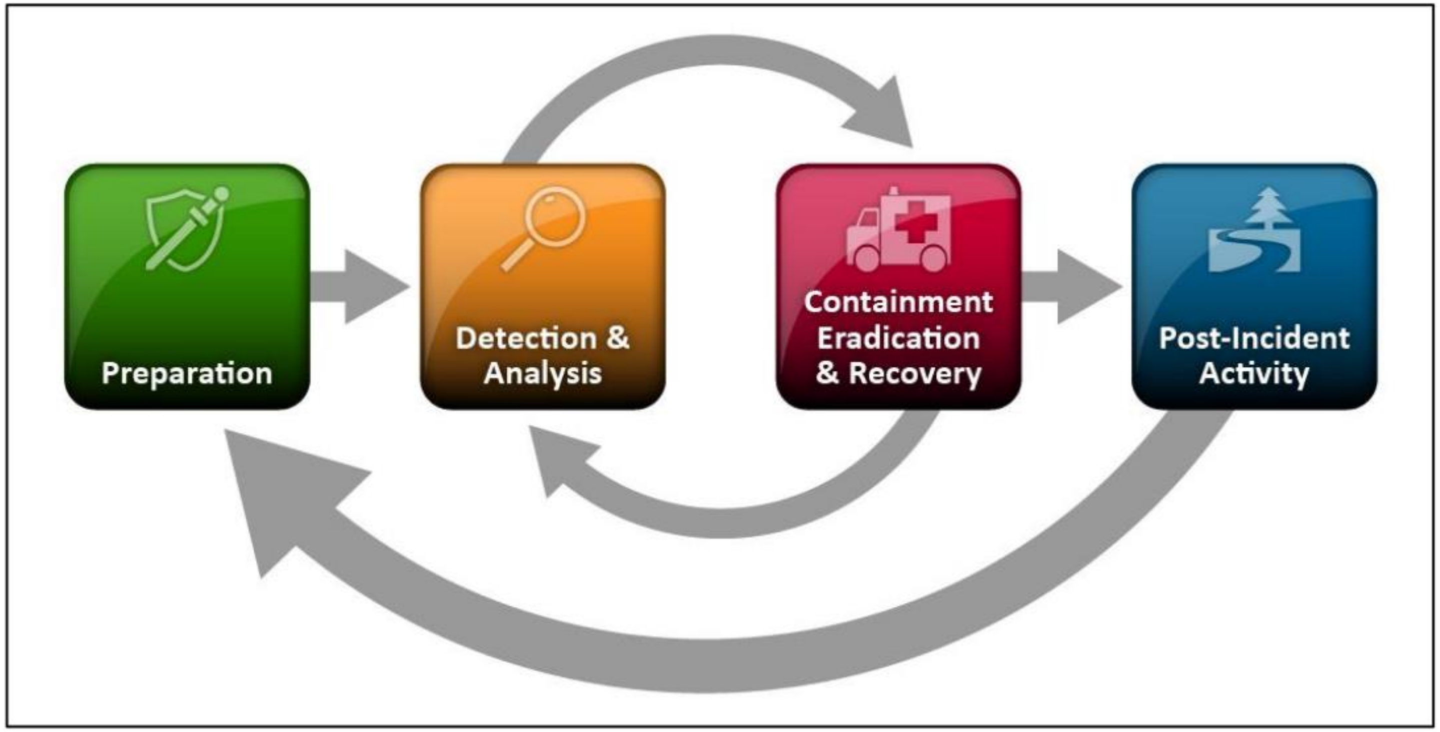
2.2 Define roles and responsibilities for the disaster recovery team

