Business Continuity and Disaster Recovery Planning

Domain 8

Overview

This domain addresses the preparation, processes, and practices required to ensure the preservation of the business in the face of major disruptions to normal business operations.

BCP and DRP involve the identification, selection, implementation, testing, and updating of processes and specific actions necessary to prudently protect critical business processes from the effects of major system and network disruptions.

Key Areas of Knowledge

- Understand business continuity requirements
- Conduct business impact analysis
- Develop a recovery strategy
- Understand disaster recovery process
- Exercise, assess and maintain the plan

Agenda

- **Understand business continuity requirements**
- Conduct business impact analysis
- Develop a recovery strategy
- Understand disaster recovery process
- Exercise, assess and maintain the plan

Business Continuity

Standards

- ISO 25999
- NIST 800-34
- ISO 27001/ ISO-IEC 27002/ ISO-IEC 27031
- NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs

Business Continuity Management

- Policy
- BIA
- BCP - DRP - COOP - Contingency Plan
- Testing
- Awareness

Business Continuity (cont.)

Standards

- ISO 25999
- NIST 800-34
- ISO 27001/ ISO-IEC 27002/ ISO-IEC 27031
- NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs

Business Continuity Management

- Policy
- BIA
- BCP - DRP - COOP - Contingency Plan
- Testing
- Awareness

Business Continuity Planning

- **Mitigate the negative effects disruptions can have:**
  - Institution's strategic plans
  - Reputation
  - Operations
  - Liquidity
  - Credit quality
  - Market position
  - Ability to remain in compliance with applicable laws and regulations

Roles and Responsibilities

Senior Executive Management

- Consistent support and final approval of plans
- Setting the business continuity policy
- Prioritizing critical business functions
- Allocating sufficient resources and personnel
- Providing oversight for and approving the BCP
- Directing and reviewing test results
- Ensuring maintenance of a current plan

Roles and Responsibilities

Senior Functional Management

- Develop and document maintenance and testing strategy
- Identify and prioritize mission-critical systems
- Monitor progress of plan development and execution
- Ensure periodic tests
- Create the various teams necessary to execute the plans

Roles and Responsibilities

BCP Committee

- Execute the BIA
- Coordinate with department representatives
- Develop analysis group
  - Plan must be developed by those who will carry it out
  - Representatives from critical departments

Roles and Responsibilities

BCP Teams

- **Rescue:** Responsible for dealing with the immediacy of disaster—employee evacuation, “crashing” the server room, etc.
- **Recovery:** Responsible for getting the alternate facility up and running
- **Salvage:** Responsible for the return of operations to the original or permanent facility (reconstitution)

BCP Teams, related plans and functions

Team/Role	Plan	Function
BCP Coordinator	DRP	Notification: Disaster declaration and alerts Emergency Management Team that the DRP is in effect
Rescue Team	Occupant Emergency Plan	Safe Evacuation of a facility, accounting for all affected personnel
Emergency management team	Crisis Communications Plan	Call trees, off site emergency operation facilities, confirmation of the incident, notification of emergency services (police, fire, medical), notification team members and other stakeholders.
Emergency management team	Succession Plan	Address loss of key team members and decision makers
Recovery Team	RP (Business Recovery Plan)	Restoring the back end infrastructure using alternate processing site, recovery of data, re-establishing services
Recovery Team	COOP	Bringing missional critical processes back online, restoring essential business functions
Incident Response Team	IT Contingency Plan	Restore domain controllers, Database, Web Functionality
Incident Response Team	Cyber Incident Response plan	Detect Malicious Attack and respond accordingly
Reconstitution/Salvage Team	Failback Procedures	Fail back plan to ensure logical order, and necessary steps, to reduce the risk of migrating to the repaired or replaced site.

BCP Team Development

- **Management should appoint members**
- **Each member must understand the goals of the plan and be familiar with the function they are responsible for**
- **Agreed upon prior to the event:**
  - Who will talk to the media, customers, share holders
  - Who will setup alternative communication methods
  - Who will setup the offsite facility
  - Established agreements with off-site facilities should be in place
  - Who will work on the primary facility

The Securities and Exchange Act of 1934

- **All publicly held companies to keep accurate records and maintain internal control systems to safeguard assets**
  - Computer systems and all the data they contain
  - Critical records and original documents
- **Company that fails to generate a record is as liable as the company that fails to preserve it**
- **A company without adequate disaster plans may not be able to create records for a substantial period of time**

Liability

Executives

- Can be held liable under several laws and regulations to ensure BCP and DRP are developed and put into place
- A civil suit can be brought against them by stock holders, customers, or anyone directly affected by a disaster or disruption

