SENG 460

Practice of Information Security and Privacy

Business Continuity and Disaster Recovery

Overview

- Business Continuity VS. Disaster Recovery
- What is Business Continuity Planning (BCP)
- BCP Standard Practises
- Practical BCP Development for an Organization

Some Concepts

Disruptions: Any unplanned event that results in the temporary interruption of any organizational asset, including people, processes, functions, and devices, etc. Three main categories:

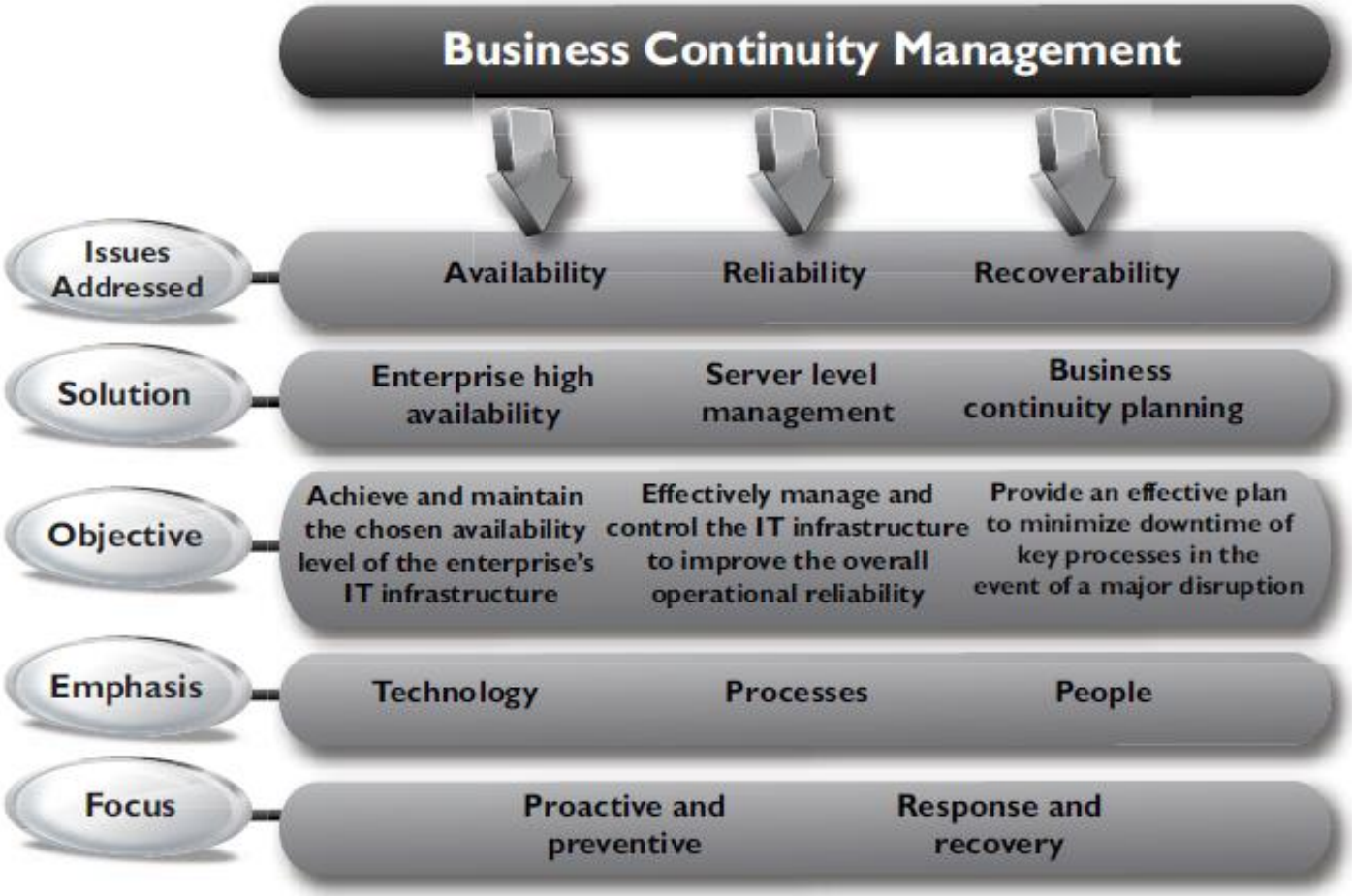
- ***Non-disasters:*** *short-term interruptions caused by system malfunction or failures.*
- ***Disasters:*** *a suddenly occurring event that has long-term impact on business.*
  - Technological disasters.
  - Man-made disasters.
  - Natural disasters.
- ***Catastrophes:*** *a disaster that has a much wider and mush longer impact to business than regular disaster.*

