Technical -Approach

# ISO 22301 - Business Continuity Management System (BCMS)

**Infopercept**
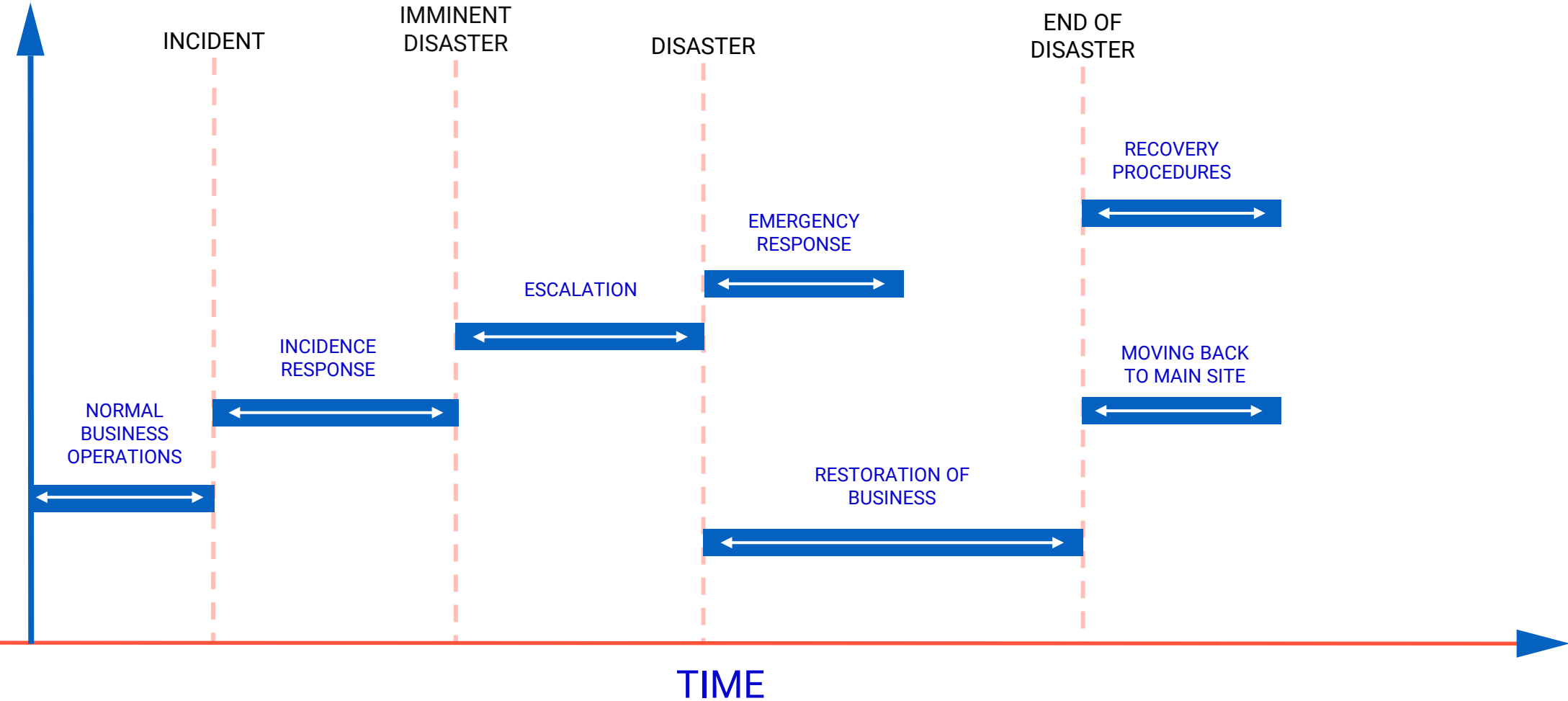
**INVINSENSE**

## Why we need BCMS ?

ISO 22301:2012 helps organizations in adapting the standard to manage the risks that threaten the smooth running of business and ensure its survival in the event of a disruption. this standard helps in identifying threats relevant to your business and critical business functions they could impact, it allows putting plans in place ahead of time to ensure organizations business doesn't come to a standstill.
