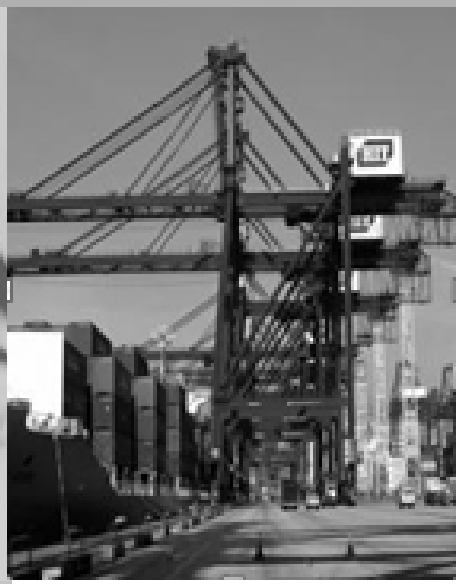
กลยุทธ์บริหารจัดการการดำเนินองค์กรอย่างต่อเนื่องในภาวะวิกฤต

ดร. รวินกานต์ ศรีนนท์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยหอการค้าไทย



Types of Contingency Plans

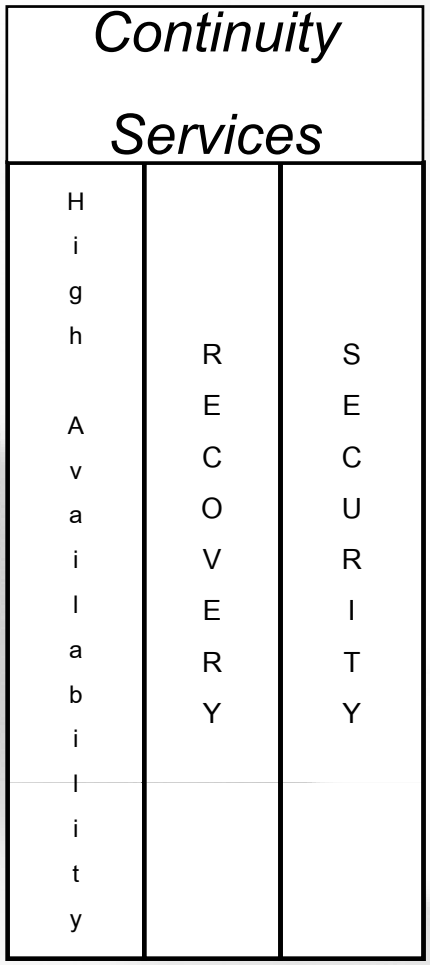
Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed only in the context of supporting business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused
Continuity of Operations Plan	Establish procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses subset of an organization's missions deemed critical; not IT-focused
Continuity of Support Plan	Establish procedures and capabilities for recovering a major application or general support system	Similar to IT contingency plan; addresses IT system disruption; not business process focused
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Incident Response Plan	Define strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Occupant Emergency Plan	Provide 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 business- or IT-focused

http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf

What is Business Continuity?

- *Business continuity describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster.*
- *Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.*

What is Business Continuity?



- Simply put, it's the means of keeping an organization up and running 24 x 7 despite any expected or unexpected disruption.
- May involve highly available, "always on" infrastructures that make traditional recovery obsolete
- May involve traditional disaster recovery services, i.e. hot/cold site, data backup, mobile recovery, contingency planning (reactive approach) OR
- May involve security services (proactive approach)

What is Disaster Recovery?

- *Disaster recovery describes how an organization is to deal with potential disasters. A disaster recovery plan (DRP) consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions.*

7-Step Process

- Review/refresh or develop security, disaster recovery, and BC plans
- Develop contingency planning policy
- Conduct business impact analysis (BIA)
- Identify preventative controls
- Develop recovery strategies
- Develop contingency plan
- Plan testing, training and simulations
- Maintain the plan

Business Impact Analysis

- Which business processes are of strategic importance?
- What disasters could occur?
- What impact would they have on the organization financially? On human life? On reputation?
- What is the required recovery time period?

