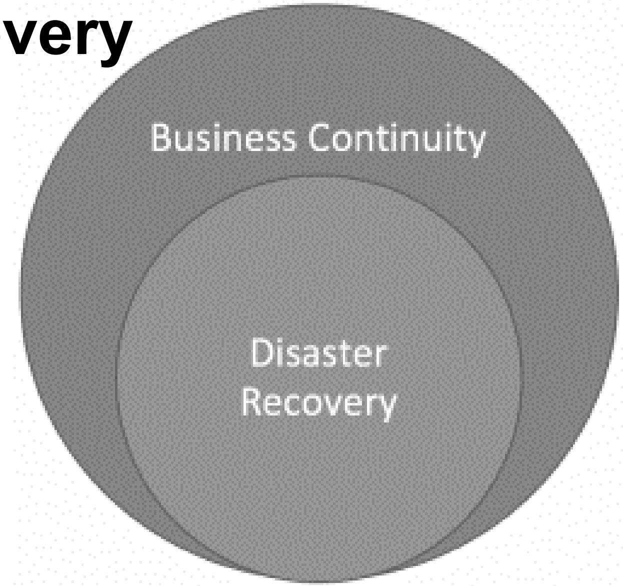
Incidents and response

Business Continuity and Disaster Recovery



Business continuity plan or **business continuity and resiliency planning,** is the process of creating systems of prevention and recovery to deal with potential threats to a company.

A Business Continuity Plan outlines a range of disaster scenarios and the steps the business will take in any particular scenario to return to regular trade. BCP's are written ahead of time and can also include precautions to be put in place. Usually created with the input of key staff as well as stakeholders, a BCP is a set of contingencies to minimize potential harm to businesses during adverse scenarios

A **disaster recovery plan** (**DRP**) is a documented process or set of procedures to recover and protect a Business IT infrastructure in the event of a disaster.

The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam).

Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan, sometimes erroneously called a **Continuity of Operations Plan** (COOP), is increasingly associated with the recovery of information technology data, assets, and facilities.

Incidents and response

Business Continuity and Disaster Recovery

The different strokes between BC and DR			
#	**Prospective**	**Business Continuity (BC)**	**Disaster Recovery**
1	Objective	To ensure that a Business entity is able to retain the Business as Usual (BAU) state	To ensure that a Business entity will be able to revert to its Business as Usual BAU state
2	Core	The Critical Business Processes	The recoverability of each Business Units
3	Responsibility	Whole Business entity	Each Business Unit (BU)
4	Accountability	Senior Management	Each BU Management
5	Trigger	Disruption	Disruption and Disaster
6	Key Task	Business Impact Analysis	Build Recoverability capability
7	Risk handling	Identify & Profile risk to plan	No risk impact as Incident occurred
8	Risk, Threat, Problem & Incident Management	Identify, analyse and profile Risk and Threats	No risk from any threat, Problem and Incident Management actions execited

Incidents and response

Business Continuity and Disaster Recovery

The common ground between BC and DR			
#	Prospective	Business Continuity	Disaster Recovery
1	Build appropriate capability and capacity when needed	BC Plan	DR Plan
2	Identify the situation	Scenario plan	Scenario plan
3	Testing	4 types	4 types
4	Approve and Publish	First time and on a regular interval	First time and on a regular interval
5	Exercise and Review	On a regular cycle	On a regular cycle
6	Training and Orientation	For all employee, contractors, suppliers and consumers	For all employee, contractors, suppliers and consumers
7	Compliance and Audit	To be done on every stage	To be done on every stage
8	Regulation, Law and Standards	To compel, drive and guide	To compel, drive and guide