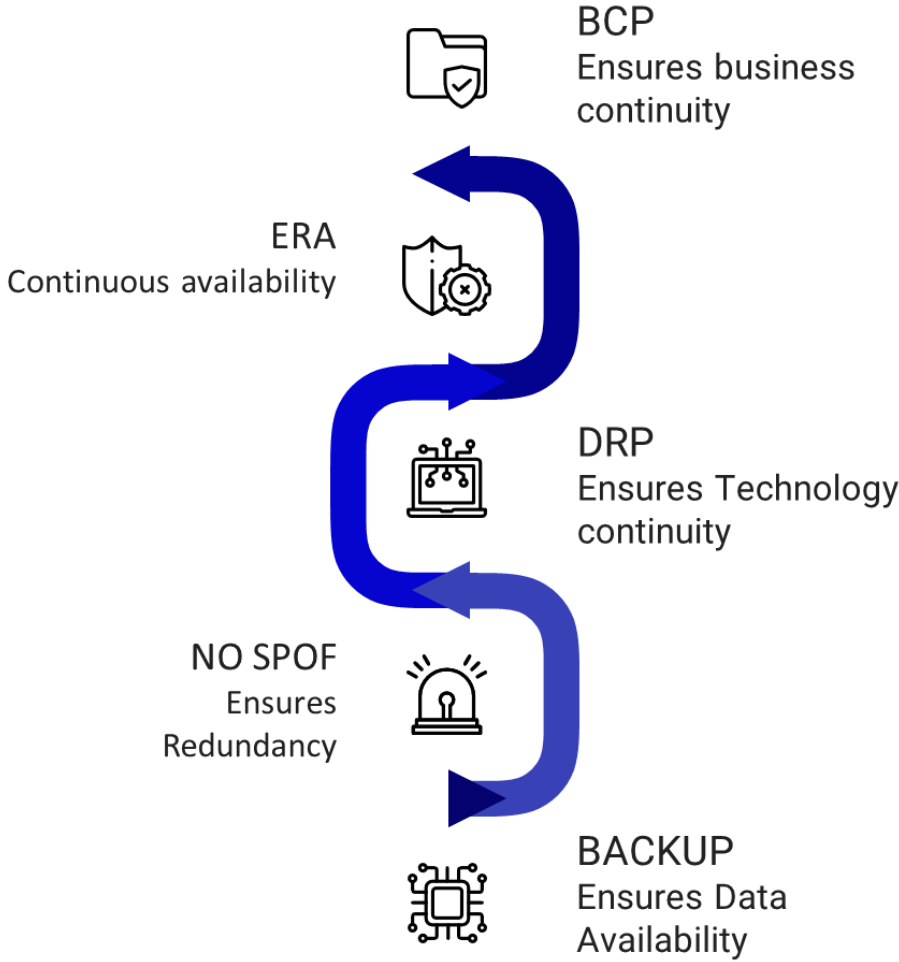
## What could be benefits of ISO 22301 ?

- Clear understanding of your entire organisation which can provide you with new opportunities for improvement
- Demonstrate that you meet the regional legal and regulatory requirements
- Ensure client confidence and gain new business opportunities.
- Ensure minimum disruptions to the services you offer during an organisational disruption.
- The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before after and during an event.
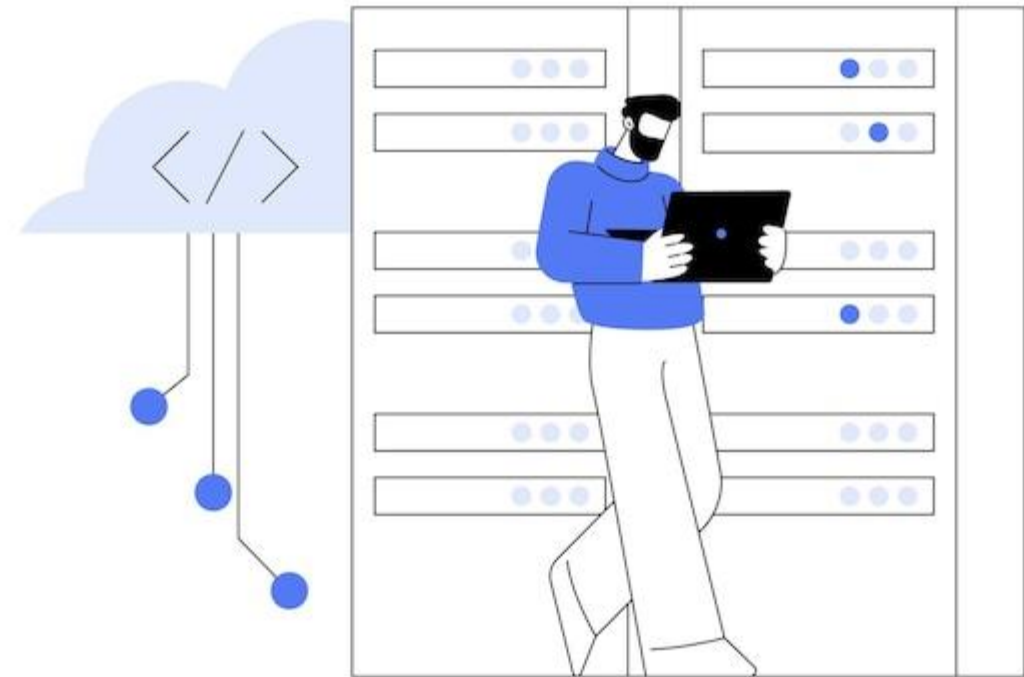
# Introduction