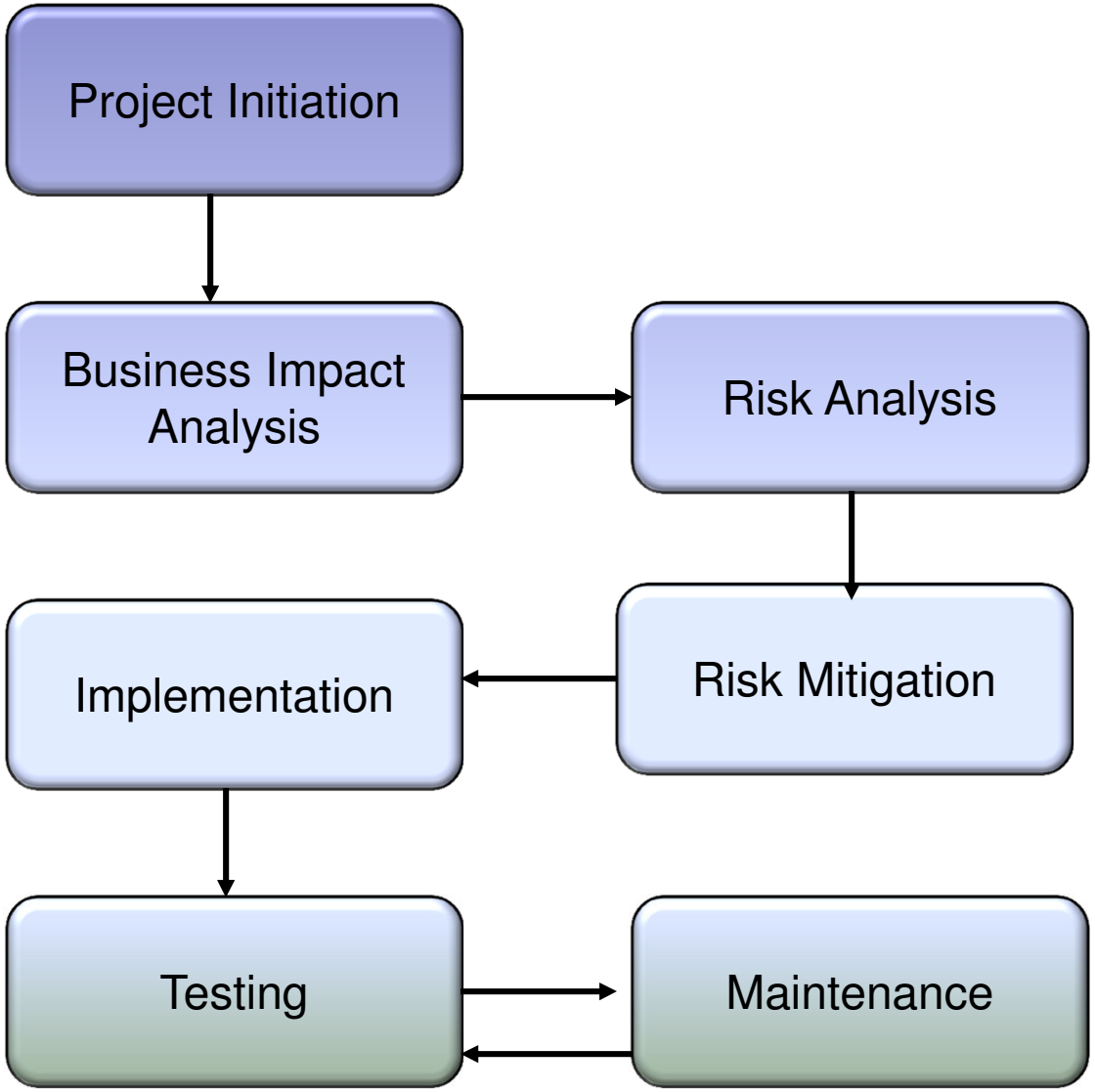
Industry-specific Regulations

- Responsible to know the regulations that pertain to their specific industry

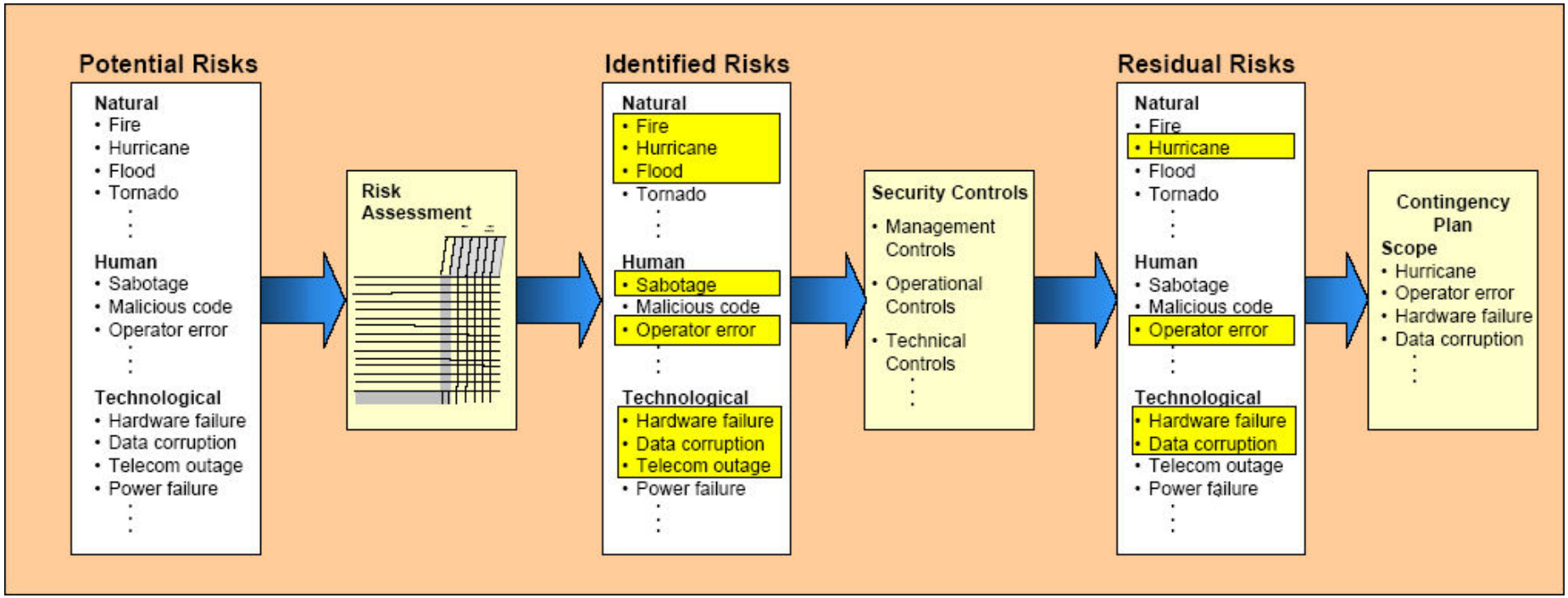
Proper Planning

- **Company is more vulnerable after a disaster hits**
  - Confidential information still needs to be kept confidential
  - Necessary resources need to be identified and protected
- **More than just a redundant server or backed up data**
  - People must be trained to know what to do
  - Redundant power supplies
  - Documented configurations
- **Disaster recovery and business continuity should be an integrated part of business decisions and a security program**