Business Continuity VS. Disaster Recovery

- Disaster Recovery
  - The goal of disaster recovery is to minimize the effects of a disaster or disruption. A disaster recovery plan (DRP) is carried out when everything is still in emergency mode, and everyone is scrambling to get all critical systems back online.

- Business Continuity
  - A business continuity plan (BCP) can include getting critical systems to another environment while repair of the original facilities is under way, getting the right people to the right places during this time, and performing business in a different mode until regular conditions are back in place.

What is Business Continuity Planning (BCP/BCM)



BCP Standard Practises

One of the most popular business continuity and disaster recovery planning standards is Special Publication (SP) 800-34 Revision 1 (R1) from the National Institute of Standards and Technology (NIST).

Develop contingency planning policy.	Conduct business impact analysis (BIA).	Identify preventive controls.	Create recovery strategies.	Develop business continuity plan (BCP).	Test, train, and exercise.	Maintain the plan.
Identify statutory or regulatory requirements. Develop IT contingency planning policy statement. Publish policy.	Identify critical processes and resources. Identify outage impacts, and estimate downtime. Identify resource requirements. Identify recovery priorities.	Identify controls. Implement controls. Maintain controls.	Develop backup and recovery strategies. Identify roles and responsibilities. Develop alternative site. Identify equipment and cost considerations. Integrate into architecture.	Document recovery strategy.	Test the plan. Train personnel. Plan exercises.	Review and update the plan. Coordinate updates with internal and external organizations. Control the distribution of the plan. Document the changes.

Although the NIST 800-34 document deals specifically with IT contingency plans, these steps are similar when creating enterprise-wide BCPs and BCM programs.

Practical BCP Development for an Organization
- Project Initiation

- Setting up a budget and staff for the program before the BCP process begins. Dedicated personnel and dedicated hours are essential for executing something as labor-intensive as a BCP. (a **Business Continuity Coordinator** must be identified first, who will lead the **BCP Committee and report to senior management)**
- Setting up the program would include assigning duties and responsibilities to the BCP coordinator and to representatives from all of the functional units of the organization.
- Senior management should kick off the BCP with a formal announcement or, better still, an organization-wide meeting to demonstrate high-level support.
- Awareness-raising activities to let employees know about the BCP program and to build internal support for it.
- Establishment of skills training for the support of the BCP effort.
- The start of data collection from throughout the organization to aid in crafting various continuity options.
- Putting into effect “quick wins” and gathering of “low-hanging fruit” to show tangible evidence of improvement in the organization’s readiness, as well as improving readiness.

Practical BCP Development for an Organization
- Define BCP Scope

- Is the team supposed to develop a BCP for just one facility or for more than one facility?
- Is the plan supposed to cover just large potential threats (hurricanes, tornadoes, floods) or deal with smaller issues as well (loss of a communications line, power failure, Internet connection failure)?
- Should the plan address possible terrorist attacks and other manmade threats?

A frequent objection to BCP is that a program is unlimited in its scope when it is applied to all the functions of an organization in one fell swoop. A practical approach is to break up the program into manageable pieces and to place some aspects of the organization outside the scope of the BCP.