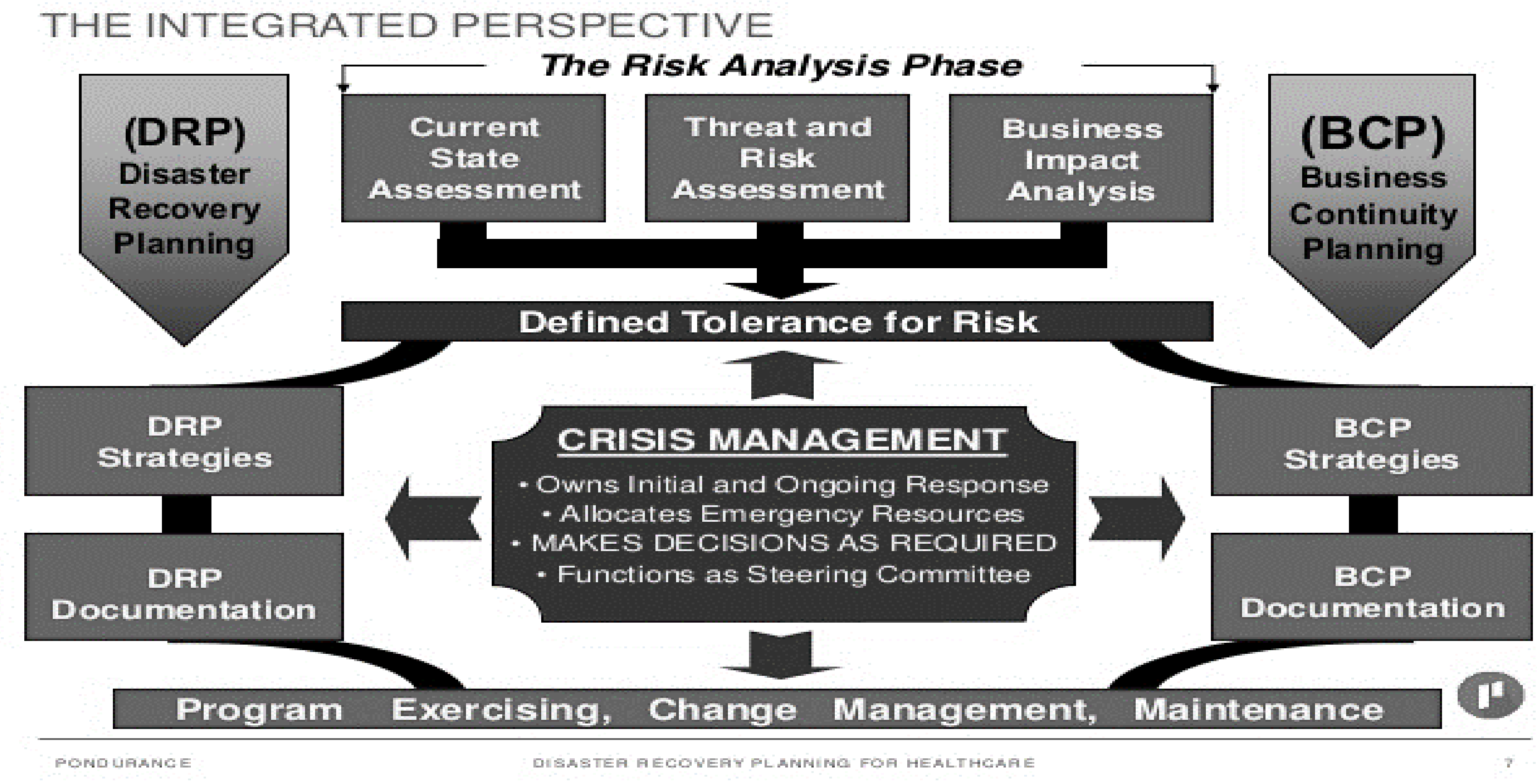
Incidents and response

Business Continuity and Disaster Recovery

Testing and Exercise			
#	Name	Description	First time and Continue
1	Table Top	A logical testing carried out from the desktop of the team	First time only
2	Facilitated Workshop	Attended by all the Function Heads and the required leads to recreate the scenarios, swim-lanes, flow charts	First time only
3	Backend/non-destructive	Attended by a few selected employee other than the cote team and done without hampering the BAU	First time only
4	Full/Destructive	A full fledged simulated exercise of one or more scenarios including whole of the organisation impacting the BAU, intentionally	First time and cyclical

Incidents and response

Business Continuity and Disaster Recovery



THE INTEGRATED PERSPECTIVE

The Risk Analysis Phase

(DRP) Disaster Recovery Planning

Current State Assessment

Threat and Risk Assessment

Business Impact Analysis

(BCP) Business Continuity Planning

Defined Tolerance for Risk

DRP Strategies

DRP Documentation

CRISIS MANAGEMENT

- Owns Initial and Ongoing Response
- Allocates Emergency Resources
- MAKES DECISIONS AS REQUIRED
- Functions as Steering Committee