Phases of Plan



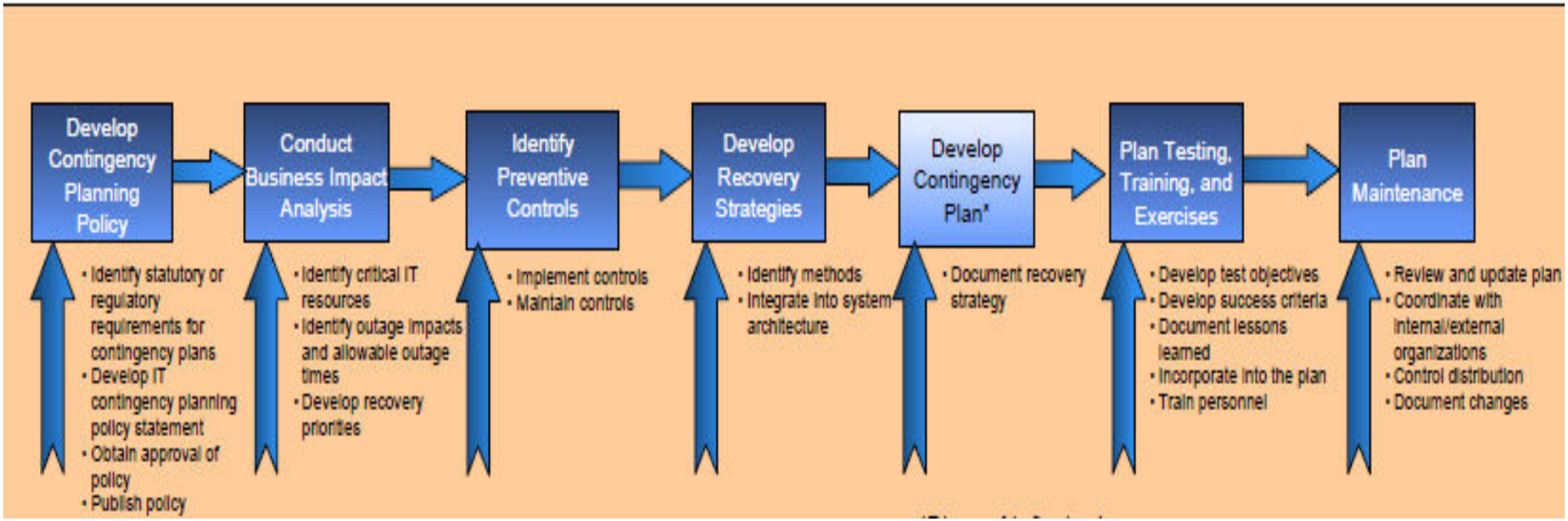
BCP Relationship to Risk Management



Seven Step Process (SP 800-34)

1. Develop contingency planning policy
2. Conduct business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop contingency plan
6. Test the plan and train personnel
7. Maintain the plan

NIST SP 800-34 - visually



Individual Plans within NIST SP 800-34

- BRP (Business Recovery Plan)
- COOP (Continuity of Operations Plan)
- Continuity of Support Plan/IT Contingency Plan
- Crisis Communication Plan
- Cyber Incident Response Plan
- DRP (Disaster Recover Plan)
- OEP (Occupant Emergency Plan)

Individual Plans - Details

Business Recovery (or Resumption) Plan (BRP)

Purpose: Provide procedures for recovering business operations immediately following a disaster

Scope: Addresses business processes; not IT-focused; IT addressed based only on its support for business process

Continuity of Operations Plan (COOP)

Purpose: Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days. This term is sometimes used in US Government to refer to the field of Business Continuity Management, but per NIST 800-34, it is a unique sub-plan of the BCP. **Note, BCP addresses ALL business processes, not just mission critical.

Scope: Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused

Individual Plans – Details (cont.)

Continuity of Support Plan/IT Contingency Plan

Purpose: Provide procedures and capabilities **for recovering a major application or general support system**

Scope: Same as IT contingency plan; addresses **IT system disruptions**; not business process focused

Crisis Communications Plan

Purpose: Provides procedures for **disseminating status reports to personnel and the public**

Scope: Addresses communications with personnel and the public; not IT focused

Cyber Incident Response Plan

Purpose: Provide strategies to **detect, respond to, and limit consequences of malicious cyber incident**

Scope: Focuses on information security responses to incidents affecting systems and/or networks

Individual Plans – Details (cont.)

Disaster Recovery Plan (DRP)

Purpose: Provide detailed procedures to facilitate recovery of capabilities at an alternate site