Practical BCP Development for An Organization
- Define BCP Policy

The process of drawing up a policy includes these steps:

- Identify and document the components of the policy.
- Identify and define policies of the organization that the BCP might affect.
- Identify pertinent legislation, laws, regulations, and standards.
- Identify “good industry practice” guidelines by consulting with industry experts.
- Perform a gap analysis. Find out where the organization currently is in terms of continuity planning, and spell out where it wants to be at the end of the BCP process.
- Compose a draft of the new policy.
- Have different departments within the organization review the draft.
- Put the feedback from the departments into a revised draft.
- Get the approval of top management on the new policy.
- Publish a final draft, and distribute and publicize it throughout the organization.

Practical BCP Development for An Organization
- BCP Policy Example

Introduction

[Company] is committed to its customers, employees, shareholders and suppliers. To insure the effective availability of essential products and services, [Company] provides this Business Continuity Planning policy in support of a comprehensive program for business continuity, disaster prevention and total business recovery.

Policy

Each department is responsible for current and comprehensive Business Continuity Planning (BCP). When implemented, the Plan should include those procedures and support agreements, which insure on-time availability and delivery of required products and services. Each Plan must be certified annually with the BCP policy compliance process through the BCP team.

Policy Leadership

[Executive] is the BCP executive management liaison for the BCP program. Resolution of issues in the development of or support for all Plans should first be coordinated with the BCP team and appropriate internal or external organizations. The "Business Continuity Planning - Policy Compliance Certification" documentation defines the issue resolution process.

Policy Compliance Certification

BCP compliance verification is provided by the BCP team. In order to meet compliance requirements, each Plan should include those appropriate procedures, staffing, tools and workplace planning requirements necessary to meet approved deliverable requirements. In order to support the Enterprise BCP Plan the format of the BCP documentation must follow the BCP team defined Plan template requirements. Detailed compliance certification requirements are provided through the BCP team and included in the "Business Continuity Planning - Policy Compliance Certification" document located at [link to network location].

BCP Plan Compliance Certification is required annually. A waiver for temporary compliance certification may be given if a detailed written waiver request issued by the department manager is approved by the BCP executive management team liaison. Maximum delay for compliance is one year.

Policy Compliance Certification Support

The BCP team is available to support the development and BCP policy compliance certification process. BCP team services and contact information is available at the BusinessContinuityPlanningTeam intranet link.

[Company] recognizes the importance of a comprehensive Business Continuity Planning Program to insure the safety, health and continued availability of employment of its employees and quality goods and services for those we serve. We require the commitment of each employee, department and vendor in support of the objectives required to protect [Company] assets, mission and survivability.

Practical BCP Development for An Organization

- Business Impact Analysis (BIA)