BCP Strategies

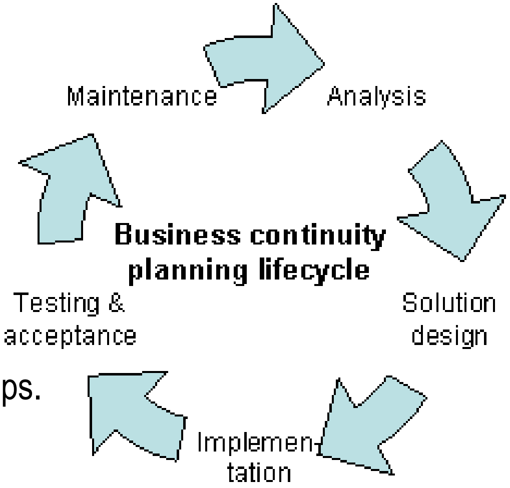
BCP Documentation

Program Exercising, Change Management, Maintenance

PONDURANCE DISASTER RECOVERY PLANNING FOR HEALTHCARE 7

Incidents and response

Business Continuity



Business continuity plan or **business continuity and resiliency planning,** is the process of creating systems of prevention and recovery to deal with potential threats to a company.

Threat and risk analysis (TRA)
After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

- Epidemic
- Earthquake
- Fire
- Flood
- Cyber attack
- Sabotage (insider or external threat)
- Hurricane or other major storm
- Power outage
- Water outage (supply interruption, contamination)
- Telecoms' outage
- IT outage
- Terrorism/Piracy
- War/civil disorder
- Theft (insider or external threat, vital information or material)
- Random failure of mission-critical systems
- Single point dependency

The above areas can cascade: Responders can stumble. During the 2002-2003 SARS outbreak, some organizations compartmentalized and rotated teams to match the incubation period of the disease. They also banned in-person contact during both business and non-business hours. This increased resiliency against the threat.

Incidents and response

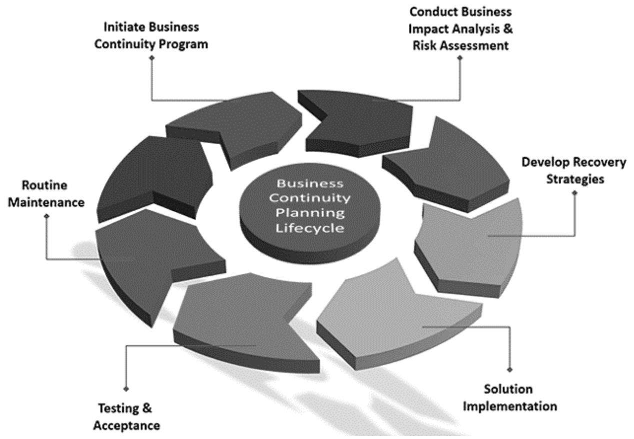
Business Continuity

Impact scenarios

Impact scenarios are identified and documented:

- need for medical supplies
- need for transportation options
- civilian impact of nuclear disasters

These should reflect the widest possible damage.


Initiate Business Continuity Program
Conduct Business Impact Analysis & Risk Assessment
Develop Recovery Strategies
Solution Implementation
Testing & Acceptance
Routine Maintenance
Business Continuity Planning Lifecycle

Solution design

Two main requirements from the impact analysis stage are:

For IT: the minimum application and data requirements and the time in which they must be available.

Outside IT: preservation of hard copy (such as contracts). A process plant must consider skilled staff and embedded technology.

This phase overlaps with ***disaster recovery planning***.

The solution phase determines:

- *crisis management* command structure
- *Telecomm. architecture* between primary and secondary work sites
- *Data replication method* between primary and secondary work sites
- *Backup site* - applications, data and work space required at the secondary work site

Incidents and response

Disaster Recovery

Obtaining top management commitment

For a disaster recovery plan to be successful, the central responsibility for the plan must reside on top management. It is also responsible for allocating adequate time and resources required in the development of an effective plan..

Establishing a planning committee

A planning committee is appointed to oversee the development and implementation of the plan. The planning committee includes representatives from all functional areas of the organization.

Performing a risk assessment

The planning committee prepares a risk analysis and a business impact analysis (BIA) that includes a range of possible disasters, including natural, technical and human threats.

Establishing priorities for processing and operations

At this point, the critical needs of each department within the organization are evaluated in order to prioritize them. Establishing priorities is important because of limited resources.

Incidents and response

Disaster Recovery

Determining recovery strategies

During this phase, the most practical alternatives for processing in case of a disaster are researched and evaluated. Alternatives, dependent upon the evaluation of the computer function, may include: hot sites, warm sites, cold sites, reciprocal agreements,.