# What is BCP?

INCIDENT

IMMINENT DISASTER

DISASTER

END OF DISASTER

RECOVERY PROCEDURES

EMERGENCY RESPONSE

ESCALATION

INCIDENCE RESPONSE

MOVING BACK TO MAIN SITE

NORMAL BUSINESS OPERATIONS

RESTORATION OF BUSINESS

TIME

BCP
Ensures business continuity

ERA
Continuous availability

DRP
Ensures Technology continuity

NO SPOF
Ensures Redundancy

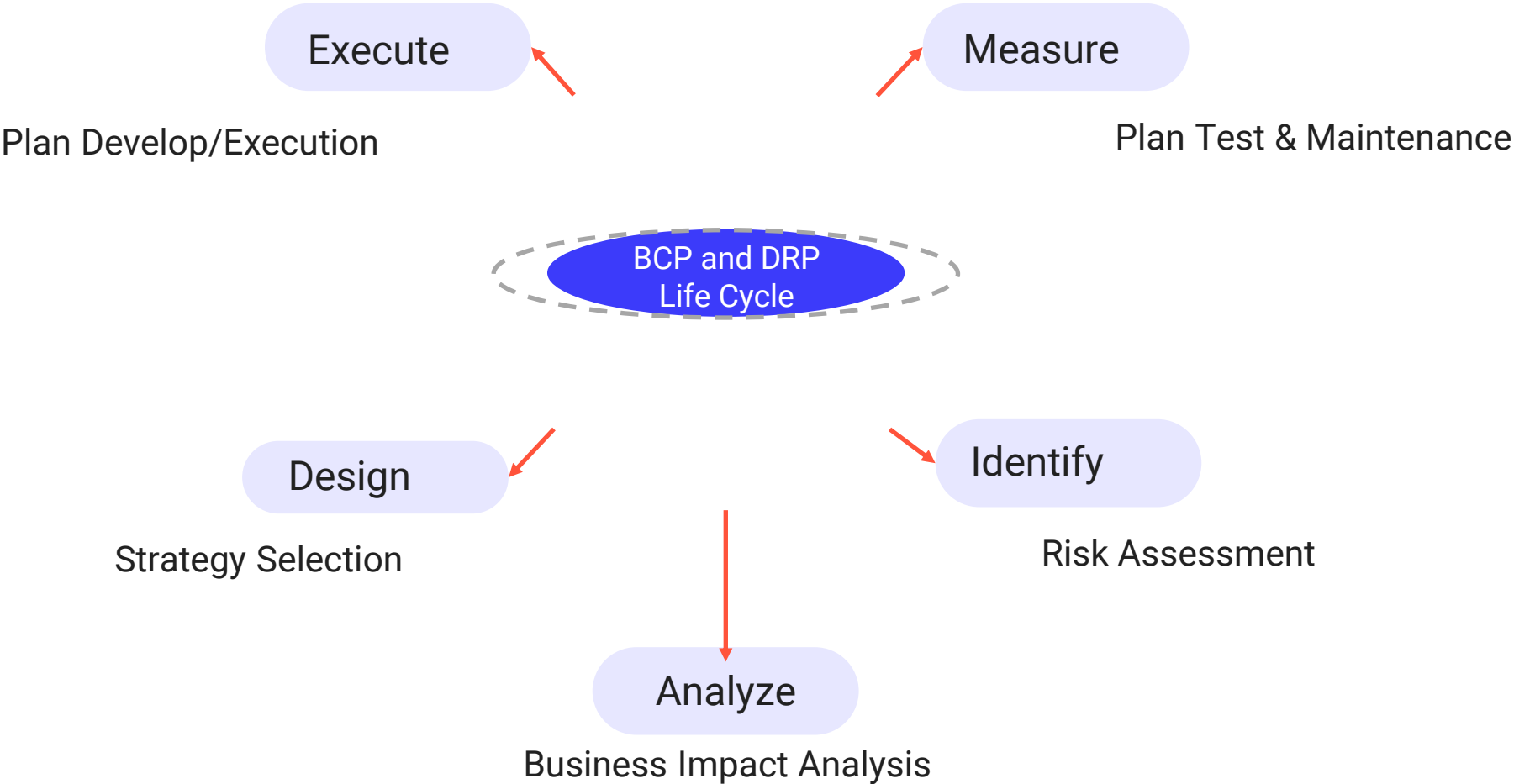BACKUP
Ensures Data Availability

# BCP and DRP

**BCP**

➤ Focuses on entire business BCP implies recovery of entire business BCP will include plans for people, facility, etc.

**DRP**

➤ Focuses mainly on IT / technology DRP is a subset of BCP dealing with the technology part DRP will include plans for servers, data, network, etc.

Execute

Plan Develop/Execution

Measure

Plan Test & Maintenance

BCP and DRP
Life Cycle

Design

Strategy Selection

Identify

Risk Assessment

Analyze

Business Impact Analysis