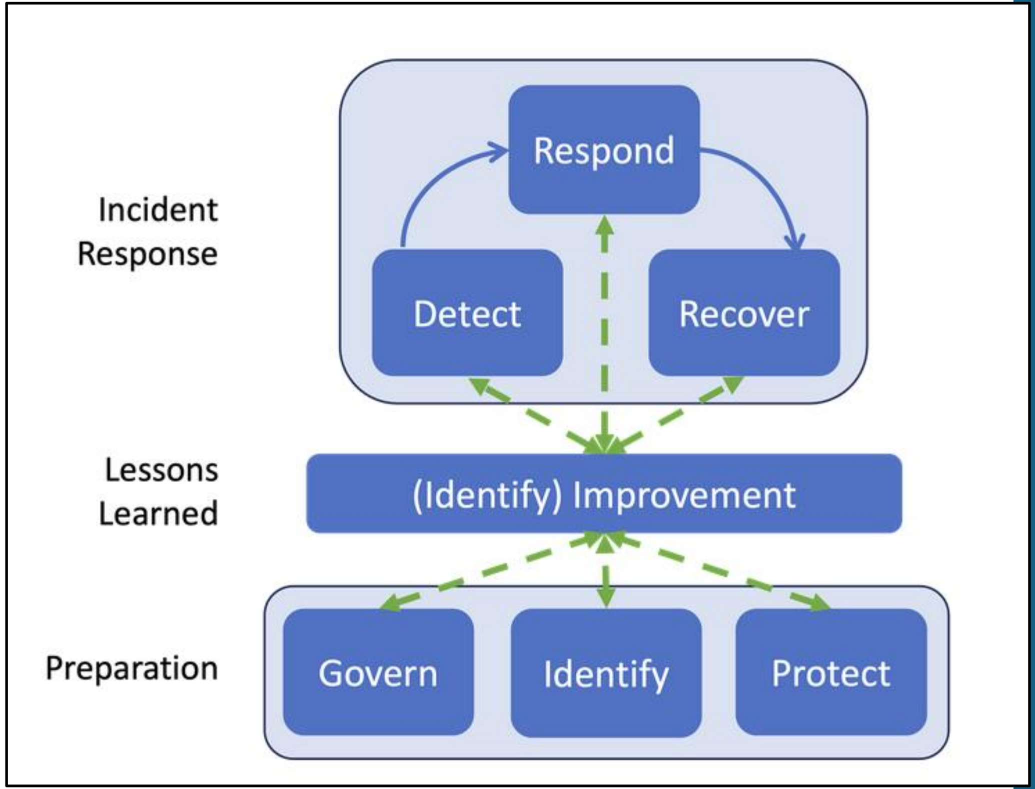
2.3 Document backup schedules

2.4 (Optional) Identify alternative site capabilities and procedures

2.5 Document specific recovery steps for different systems (ISCPs)

2.1 - Select a Disaster Handling Lifecycle





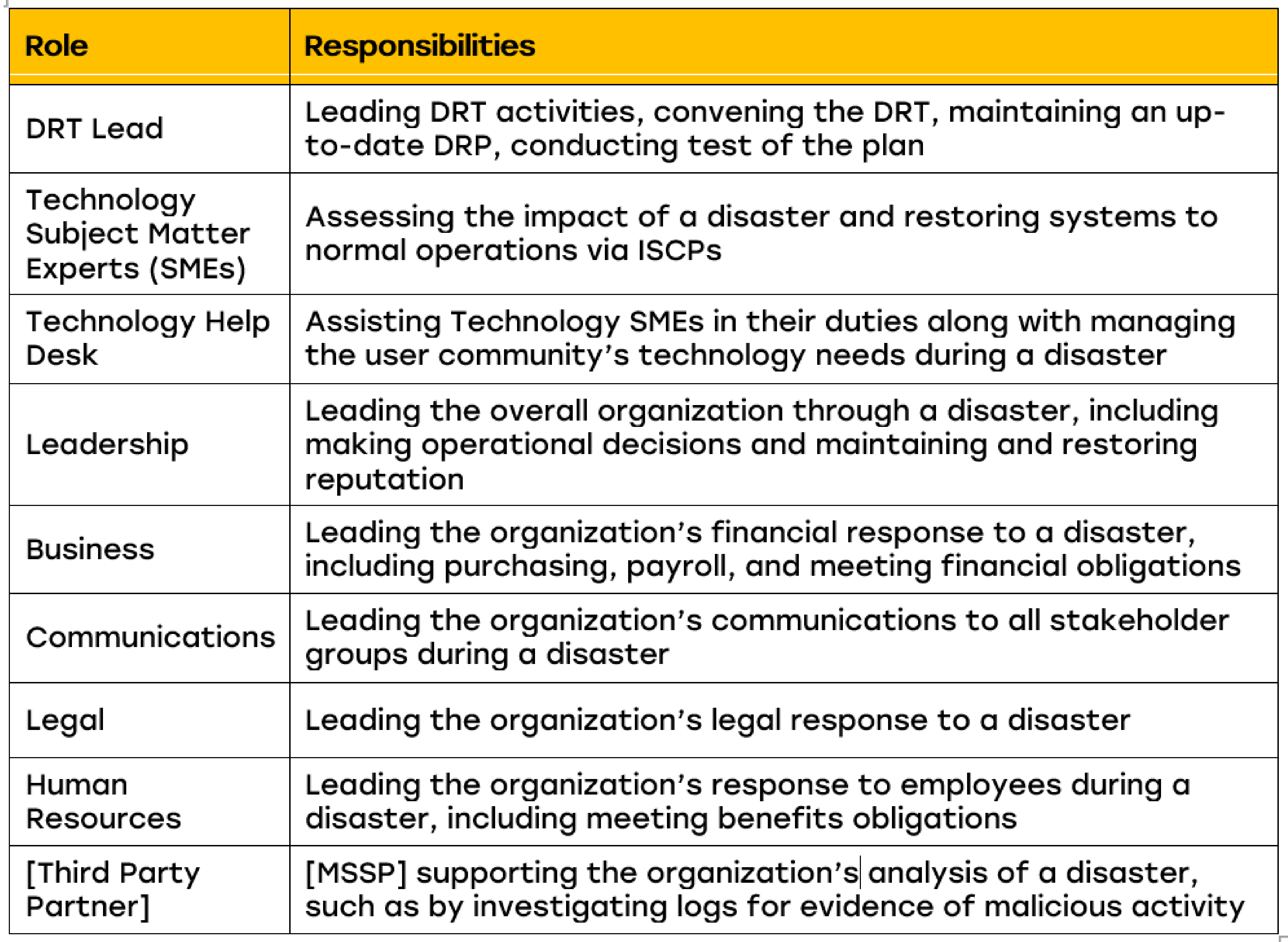
NIST 800-61 Rev.2 (2012)

NIST 800-61 Rev.3 (2025)

Disaster Handling Lifecycle

- Analyze - determine the scope, cause, and impact
- (Contain) - optional - if needed, contain the harm such as putting out the fire in the data center or invoking the IRP for a ransomware scenario before you rebuild/restore your encrypted systems
- (Relocate) - optional - if needed, activate your hot/warm/cold site
- Rebuild - deploy new systems to replace those that were damaged
- Restore - bring rebuilt systems up-to-date with the latest backups
- Recover - put rebuilt and restored systems back into operation for use

2.2 - Define Roles & Responsibilities for the DRT



Role	Responsibilities
DRT Lead	Leading DRT activities, convening the DRT, maintaining an up-to-date DRP, conducting test of the plan
Technology Subject Matter Experts (SMEs)	Assessing the impact of a disaster and restoring systems to normal operations via ISCPs
Technology Help Desk	Assisting Technology SMEs in their duties along with managing the user community’s technology needs during a disaster
Leadership	Leading the overall organization through a disaster, including making operational decisions and maintaining and restoring reputation