Event Damage Classification

- **Negligible:** No significant damage
- **Minor:** A non-negligible event with no material or financial impact on the business
- **Major:** Impacts one or more departments and may impact outside clients
- **Crisis:** Has a major material impact on the organization
- **Minor, Major, & Crisis events should be documented and tracked to repair**

Workbook: Disasters and Impact

Problematic Event or Disaster	Affected Business Process(es) (Assumes a university)	Impact Classification & Effect on finances, legal liability, human life, reputation
Fire	Class rooms, business departments	Crisis, at times Major, Human life
Hacking Attack	Registration, advising,	Major, Legal liability
Network Unavailable	Registration, advising, classes, homework, education	Crisis
Server Failure (Disk/server)	Registration, advising, classes, homework, education.	Major, at times: Crisis

Workbook: Disasters and Impact

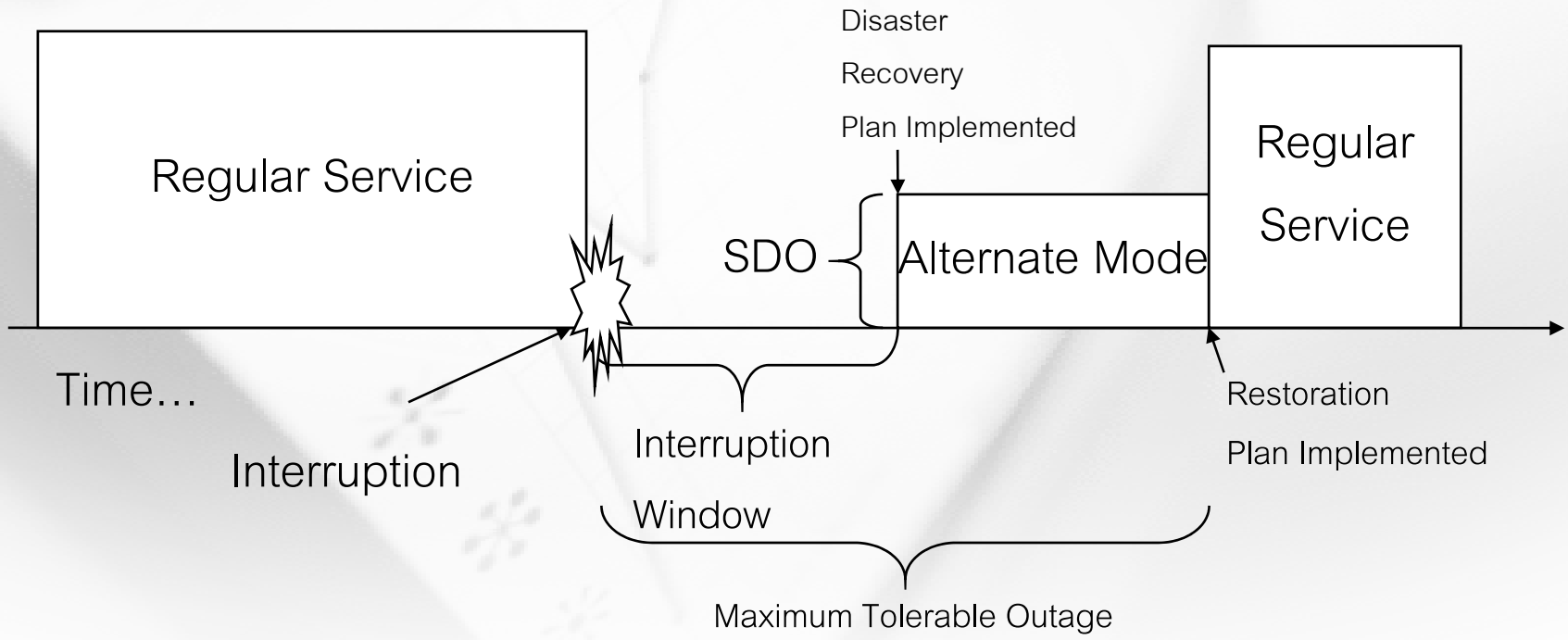
Problematic Event or Disaster	Affected Business Process(es) (Assumes a medical warehouse)	Impact Classification & Effect on finances, legal liability, human life, reputation
Warehouse is flooded	Damaged goods	Crisis
Staff houses are affected by flood	Not enough staff	Major
Road interrupted	Transportation	Major