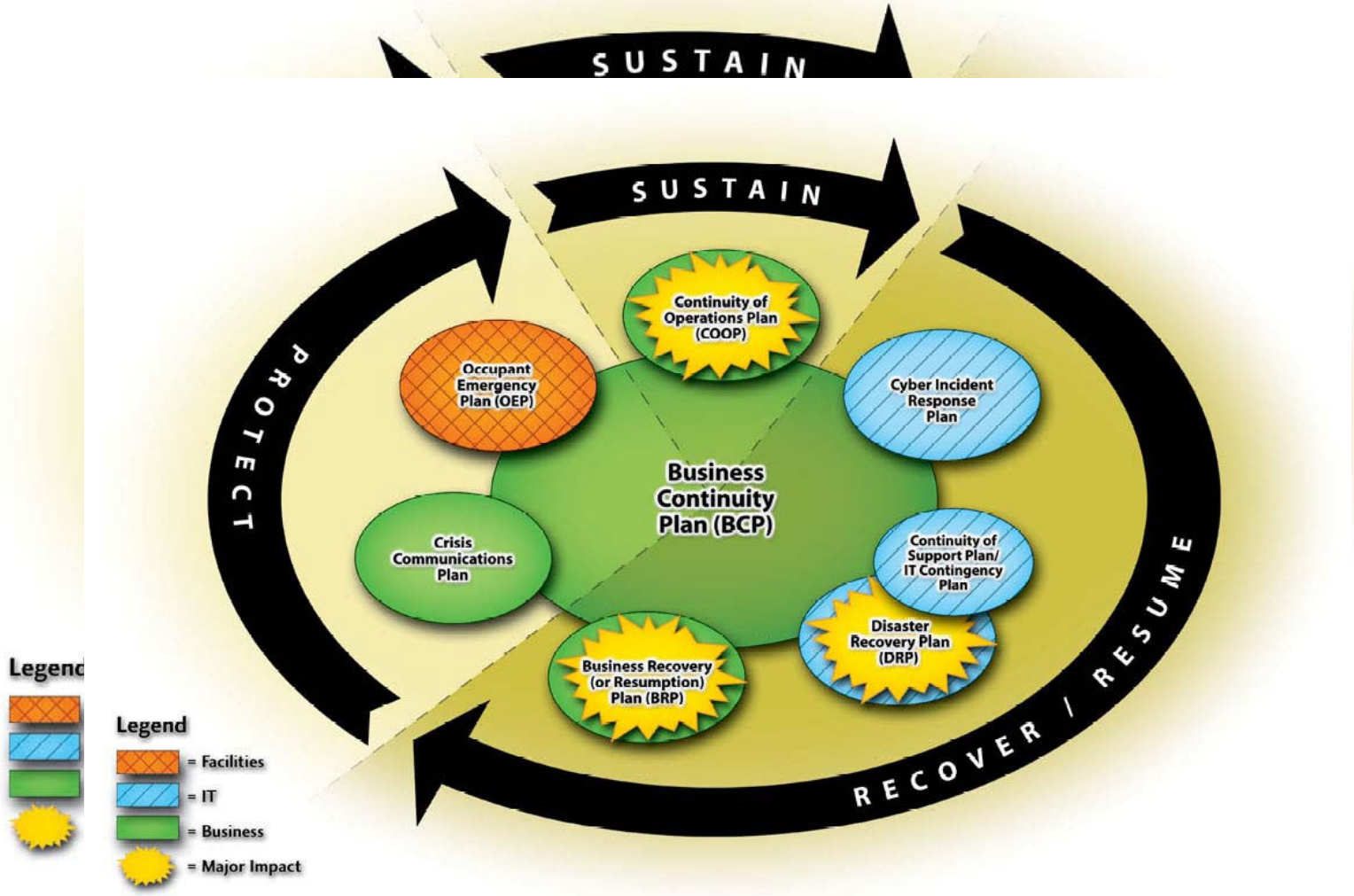
Scope: Often IT-focused; limited to major disruptions with long-term effects

Occupant Emergency Plan (OEP)

Purpose: Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat

Scope: Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based. May also be referred to as Crisis or Incident management plans. However, the OEP concept should be recognizable as the "initial response to the emergency event"

Individual Plans – Interrelationship



Agenda

- Understand business continuity requirements
- **Conduct business impact analysis**
- Develop a recovery strategy
- Understand disaster recovery process
- Exercise, assess and maintain the plan

Business Impact Analysis (BIA) – 1 of 2

- Goal is to see how the company would be affected by different identified threats
- Gather quantitative and qualitative information on impact
- Identify areas that would suffer greatest financial and operational loss
- Identify company's critical systems needed for survival