Business	Leading the organization’s financial response to a disaster, including purchasing, payroll, and meeting financial obligations
Communications	Leading the organization’s communications to all stakeholder groups during a disaster
Legal	Leading the organization’s legal response to a disaster
Human Resources	Leading the organization’s response to employees during a disaster, including meeting benefits obligations
[Third Party Partner]	[MSSP] supporting the organization’s analysis of a disaster, such as by investigating logs for evidence of malicious activity

2.3 - Document Backup Schedules

- What systems are backed up?
- How often do backups occur?
- Where are backups stored?

Application	Application Location	Backup Solution	Backup Schedule	Backup Location – On-prem	Backup Replication - BOCES	Backup Replication 2 - Cloud	Backup Retention
VM_1	VMWare (on-premises)	Veeam (on-premises)	1.) Daily incrementals between 7:00 – 9:00 p.m. 2.) Weekly full backup on Saturdays at 7:00 p.m.	Daily Full	Full	Full	1.) Incremental – 1 week 2.) Full – 3 months

Backup and Restoration Best Practices

- Maintain backups for all critical systems
- 3-2-1 method
- Take backups as often as your RPO requires
- Test backups to have a low RTO
- Retain backups for as long as legal or business needs require
- Consider WORM, immutability, and air-gapped solutions

2.4 - (Optional) Activate Alternative Site

- Key Question – what would you do if your MDF was destroyed?