Recovery Time: Terms

Interruption Window: Time duration organization can wait between point of failure and service resumption

Service Delivery Objective (SDO): Level of service in Alternate Mode

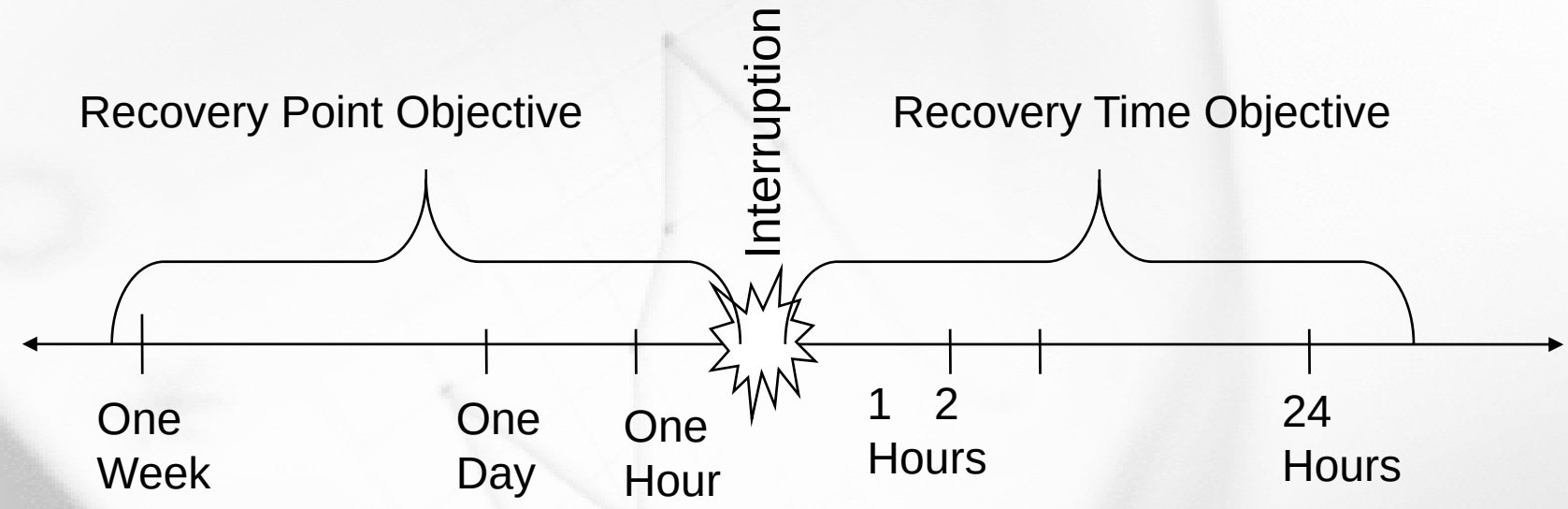
Maximum Tolerable Outage: Max time in Alternate Mode



Definitions

- Business Continuity: Offer critical services in event of disruption
- Disaster Recovery: Survive interruption to computer information systems or Personal Interruption
- Alternate Process Mode: Service offered by backup system
- Disaster Recovery Plan (DRP): How to transition to Alternate Process Mode
- Restoration Plan: How to return to regular system mode

RPO and RTO



How far back can you fail to?