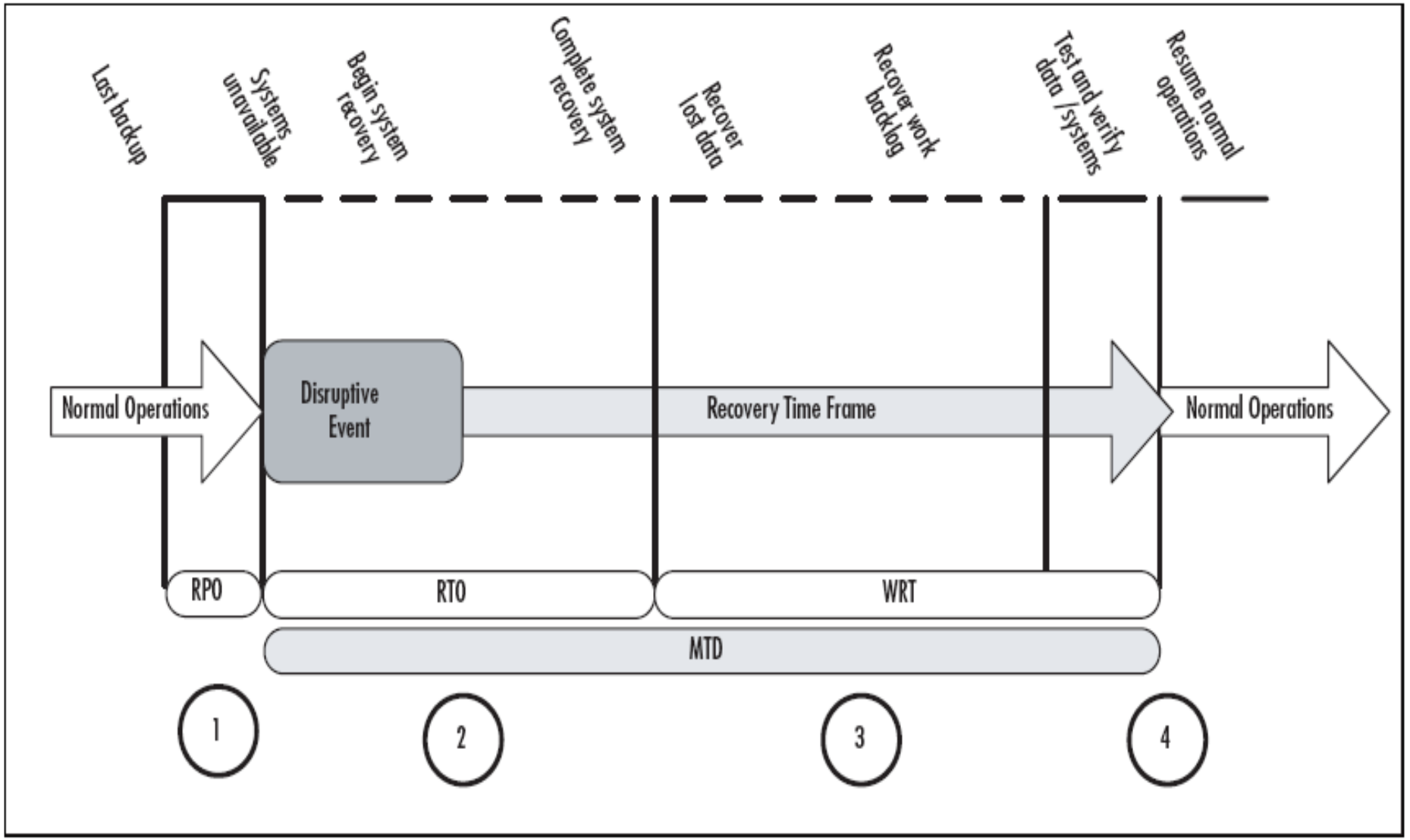
Business Impact Analysis (BIA) – 2 of 2

- Estimate outage time that can be tolerated as a result of a disaster or disruption (MTD)
- Compile resource requirements including recovery point objective (RPO)
- Identify recovery alternatives
- Document and submit for approval

Important BIA Questions

- **Management should establish recovery priorities for business processes that identify:**
  - Essential personnel
  - Technologies
  - Facilities
  - Communications systems
  - Vital records and data

BIA Key Metrics and their relationship



Possible Threats

- **Disaster recovery and continuity planning deal with uncertainty and chance**
  - Must identify all possible threats and estimate possible damage
  - Develop viable alternatives
- **Threat Types:**
  - Man-made
    - Strikes, riots, fires, terrorism, hackers, vandals
  - Natural
    - Tornado, flood, earthquake, hurricane
  - Technical
    - Power outage, device failure, loss of a T1 line, virus infection on the network

Categories of Disruptions

- **Non-disaster**
  - Disruption of service
  - Device malfunction
- **Disaster**
  - Entire facility unusable for a day or longer
- **Catastrophe**
  - Destroys facility
- **A company should understand and be prepared for each category**

How Much Will It Impact Us?

- **Examples of Maximum Tolerable Downtime (MTD) Categories:**
  - Non-essential – 30 days
  - Normal – 7 days
  - Important – 72 hours
  - Urgent – 24 hours
  - Critical – Minutes to hours

Business Functions

- **Essential business functions need to be identified:**
  - IT Network Support
  - Data Processing
  - Accounting
  - Payroll
  - Customer Support
  - Production Scheduling
  - Communications

Loss Criteria – Short-term

- **Once threats are identified and critical business functions are understood, a specific loss criteria must be developed**

- **Short-term loss criteria:**
  - Loss in profits
  - Loss in productivity
  - Increase in operational expenses
  - Violations of contract agreements

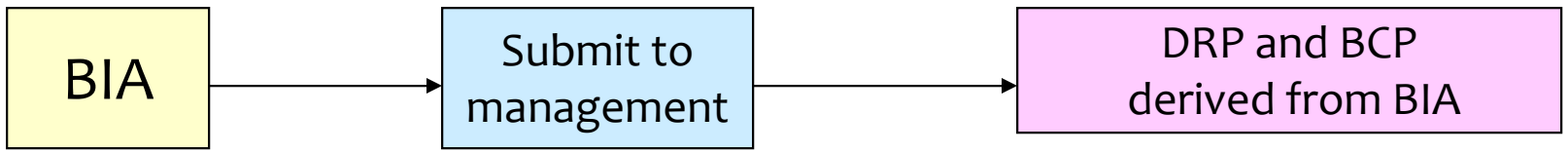
Loss Criteria – Long-term

Long-term loss criteria:

- Delayed income costs
- Loss in reputation and public confidence
- Loss of competitive advantages
- Hidden costs
  - These need the greatest attention because they are not always insurable expenses

Results from the BIA

- **Results of Business Impact Analysis contain**
  - Identified critical departments and required resources
  - Identified threats and risks
  - Impact company can handle dealing with each risk
  - Outage time that would not be critical
  - Recovery alternatives
- **Document and present to management for approval**
- **Results are used to create the recovery plans**