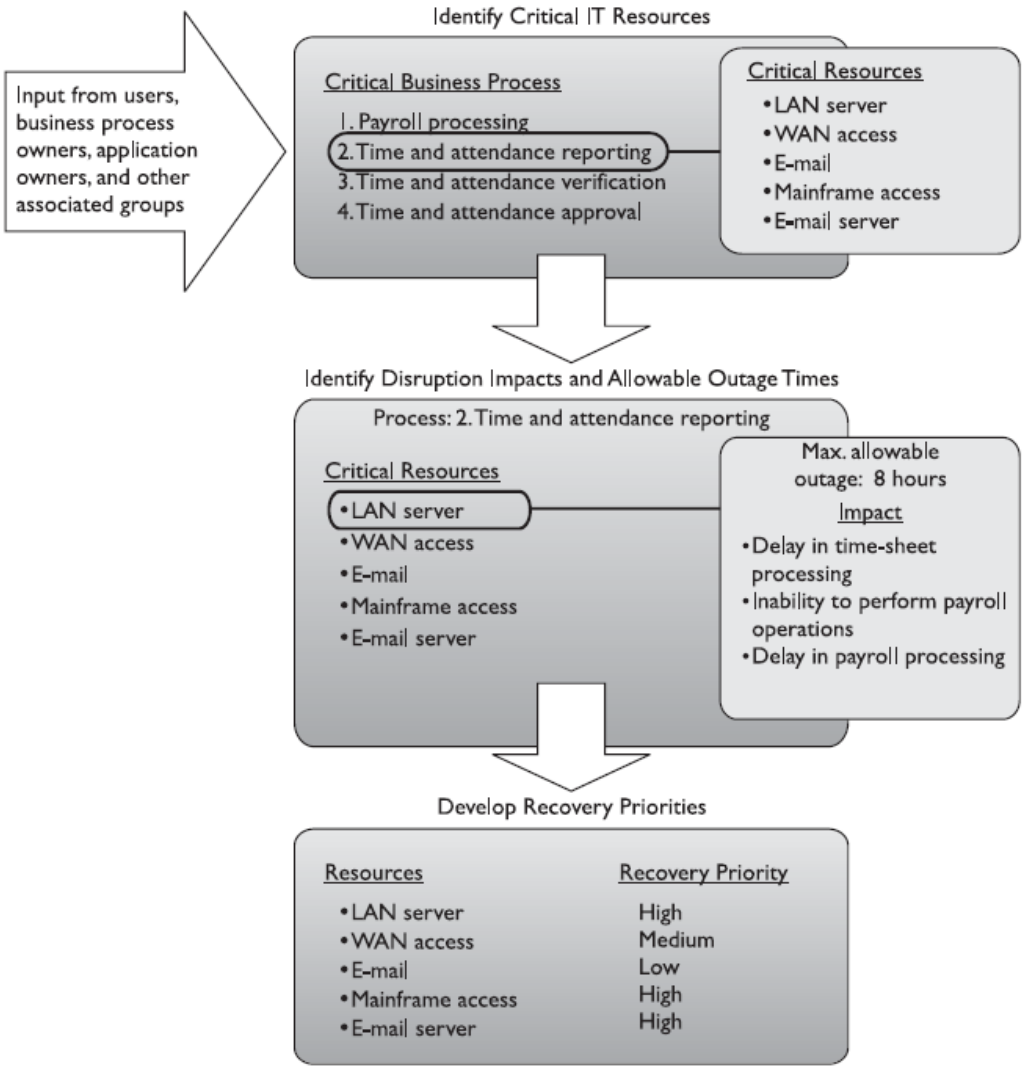
A **BIA** (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.

1. Identify critical processes and resources.
2. Identify outage impacts, and estimate downtime.
3. Identify resource requirements.
4. Identify recovery priorities.

Maximum tolerable downtime (MTD): The maximum amount of time that an organization can tolerate a single resource or function being down. Also referred to as maximum period time of disruption (MPTD). **MTD** can be used to evaluate critical level of process or resources.

Practical BCP Development for An Organization
- BIA Example

Risk assessment to business process and resources is usually part of BIA, which evaluates the real risk level the company faces.