Collecting data

In this phase, data collection takes place. Among the recommended data gathering materials and documentation often included are various lists.

Organizing and documenting a written plan

An outline of the plan’s contents is prepared to guide the development of the detailed procedures. Top management reviews and approves the proposed plan.

Developing testing criteria and procedures

Best practices dictate that DR plans be thoroughly tested and evaluated on a regular basis (at least annually

Testing the plan

Types of tests include: checklist tests, simulation tests, parallel tests, and full interruption tests.

Obtaining plan approval

Once the disaster recovery plan has been written and tested, the plan is then submitted to management for approval.

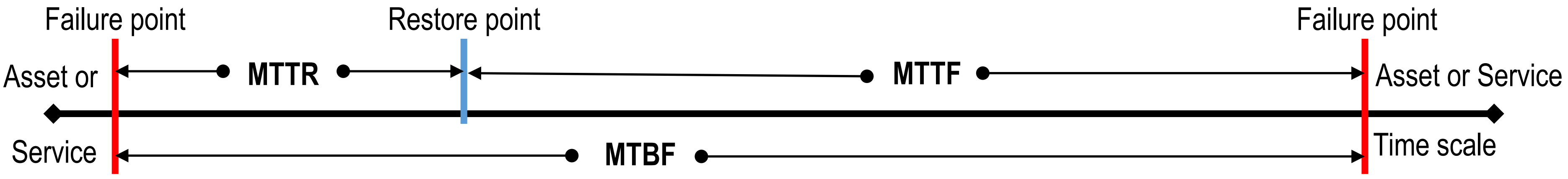
Incidents and response

Matrices for BD & DR

Important BC/DR Metrics

There are *7 important BC/DR metrics* that you should be tracking to grow and measure recovery plans:

1. **Recovery Time Objectives (RTO)** refers to the point in time in the past to which you will recover
2. **Recovery Point Objectives (RPO)** refers to the point in time in the future at which you will be up and running again
3. **Maximum Tolerable Downtime (MTD) or Maximum Tolerable Outagetime (MTO)** refers to a point in time by which time if the Business is back to BAU state that it may never be able to come back to its BAU state or will cease to exist or operate
4. **Mean Time to Recover (MTTR)** refers to the average time taken to repair or recover a service or product or both
5. **Mean Time to Fail (MTTF)** refers to the average time period between one restoration point to the next expected failure
6. **Mean Time Before Failure (MTBF)** refers to the average time period between one failure point to the next expected failure
7. The difference between your target and actual recovery time



Incidents and response

Matrices for BD & DR

Managing the uptime or availability of an asset or service

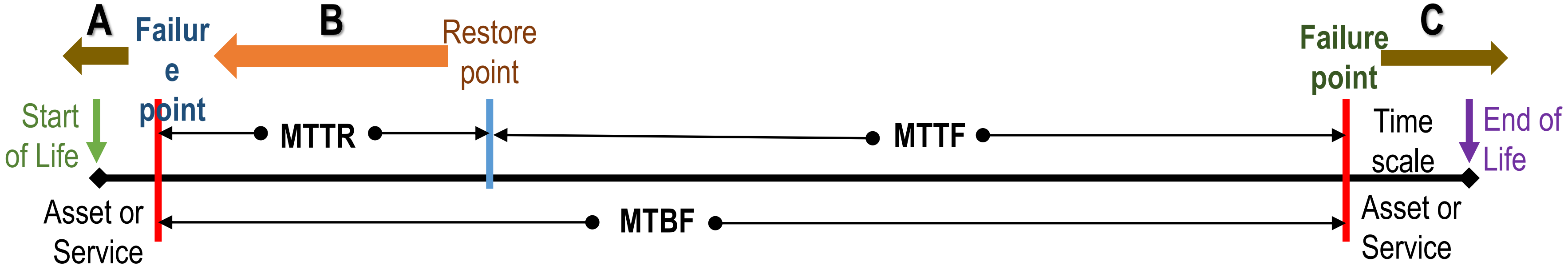
A Shift the first **Failure Point** to the left beyond the **Start of Life point**

B Shift the Restore Point to the left as close as possible if not on the first **Failure Point** **to r**educe the **MTTR** to ‘0’

C Shift the second **Failure Point** to the right beyond the End of Life point

Either A or C or a combination of both ensures that the Availability of the Asset or Service is 100% or almost i.e., no Down Time

Just achieving B ensures that the restoration effort is minimized or 0 for each individual incident situation or down time by taking advantage of the Problem Management Process or Incident Management Process, Capacity Management process or Availability Management process as defined by ITIL IT Service Management