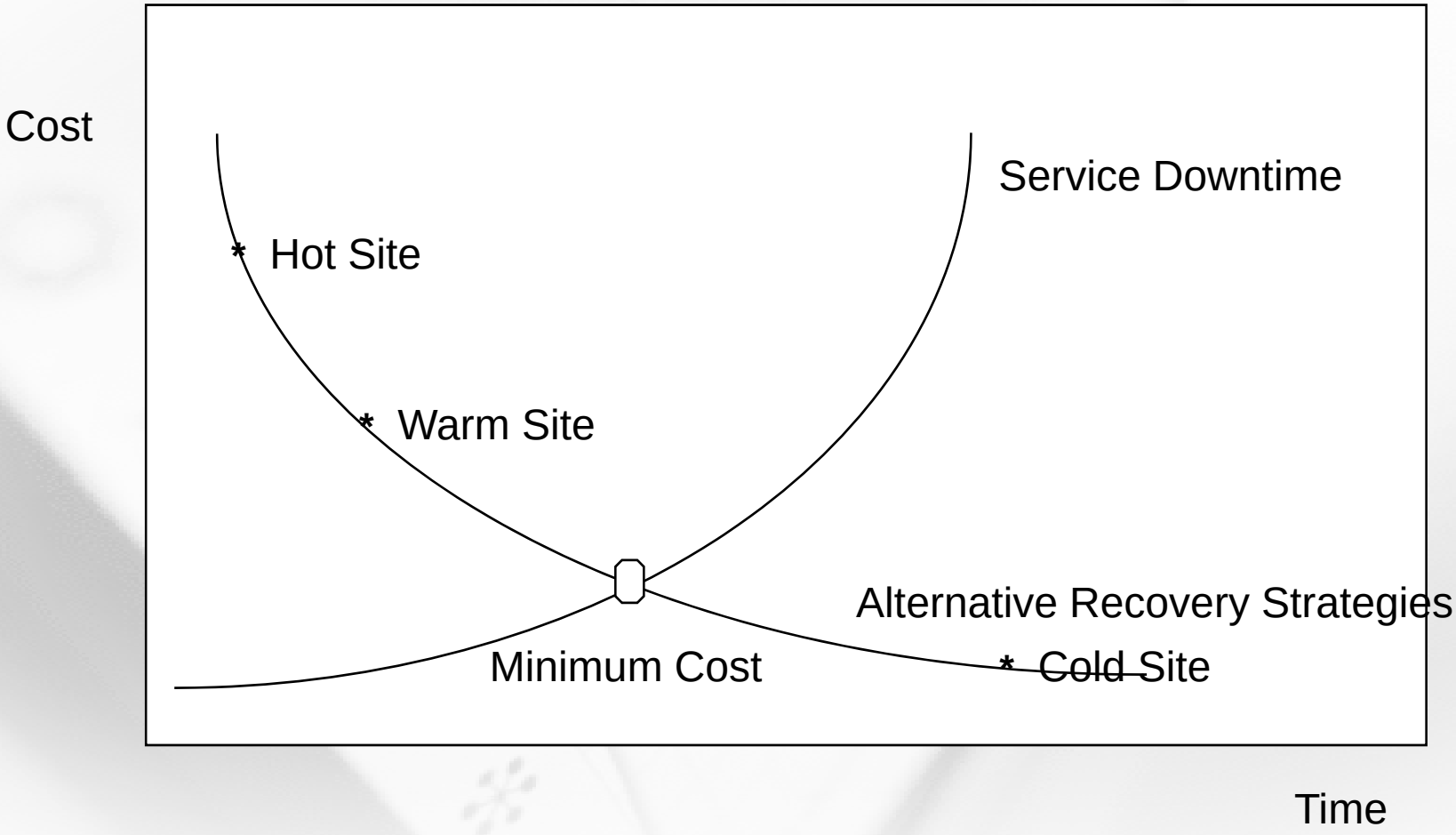
How long can you operate without a system?
Which services can last how long?

Business Impact Analysis Summary

Work Book

Service	Recovery Time Objective (Hours)	Recovery Point Objective (Hours)	Critical Resources (Computer, people, peripherals)	Special Notes (Unusual treatment at Specific times, unusual risk conditions)
Registration	4 hours	0 hours	SOLAR, network Registrar	High priority during Nov-Jan, March-June, August.
Personnel	8 hours	2 hours	PeopleSoft	Can operate manually for some time
Teaching	1 hour	1 day	D2L, network, faculty files	During school semester: high priority.

Disruption vs. Recovery Costs



Alternative Recovery Strategies

Hot Site: Fully configured, ready to operate within hours

Warm Site: Ready to operate within days

Cold Site: Ready to operate within weeks.