Practical BCP Development for An Organization

- Identify Preventive Controls

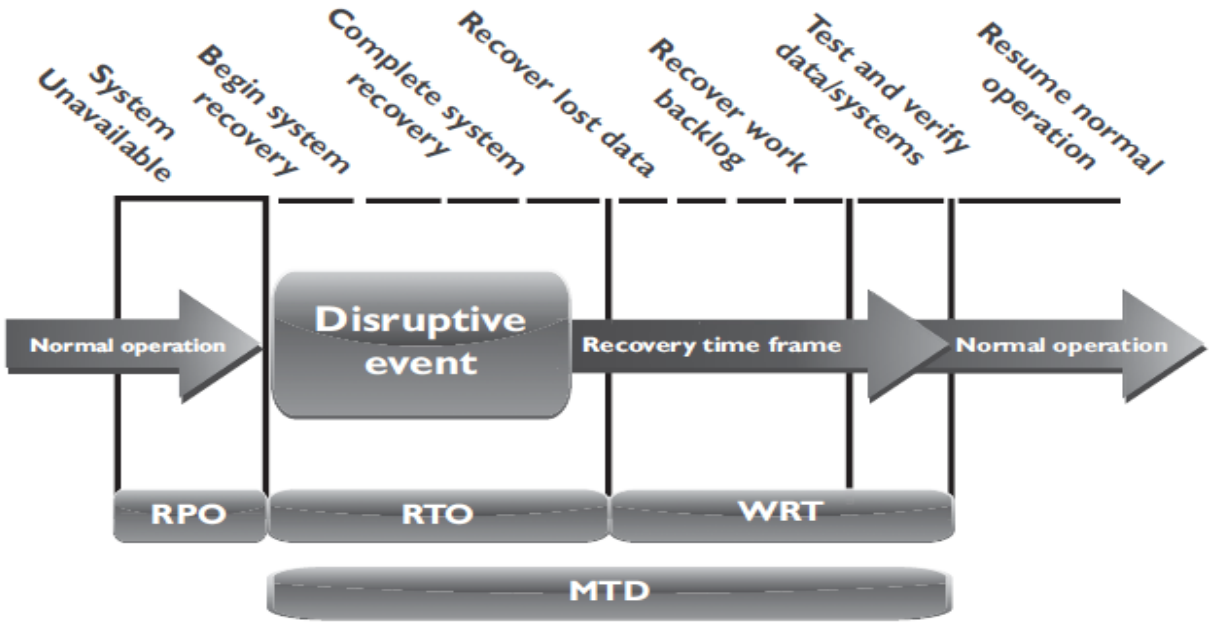
Preventive methods are preferable to actions that might be necessary to recover the system after a disruption.

- **Redundant Systems, Facilities, and Powers:** In anticipation of disasters and disruptive events, organizations should implement redundancy when redundant systems are cost-effective.
- **Fault Tolerance Technologies:** By implementing fault-tolerant technologies, an organization can ensure that normal operation occurs if a single fault-tolerant component fails.
- **Insurance:** If an organization purchases insurance, it ensures that the organization will have access to additional financial resources to help in the recovery. A special type of insurance called ***business interruption insurance*** provides monetary protection for expenses and lost earnings.
- **Data backup:** provides prevention against data loss but not prevention against the disruptive event. All organizations should ensure that all systems that store important files are backed up in a timely manner.
- **Fire Detection and Suppression:** Organizations should implement fire detection and suppression systems as part of any BCP.

Practical BCP Development for An Organization

- Develop Recovery Strategies

- **Recovery Point Objective (RPO)** : the acceptable amount of data loss measured in time.
- **Recovery Time Objective (RTO)** ***: t***he earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.
- **Work Recovery Time (WRT):** is the remainder of the overall MTD value.



Practical BCP Development for An Organization
- Develop Recovery Strategies

- *Higher level* recovery strategies identify the order in which processes and functions are restored.
  - BCP committee can define *Higher level* recovery strategies

- *System-level* recovery strategies define how a particular system is to be restored.
  - System administrators and other IT personnel need to be involved in the development of recovery strategies for IT assets.