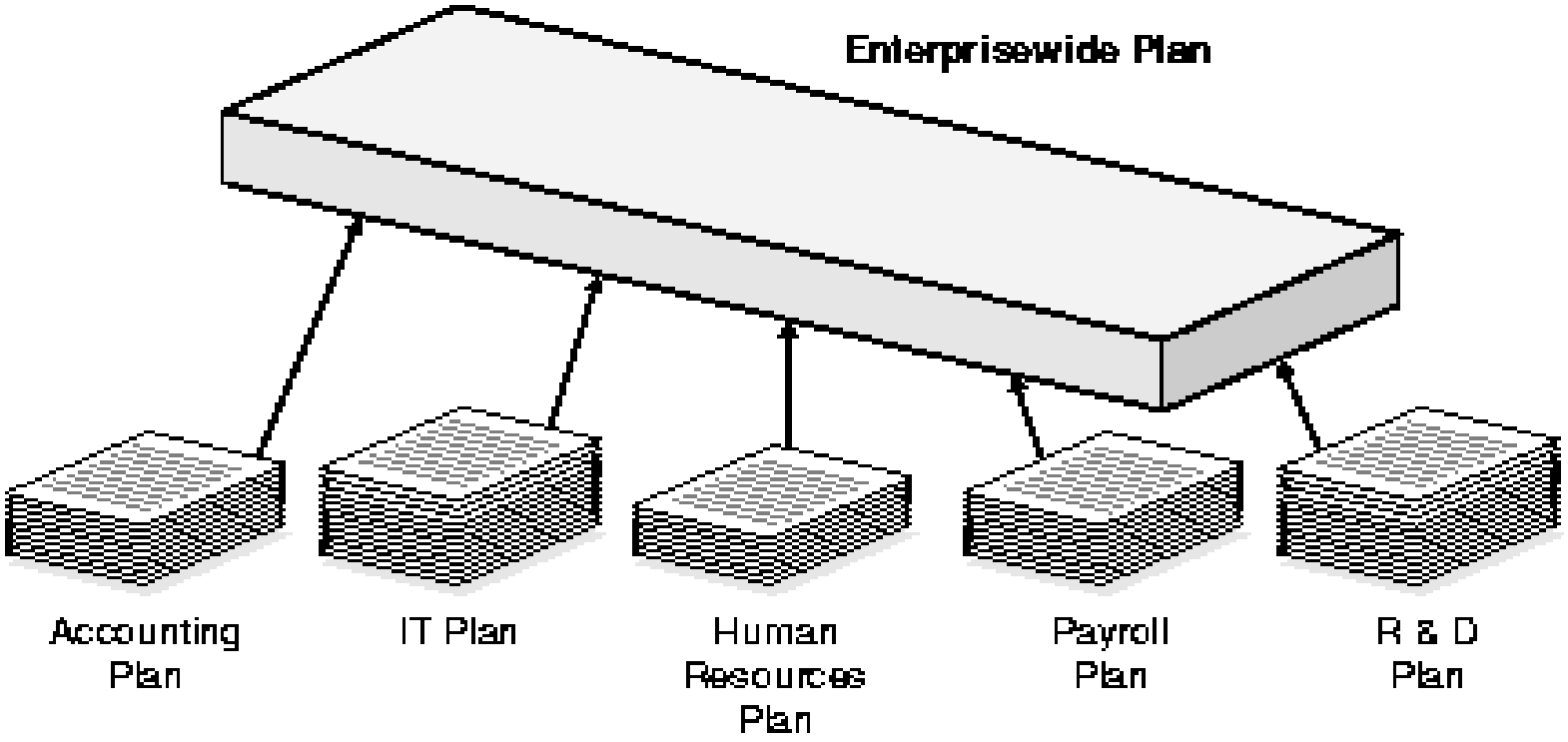
Agenda

- Understand business continuity requirements
- Conduct business impact analysis
- **Develop a recovery strategy**
- Understand disaster recovery process
- Exercise, assess and maintain the plan