Duplicate or Redundant Info. Processing Facility: Standby hot site within the organization

Reciprocal Agreement with another organization or division

Mobile Site: Fully- or partially-configured trailer comes to your site

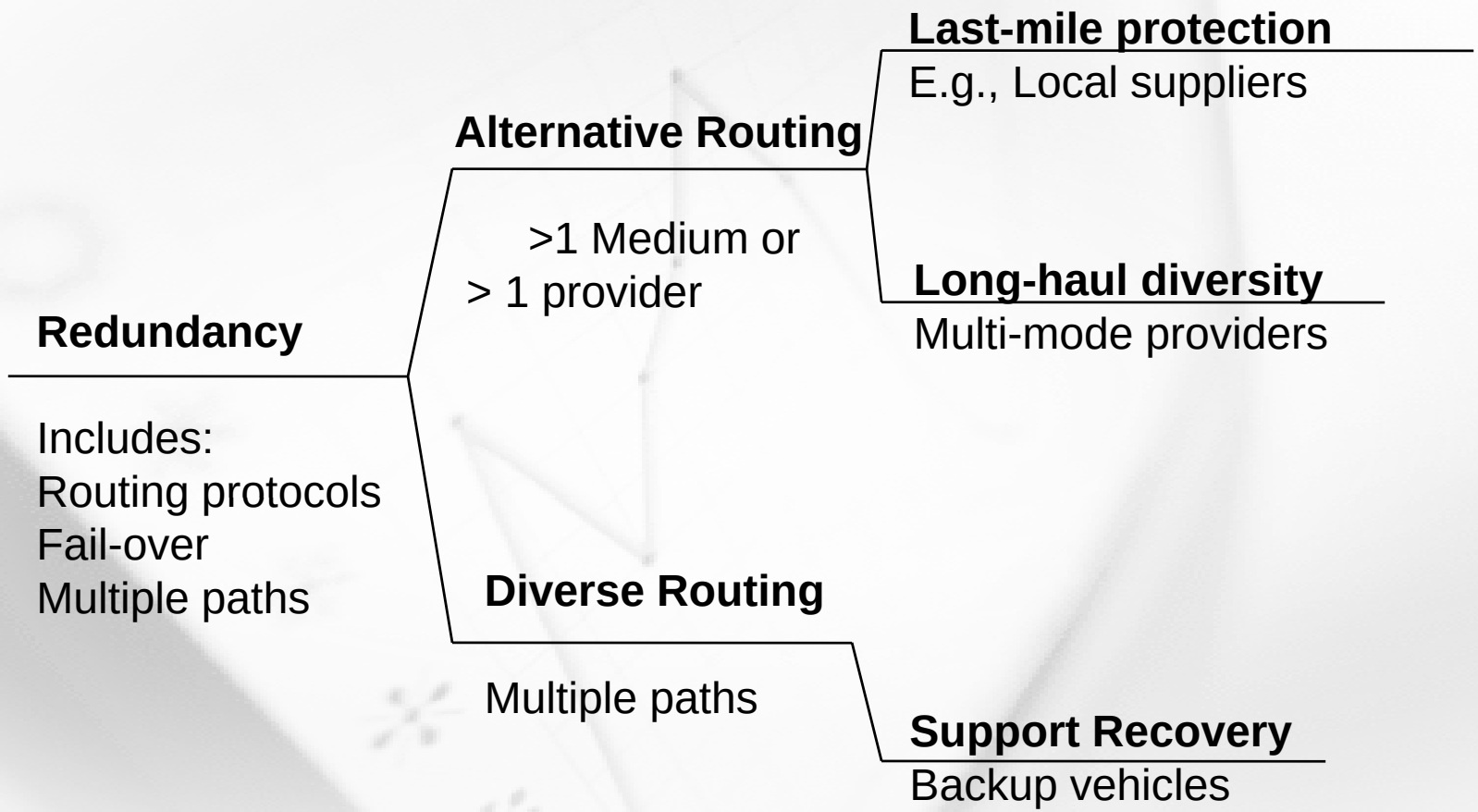
Hot Site

- Contractual costs include: monthly fee, and other costs
- Contractual issues include: speed of access, configurations, staff assistance
- Hot site is for emergency use – not long term
- May offer warm or cold site for extended durations