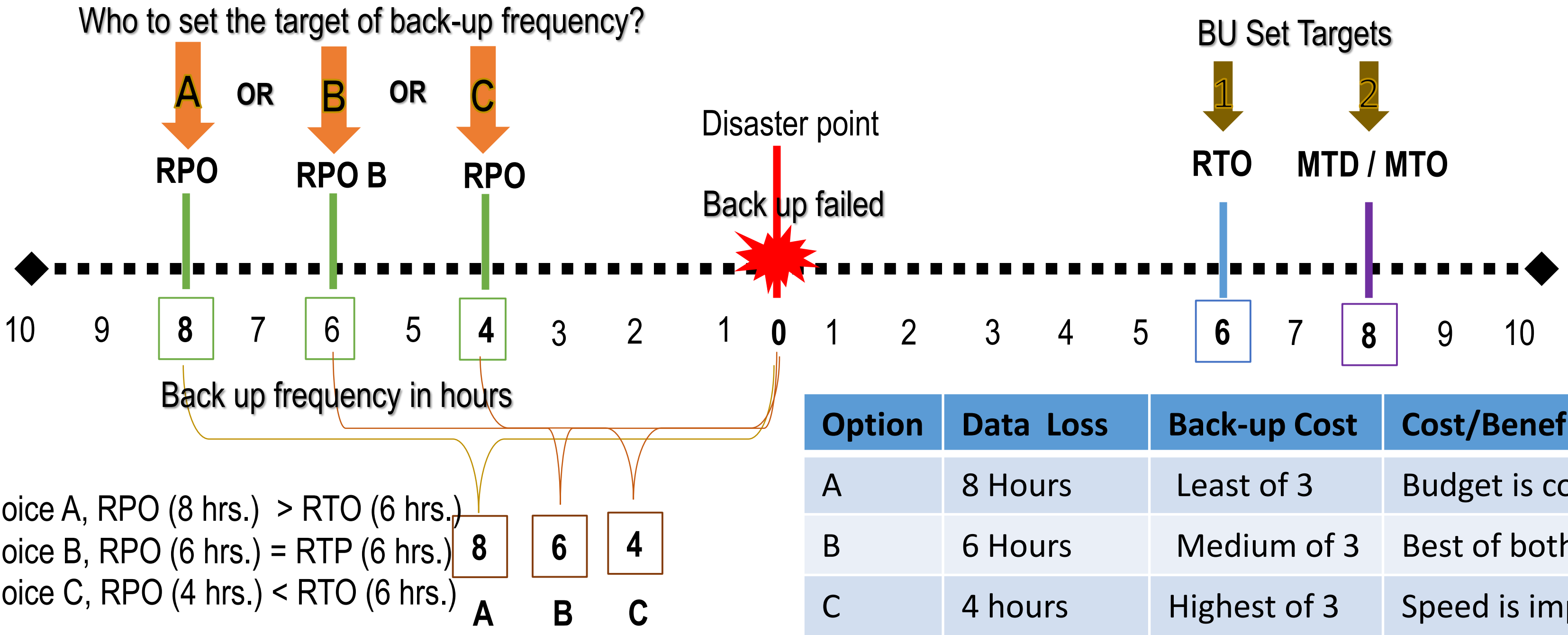


Incidents and response

Matrices for BD & DR

Managing the Recovery Time Objective (RTO) and Recovery Time Objective (RPO)

During the BCP Bus set the targets of MTD / MTO and the RTO as it impacts the ability of the business to restore BAU status A corresponding RPO will have to be agreed between the IT and the BUs, to which both parties will have to agree and the budget for the back-up solution required will have to be approved by Business while spent by IT.
IT can offer 3 options of Cost-Benefit to chose the appropriate one. There is no right no wrong. Its entirely a Business based decision. There can be 3 choices namely, RPO greater the RTO **(A)** or RPO equal to RTP **(B)** or RPO lesser than RTO **(C).**



1. Choice A, RPO (8 hrs.) > RTO (6 hrs.)
2. Choice B, RPO (6 hrs.) = RTP (6 hrs.)
3. Choice C, RPO (4 hrs.) < RTO (6 hrs.)

Option	Data Loss	Back-up Cost	Cost/Benefit
A	8 Hours	Least of 3	Budget is constraint
B	6 Hours	Medium of 3	Best of both
C	4 hours	Highest of 3	Speed is important