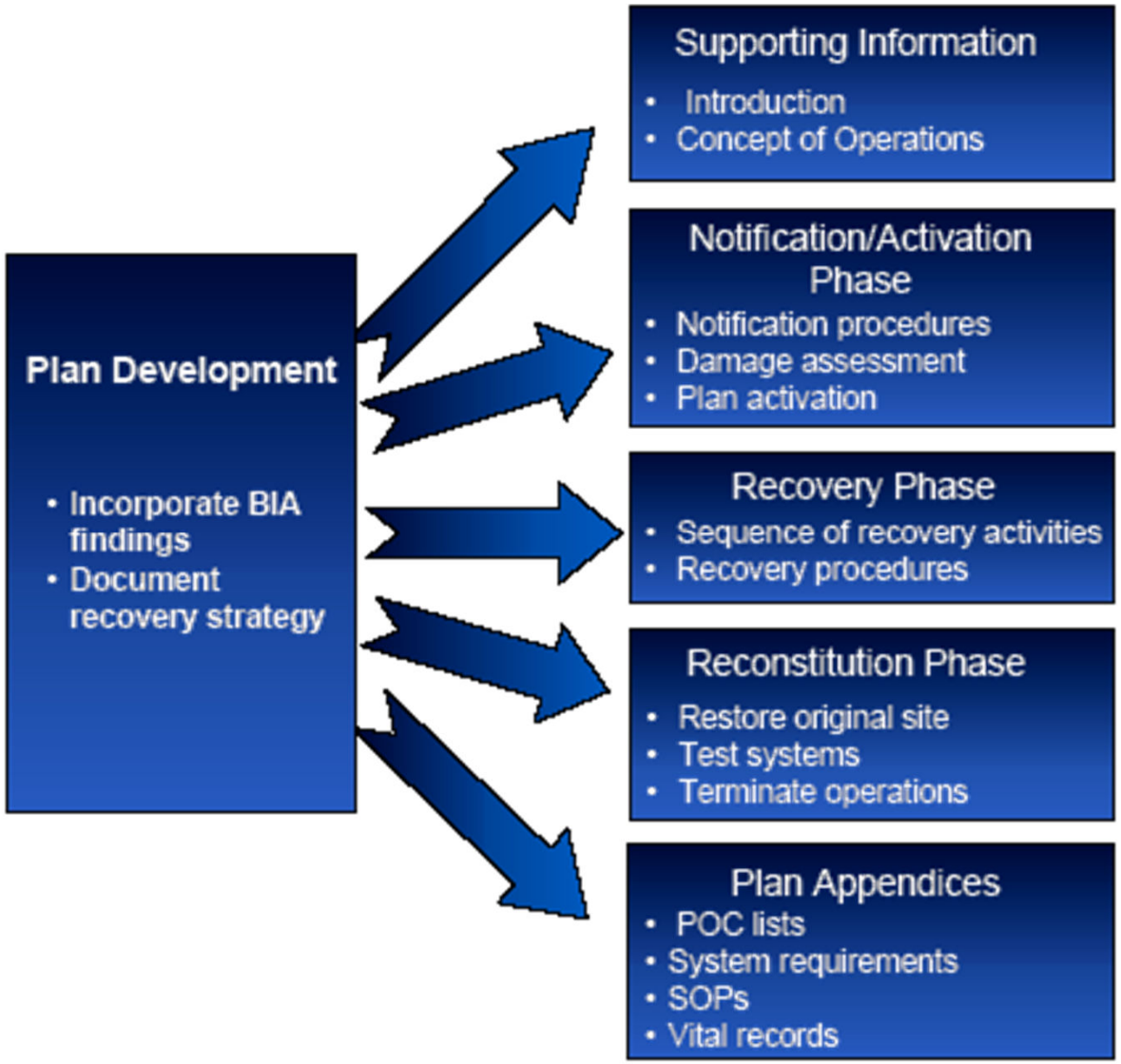
Writing the Plan

- **Now that all the research and planning has been done, the next step is to actually write/document the plan.**
- **Should address**
  - Responsibility
  - Authority
  - Priorities
  - Testing

Different Plans



Contingency Plan Structure



Disaster Recovery Plan Objectives

- **Protect company if parts or all of services become unusable**
- **Improve responsiveness by employees in different situations**
  - Ease confusion with written procedures and drills
  - Help make logical decisions during a crisis
- **Guarantee reliability of standby systems**
- **If employees know what they are expected to do during a disaster, then management can address the larger picture**

Priorities

Number One Priority in Disaster Recovery:

- Safety of people
- If there is a conflict between saving data, equipment, or people, people come first

Other priorities in DRP

- Protect the company as a whole
- Minimizing property damage

Disaster Recovery Plan – 1 of 2

Written recovery plan should include:

- Activation Criteria and Procedure
- People
- Facility Issues
- Utilities: power, telecommunications
- Hardware
- Vendor assistance and service providers

Disaster Recovery Plan – 2 of 2

Written recovery plan should include:

- Software
  - Operating systems, applications, and data
- Supplies
  - HVAC, UPS, and office supplies
- Recovery and Emergency Procedures
- Critical documentation and/or records

Environment

- **It is important to truly understand the current environment in case it has to be totally replicated after a disaster**
  - Device types for proper replacement
  - Applications and data backup
  - Proper software configurations
  - Interfacing with outside communication lines
  - Interfacing with outside partners and suppliers

Agenda

- Understand business continuity requirements
- Conduct business impact analysis
- Develop a recovery strategy
- **Understand disaster recovery process**
- Exercise, assess and maintain the plan

Three Phases Following a Disruption

1. Notification/Activation

- Notifying recovery personnel
- Performing a damage assessment

2. Recovery Phase - Failover

- Actions taken by recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities

3. Reconstitution - Failback

- Outlines actions taken to return the system to normal operating conditions

Offsite Facilities

- What if our primary site is damaged?
- Where should the company redeploy?

Secondary Issues

After the Disaster:

- Looting and vandalism
- Fraud opportunities
- Media and press
- Responsibilities to families
- Legal responsibilities
- Further expenses

Backup Alternatives

Subscription Services

- Hot, warm, cold sites

Reciprocal Agreements

Others

- Redundant/Mirrored site (partial or full)
- Outsourcing
- Rolling hot site
- Prefabricated building

Backup Alternatives

Alternative	Time to Occupy	Readiness	Cost
Mirrored Site	Within 24 hours	Fully redundant in every way	Highest
Hot Site	Within 24 hours	Fully configured equipment and communications links; need only load most recent data	Higher
Rolling Hot Site	Usually 24 hours	Similar to hot site, but supports data center operations only	High
Warm Site	Within a week	Between a hot and cold site. Partially configured equipment and does not contain any live data; some activation activity needed	Medium
Cold Site	Within 30 days	Typically contains the appropriate electrical and heating/air conditioning systems, but does not contain equipment or active communication links	Lowest

Reciprocal Agreement Issues

- How long will the facility be available to the company in need?
- How much assistance will the staff supply in the means of integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the resources will be available to the company in need?
- How will differences and conflicts be addressed?
- How does change control and configuration management take place?

Criteria for an Offsite Storage Facility

- Is the facility closed on weekends or holidays?
- Are the access controls tied in to emergency services?
- Is the facility fire resistant in its construction?
- What is the availability of a bonded transport service?
- Are there any geographical environmental hazards?
- Does the facility provide proper environmental controls?
- Is there a fire detection and suppression system?
- What is the vendor's liability of stored media?

Hardware/Technology Recovery

- **Technology Recovery is dependent upon good configuration management documentation and includes such things as:**
  - PC's/Servers
  - Network Equipment
  - Supplies
  - Voice and data communications equipment
  - SLA's can play an essential role in hardware recovery—See notes below

Software Recovery

- BIOS Configuration information
- Operating Systems
- Licensing Information
- Configuration Settings
- Applications
- Contingency plans for what to do in the event that the operating system/applications are no longer available to be purchased

Personnel Recovery

- Identify Essential Personnel—Entire staff is not always necessary to move into recovery operations
- How to handle personnel if the offsite facility is a great distance away
- Eliminate single points of failure in staffing and ensure backups are properly Trained