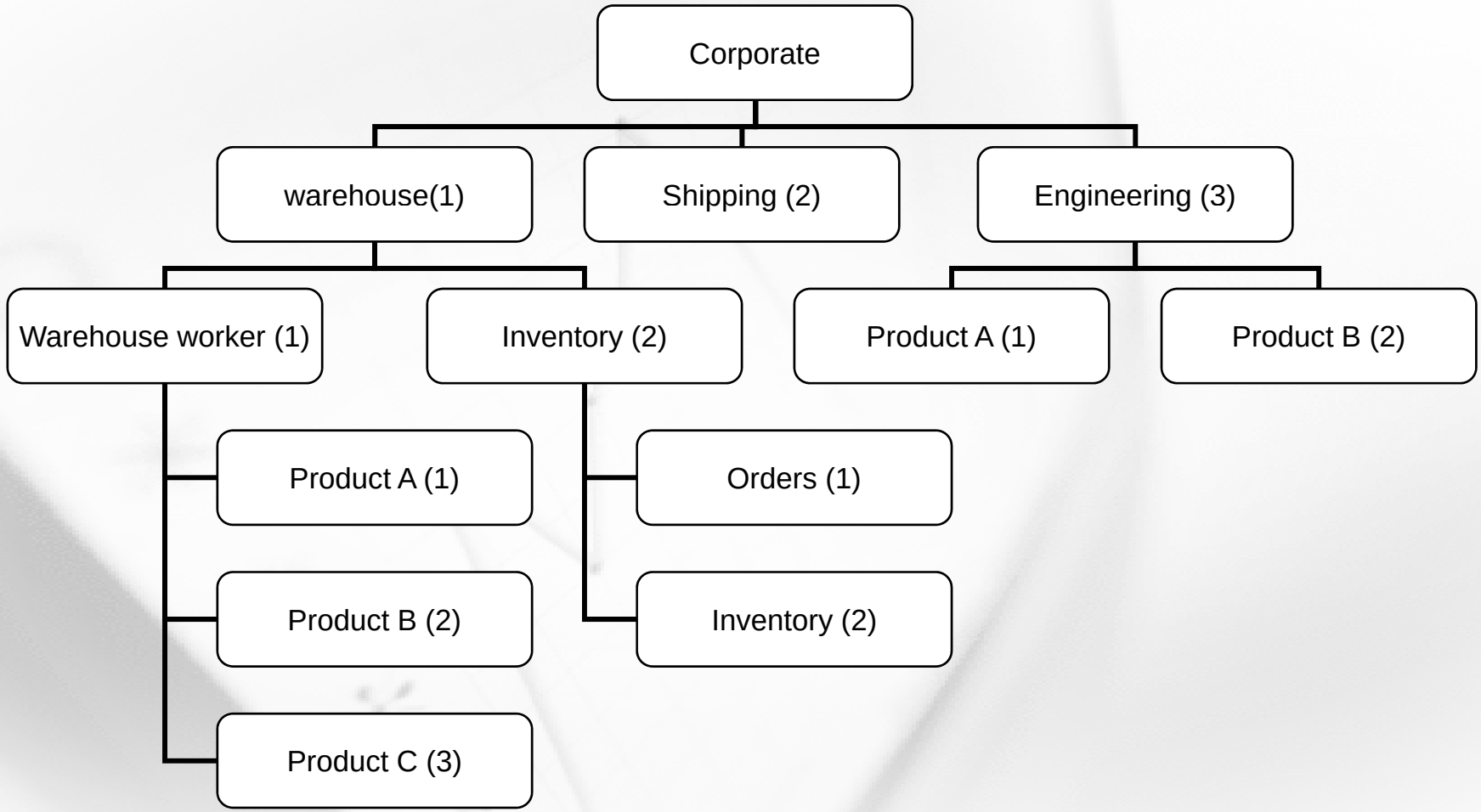
Reciprocal Agreements

- Advantage: Low cost
- Problems may include:
  - Quick access
  - Compatibility (computer, software, …)
  - Resource availability: computer, network, staff
  - Priority of visitor
  - Security (less a problem if same organization)
  - Susceptibility to same disasters
  - Length of welcomed stay