- Hot Site – live, mirrored systems and data between primary and secondary site
- Warm Site – most systems mirrored between primary and secondary site, but requires some system setup and data restoration
- Cold Site – secondary site with no systems or data

2.5 - Recovery Playbooks (ISCP)

- Document specific recovery steps for critical IT services (e.g., DC, core switch, database)
  - Who would do the work?
  - Is the system a SPOF or are their redundancies/spares in place?
  - What step-by-step actions are needed to rebuild, restore, and recover the system?
- Systems are typically recovered in order:
  - Networking (routing, switching, DNS, DHCP)
  - Identity, Authentication, and Authorization
  - Applications

Quest #3 - Complete!

- **Objective**: I will be able to follow the steps to create a DRP:
  a) Identify Attack Surface and Priorities
  b) Develop Contingencies and Document them in a DRP
  ~~c) Distribute, Test, and Maintain the DRP~~

- **Reward**: Ring of Protection – Defense +5

Step 3: Distribute, Test, and Maintain the Plan

3.1 Train Stakeholders

3.2 Test the Plan

3.3 Update and Maintain the Plan

3.1 - Train Stakeholders

- All DRT member should know, at minimum:
  - Where copies of the DRP are
  - What their responsibilities are
  - How to get ahold of each other
- Other stakeholders should know:
  - Where copies of the BCP are
  - What their responsibilities are
  - How to get ahold of the DRT coordinator

3.2 - Test the Plan

- TTX
  - Dialogic, scenario-based exercise with DRT members
  - Easiest to conduct
- Isolated Functional Test
  - Simulated disruption to a particular service
  - Moderately difficult to conduct
- Full Scale Functional Test
  - Full-scale simulated disruption to services
  - Most difficult to conduct

3.3 - Update and Maintain the Plan

- Review the plan at least annually
- Consider:
  - Have my risks changed?
  - Are new business functions being conducted?
  - Has my technology stack changed?
  - Have team members changed?

Quest #4 - Complete!

- **Objective**: I will be able to follow the steps to create a DRP:
  a) Identify Attack Surface and Priorities
  b) Develop Contingencies and Document them in a DRP
  c) Distribute, Test, and Maintain the DRP

- **Reward**: Boots of Speed – Endurance +3

DRP Project Plan

Week	Topic	Stakeholders	Evidence
1	Overview of DR goals	Leadership IT	
2	Risk assessment	IT	Risk assessment
3	Risk assessment	IT	Risk assessment
4	BIA	Various departments	BIA
5	BIA	Various departments	BIA
6	BIA	Various departments	BIA
7	Map your infrastructure	IT	Network map
8	DRP – DRT role and responsibilities	IT	
9	DRP – backup schedule	IT	Backup Schedule
10	DRP – ISCP	IT	ISCP
11	DRP – ISCP	IT	ISCP
12	DRP - ISCP	IT	ISCP
13	DRP - communication templates, alternative site operations, etc.	IT	
14	Test DRP with a Tabletop Exercise (TTX)	DRT	DRP
15	Final review	Leadership Technology	DRP