# Approaches to BCP

- There are different approaches to BCP
- Most of them speak the same language

**Impact Analysis**

**Develop**

**Approaches to BCP**

**Test & Maintain**

**Implement**

# Business Continuity Planning



**⌐ Infopercept**

1. Project Initiation and Planning
2. Risk Assessment
3. Business Impact Analysis
4. Strategy Selection
5. Risk Reduction and Strategy implementation
6. Emergency Response and Operations
7. Developing and Implementing Business Continuity Plans
8. Plan Testing
9. Crisis Management
10. BCP Awareness and Training

- Objective
  - Scope of BCP
  - Structure of BCP Management
  - Missing of BCP
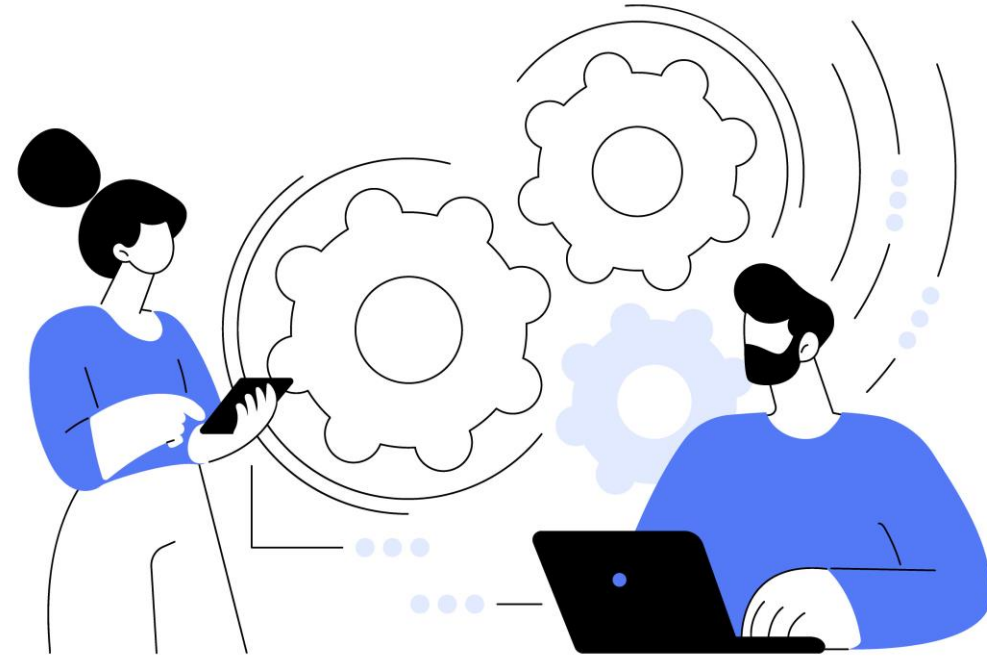  - Project Plan
- Identify the scope of the BCP
- Detailed project plan
- BCP organization structure
  - BCP steering committee
  - BCP implementation team
  - Functional experts
- Define BCP team and responsibilities
- Management sign off