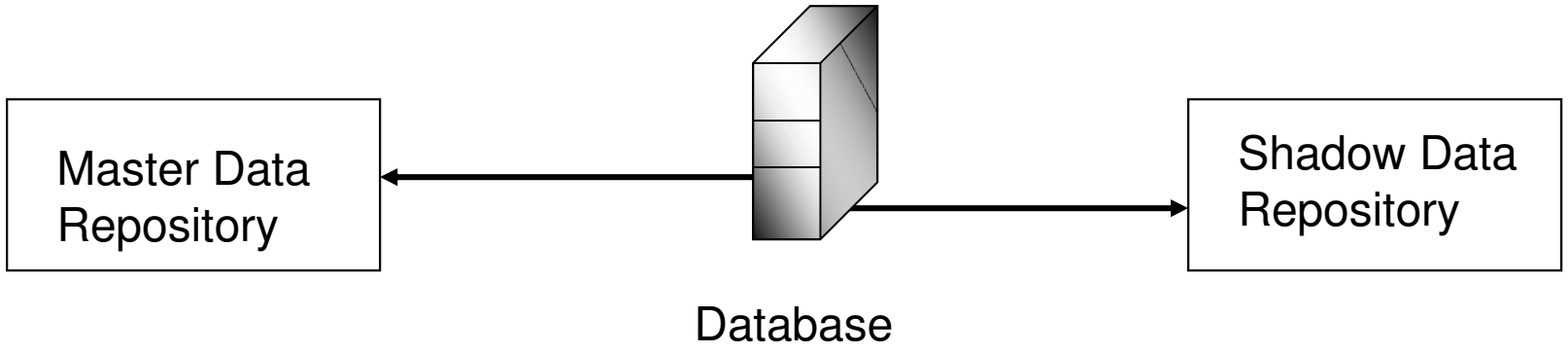
Data Recovery

- Data Recovery options are driven by metrics established in the BIA (MTD, RTO, RPO, etc.)
- Backups
- Database Shadowing
- Remote Journaling
- Electronic Vaulting

Software Backups

Database Backups

- Disk-shadowing
  - Mirroring technology
  - Updating one or more copies of data at the same time
  - Data saved to two media types for redundancy



Transaction Redundancy

Electronic Vaulting

- Copy of modified file is sent to a remote location where an original backup is stored
- Transfers bulk backup information
- Backup of data is real time
- Transmission of backup to offsite facility is done by batch

Remote Journaling

- Moves the journal or transaction log to a remote location, not the actual files
- Parallel processing of transactions to an alternate site
- Communication line used to transmit data as it is generated

Who repairs the primary site?

Reconstitution:

- Company is not out of an emergency state until operational at primary site
- The Salvage team

Restoration / Reconstitution

- **Restoring a full environment can be an overwhelming task**
  - Responsible individuals should be properly trained
  - Have written documentation
  - Tested and drilled
- **Teams**
  - Rescue team gets employees to safety
  - Recovery team to prepare offsite facility and movement
  - Salvage team to bring primary site online
- **Restoring Operations**
  - Returning to primary site also a risk
  - Least critical department returned first

Restoring Applications

Processing Priorities

- Categories should be defined that indicate which critical applications should come on-line first
- Each category should have a time frame to recover and a priority level
- Category I could have a required turn-around time of 24 hours, while category III could have a turn-around time of 2 weeks
- Remember to evaluate and assign a category to applications as they are added to the environment

Agenda

- Understand business continuity requirements
- Conduct business impact analysis
- Develop a recovery strategy
- Understand disaster recovery process
- **Exercise, assess and maintain the plan**

DRP Testing

- **Demonstrate if a company can actually recover from a disaster**
  - Predetermined scenario
  - Decide upon goal prior to test
- **Performed at least once a year**
  - No confidence in plan until it has been tested
  - Point out issues that need to be improved upon (never to find fault or blame)
  - The particular type of testing is based upon the criticality of the organization, resources available and risk tolerance

DRP Testing (continued)

- **Plan testing should be performed if significant changes have taken place within the company**
- **Plan testing should take place if significant changes are made to contingency plan**
- **Expect mistakes during tests**
  - Learning experience
  - Verify compatibility of backup facilities and hardware
- **Report results to management**

Types of Tests

Checklist Test

- Copies of plan distributed to different departments
- Functional managers review

Structured Walk-Through (Table Top) Test

- Representatives from each department go over the plan

Simulation Test

- Going through a disaster scenario
- Continues up to the actual relocation to an offsite facility

Types of Tests

Parallel Test

- Systems moved to alternate site, and processing takes place there

Full-Interruption Test

- Original site shut down
- All of processing moved to offsite facility

Post-incident Review

- **After a test or disaster has taken place:**
  - Focus on what happened
  - What should have happened
  - What should happen next
  - Not who's fault it was; this is not productive

Plans Become Obsolete

- **Change Management:**
  - Technical – hardware/software
  - People
  - Environment
  - Laws
- **Large plans can take a lot of work to maintain**
- **Does not have a direct line to profitability**

Plan Maintenance

Keeping plan in date

- Make it a part of business meetings and decisions
- Centralize responsibility for updates
- Part of job description
- Personnel evaluations
- Report regularly
- Audits
- As original plans are revised, original copies should be retrieved and destroyed

Review of the Plan Development Tasks

- Identifying regulatory and legal requirements
- Identifying possible threats and risks
- Risk Analysis
- Performing the BIA
- Outlining which departments, systems, and processes must be up and running first
- Developing procedures and steps for resuming business after a disaster
- Developing the rescue, recovery, and salvage teams
- Documenting, communicating to employees, and performing training and drills

Bringing Things Together – 1 of 2

- Understanding risks is the first step
- BIA
- BCP and DRP protect lives, equipment, liability, and company survival
- Disaster recovery plan is developed after BIA is completed and submitted to management

Bringing Things Together – 2 of 2

- Measures need to be taken to deal with several different types of disasters and non-disasters
- Different types of hardware, software, and facility backups
- Plan has to be implemented and updated
- Disaster Recovery should be part of any business decision
- Prevention is the best protection