DRP Template

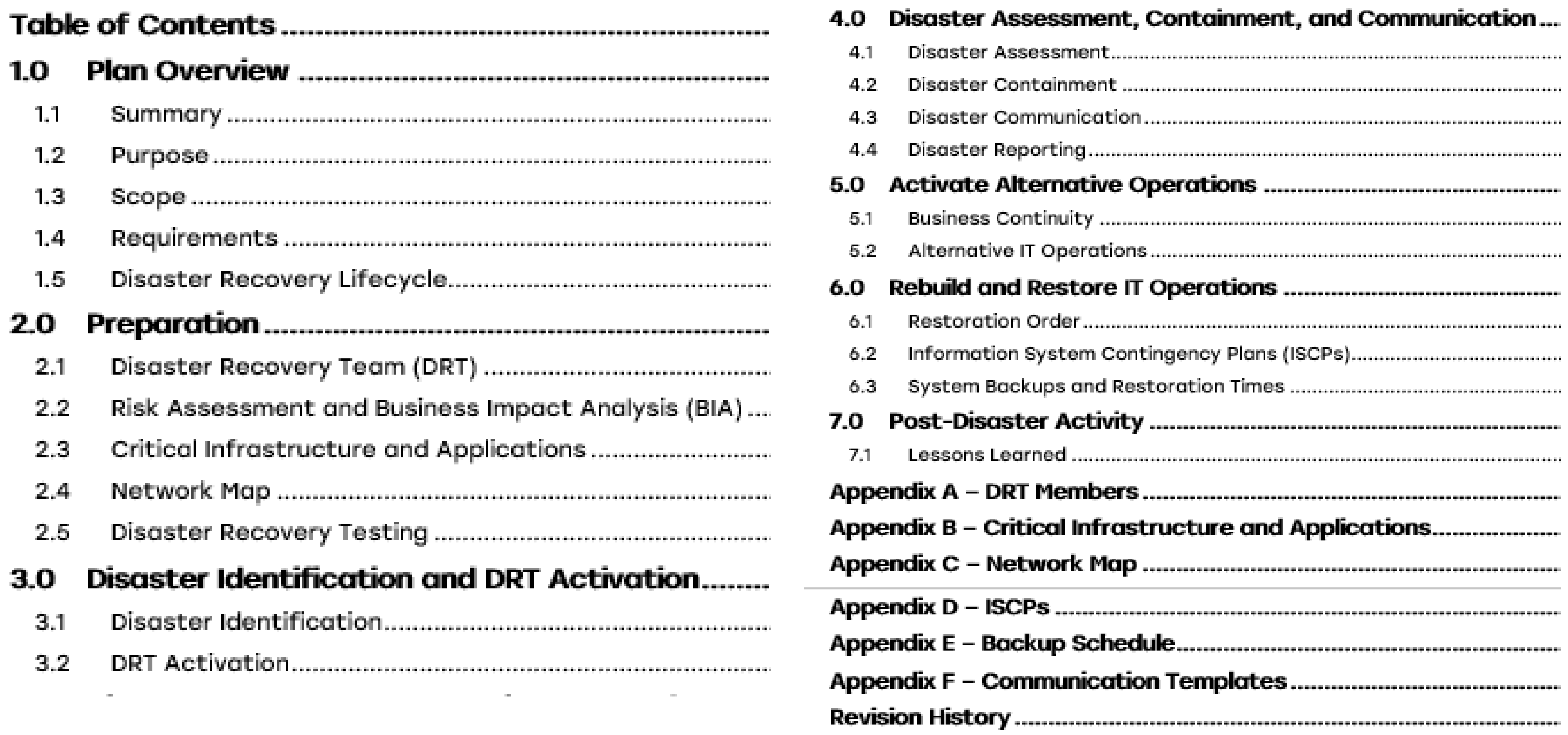
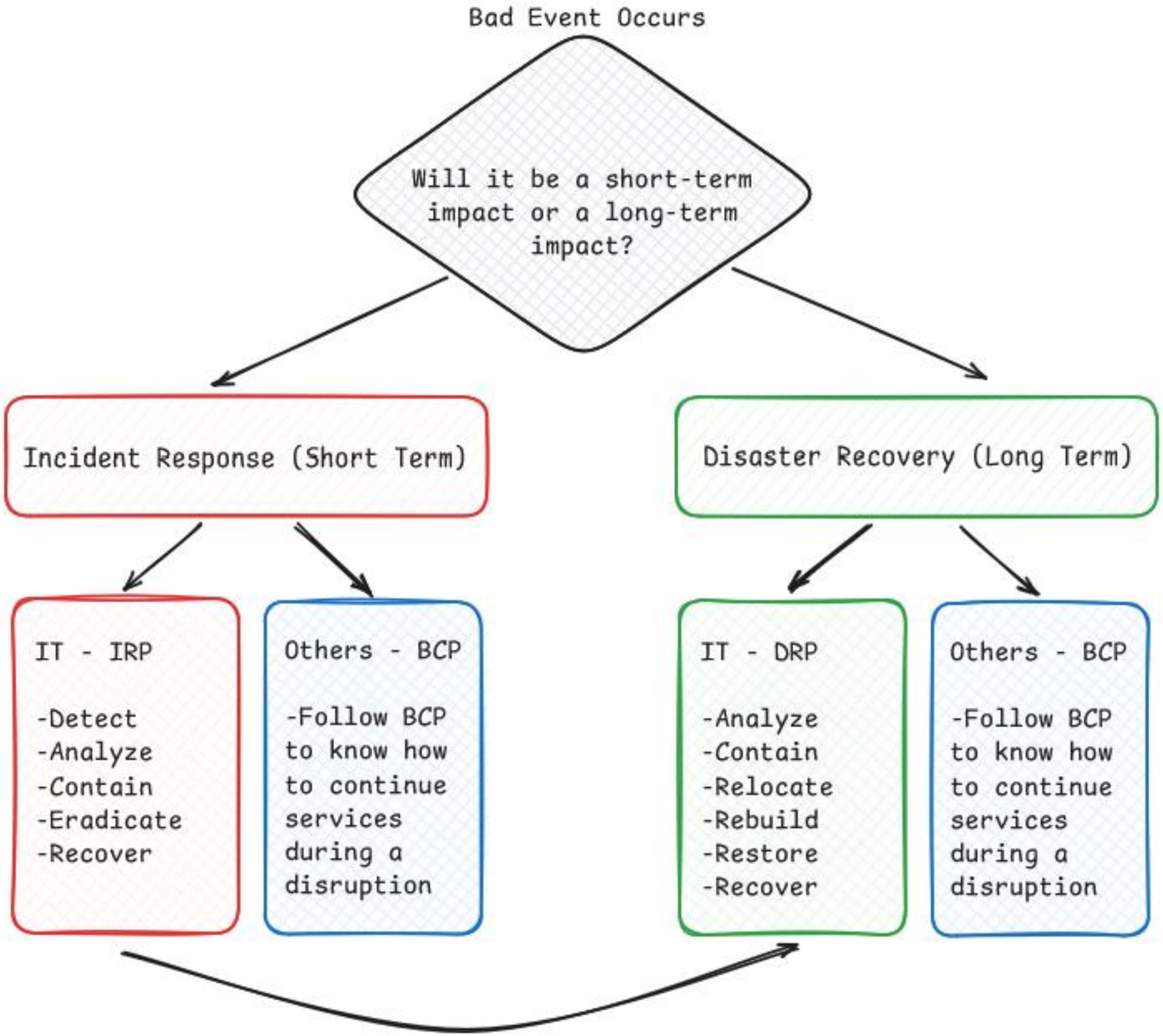