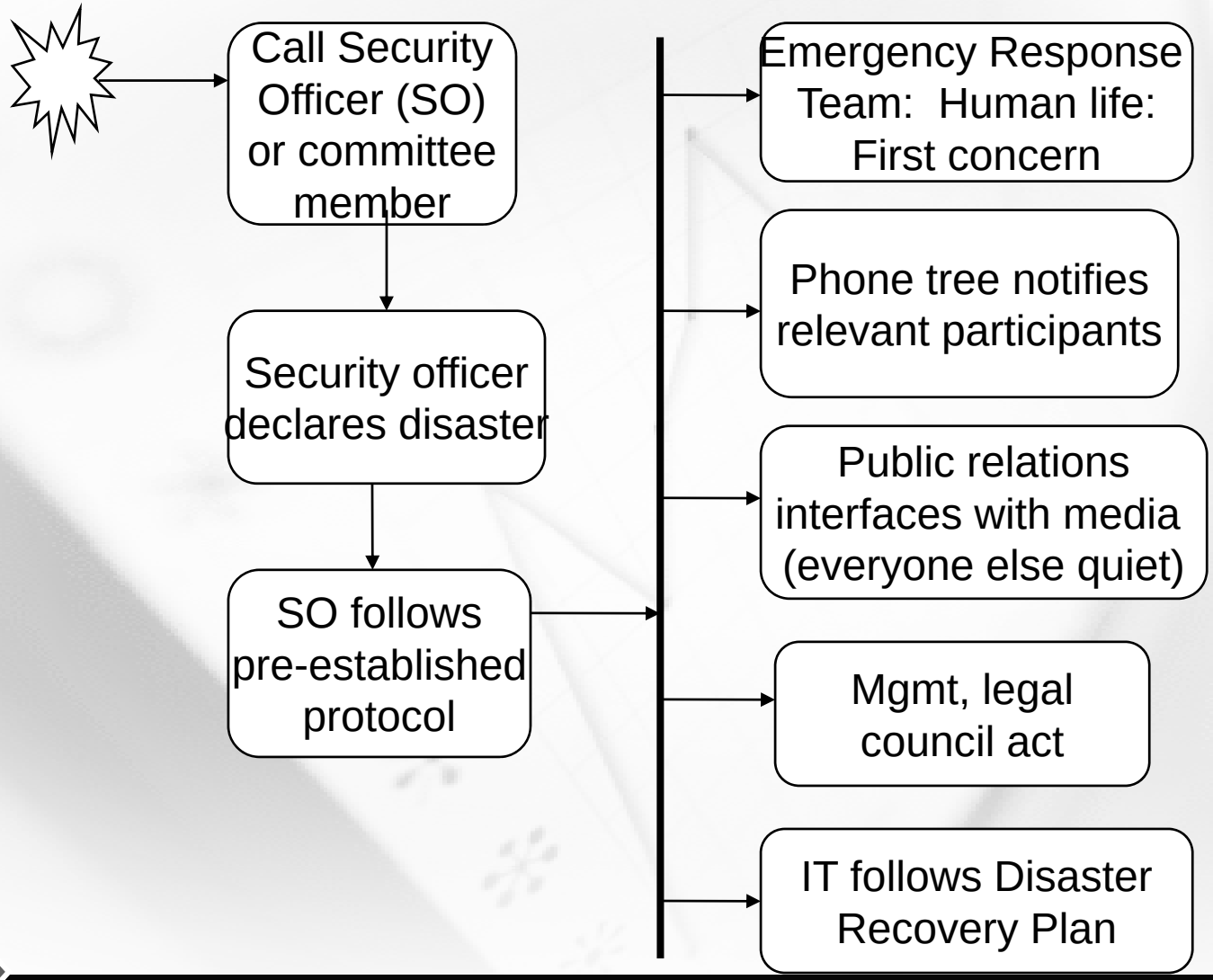
Network Disaster Recovery



Determine Criticality of Business Processes



An Incident Occurs



Concerns for a BCP/DR Plan

- Evacuation plan: People's lives always take **first priority**
- Disaster declaration: Who, how, for what?
- Responsibility: Who covers necessary disaster recovery functions
- Procedures for Disaster Recovery
- Procedures for Alternate Mode operation
  - Resource Allocation: During recovery & continued operation
- Copies of the plan should be off-site

Disaster Recovery Responsibilities

General Business

- First responder: Evacuation, fire, health…
- Damage Assessment
- Emergency Mgmt
- Transportation/ Relocation/Coordination (people, equipment)
- Supplies
- Salvage