Practical BCP Development for An Organization

- Develop Recovery Strategies

- **Business Process Recovery:** Required roles, Required resources, Input and output mechanisms, Workflow steps, Required time for completion, Interfaces with other processes, etc.
- **Facility Recovery:** Hot site, Warm site, Cold site, Tertiary Sites, Reciprocal Agreements, Redundant Sites
- **Supply and Technology Recovery:** Network and computer equipment, Environment issues (HVAC), etc.
- **User Environment Recovery:** user working computers, ect.
- **Data Recovery:** full backup, differential backup, incremental backup

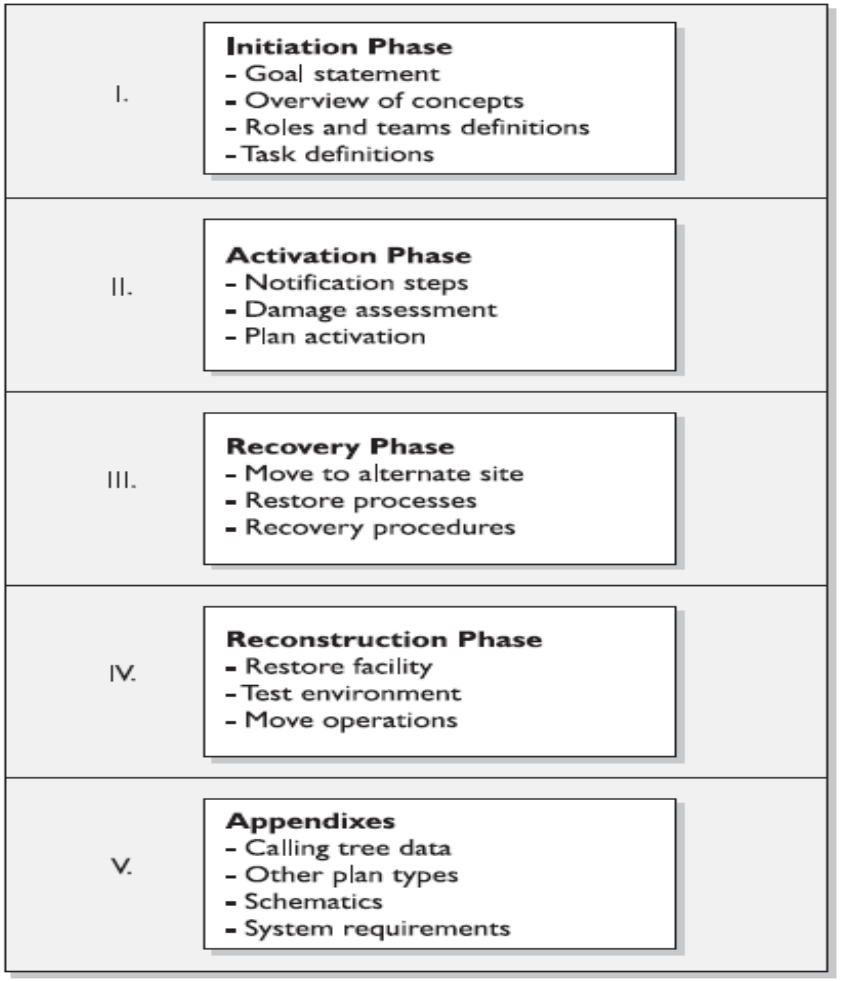
Practical BCP Development for An Organization

- Establish Contingency Teams and Duties

- Damage assessment team
- Legal team
- Media relations team
- Recovery team
- Relocation team
- Restoration team
- Salvage team
- Security team

Practical BCP Development for An Organization
- BCP Implementation

- Version control should be maintained.
- Copies should be provided to personnel for storage both onsite and offsite.



Practical BCP Development for An Organization
- BCP Testing and Maintenance

A few different types of drills and tests can be used, each with its own pros and cons:

- Checklist Test
- Structured Walk-Through Test
- Simulation Test
- Parallel Test
- Full-Interruption Test

Organizations can keep the plan updated by taking the following actions:

- Make business continuity a part of every business decision.
- Insert the maintenance responsibilities into job descriptions.
- Include maintenance in personnel evaluations.
- Perform internal audits that include disaster recovery and continuity documentation and procedures.
- Perform regular drills that use the plan.
- Integrate the BCP into the current change management process.
- Incorporate lessons learned from actual incidents into the plan.

Practical BCP Development for An Organization

- BCP Overall Review