Table of Contents

LEVEL UP!

DR vs. IR vs. BC



Bad Event Occurs

Will it be a short-term impact or a long-term impact?

Incident Response (Short Term)

Disaster Recovery (Long Term)

IT - IRP

- -Detect
- -Analyze
- -Contain
- -Eradicate
- -Recover

Others - BCP

-Follow BCP to know how to continue services during a disruption

IT - DRP

- -Analyze
- -Contain
- -Relocate
- -Rebuild
- -Restore
- -Recover

Others - BCP

-Follow BCP to know how to continue services during a disruption

Steps to Create a DRP

1 – Identify Attack Surface and Priorities

- 1.1 Conduct a Risk Assessment
- 1.2 Conduct a Business Impact Analysis (BIA)
- 1.3 Define Recovery Objectives
- 1.4 Map your infrastructure

2 – Develop Contingencies and Document them in a DRP

- 2.1 Select a Disaster Handling Lifecycle
- 2.2 Define roles and responsibilities for the disaster recovery team
- 2.3 Documents backup schedules
- 2.4 (Optional) identify alternative site capabilities and procedures
- 2.5 Document specific recovery steps for different systems (i.e., ISCPs)

3 - Distribute, Test, and Maintain the DRP

- 3.1 Train Stakeholders
- 3.2 Test the Plan
- 3.3 Update and Maintain the Plan