IT-Specific Functions

- Software
- Application
- Emergency operations
- Network recovery
- Hardware
- Database/Data Entry
- Information Security

Workbook Disaster Recovery Plan

Classification (Critical or Vital)	Business Function	Disaster or Problem Event(s)	Procedure for Handling (Section 5)
Vital	Registration	Computer Failure	If total failure, forward requests to UW-System Otherwise, use 1-week-old database for read purposes only
Critical	Teaching	Computer Failure	Faculty DB Recovery Procedure
Sensitive	Personnel	Hacking attack, fraud, social engineering	Call Manager of IT Notify management. If hacking attack, bring DB off-line. Complete Incident event form Adhere to Breach Notification Law

Workbook Disaster Recovery Plan

Classification (Critical or Vital)	Business Function	Disaster or Problem Event(s)	Procedure for Handling (Section 5)
Vital	Registration	Computer Failure	If total failure, forward requests to UW-System Otherwise, use 1-week-old database for read purposes only

Disaster Recovery Test Execution

Always tested in this order:

- Desk-Based Evaluation/Paper Test: A group steps through a paper procedure and mentally performs each step.
- Preparedness Test: Part of the full test is performed. Different parts are tested regularly.
- Full Operational Test: Simulation of a full disaster

Business Continuity Test Types

- Checklist Review: Reviews coverage of plan – are all important concerns covered?
- Structured Walkthrough: Reviews all aspects of plan, often walking through different scenarios
- Simulation Test: Execute plan based upon a specific scenario, without alternate site
- Parallel Test: Bring up alternate off-site facility, without bringing down regular site
- Full-Interruption: Move processing from regular site to alternate site.

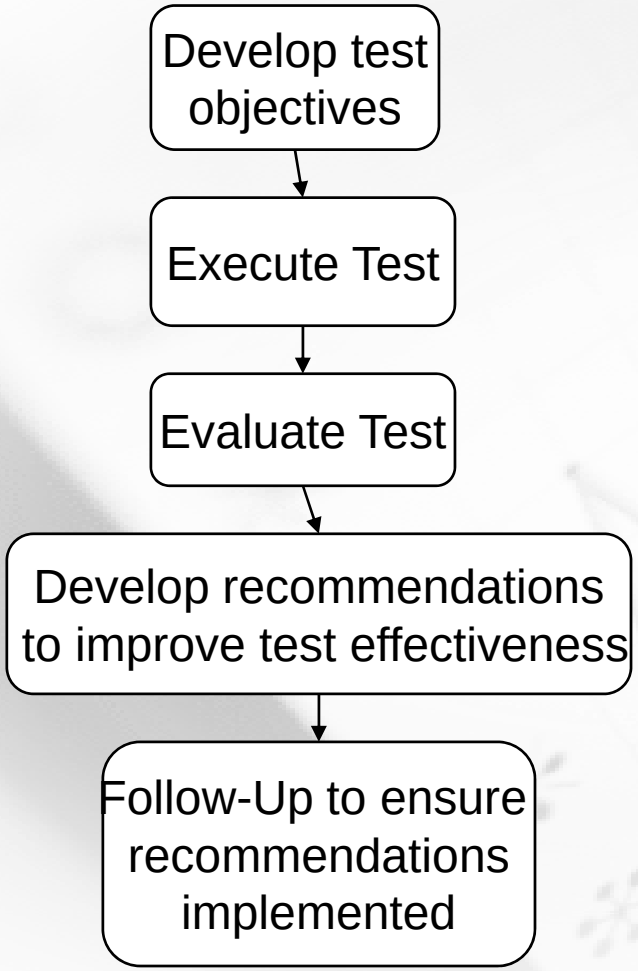
Testing Objectives

Main objective: existing plans will result in successful recovery of infrastructure & business processes

Also can:

- Identify gaps or errors
- Verify assumptions
- Test time lines
- Train and coordinate staff

Testing Procedures



Tests start simple and become more challenging with progress

Include an independent 3rd party (e.g. auditor) to observe test

Retain documentation for audit reviews

Gap Analysis

Comparing Current Level with Desired Level

- Which processes need to be improved?
- Where is staff or equipment lacking?
- Where does additional coordination need to occur?