# Risk Assessment

- Objective
  - ▸ Understand key risk to assets of the business
  - ▸ Suggest mitigation that can be part of the system

- Collect information about threat agents, threat events and vulnerabilities
- Analyze Policy and Standards Compliance
- Perform asset sensitivity analysis
- Perform a threat analysis
- Perform a vulnerability analysis
- Perform a risk analysis

## BIA provides answers to the following questions:

- Which business functions are critical for survival?
- What is the sequence of restoration of these functions?
- How these functions are interrelated?
- What are the financial consequences?
- What is the impact on revenue, reputation, market share?
- What are the minimum resources required to recover the critical business functions?
- Identify critical business functions

# Business Impact Analysis ( BIA )
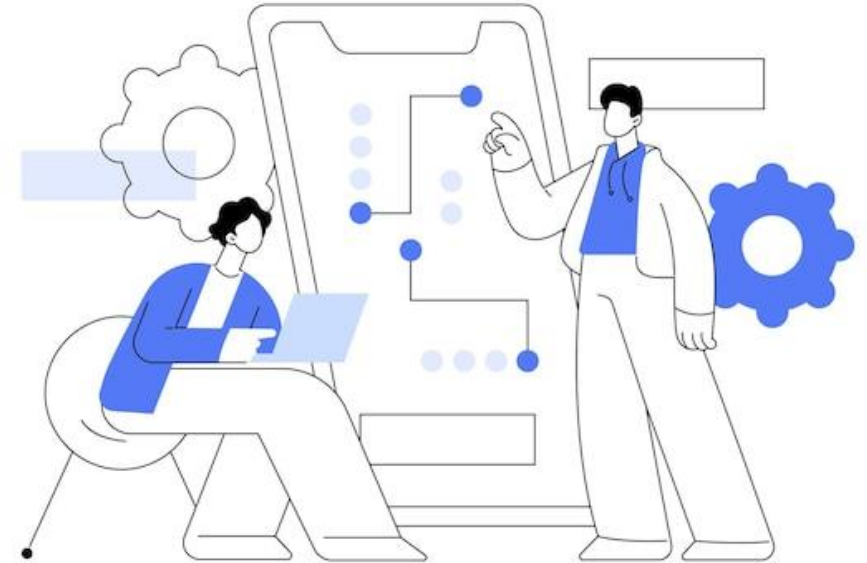


- Prioritize critical processes

- Impact Analysis for critical processes
  - ❯ Revenue?
  - ❯ Reputation?
  - ❯ Market share?
  - ❯ Quantitative / Qualitative

- Identify interrelation between critical processes and other

  processes
  - ❯ Link between different critical processes and how they affect the functionality of critical processes

- Link between different critical processes and how they

  affect the functionality of critical processes

- Identify priorities for restoration
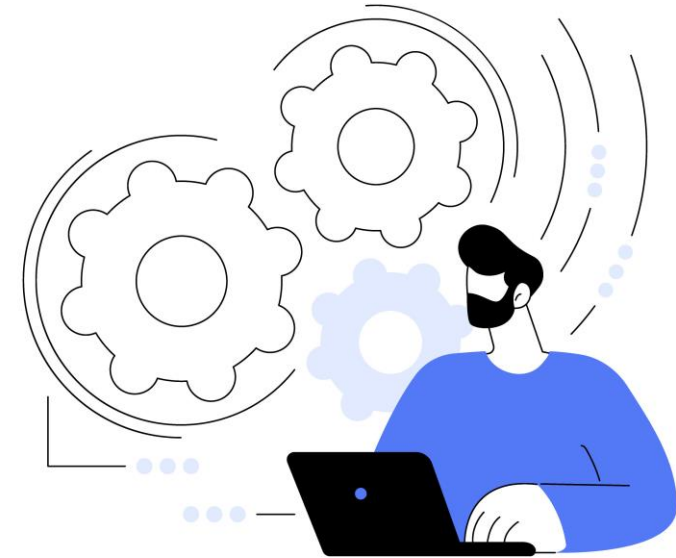
- Presentation of Impact Analysis

- RTO – Recovery Time Objective

- RPO – Recovery Point Objective

Objectives

- Identify critical processes
- Identify Maximum outage that the business can sustain before significant damage (RTO)
- Identify RPO

## Definition

"Recovery strategies are a set of predefined and management approved actions that will be followed and implemented in response to a business interruption."

## Key points

- Recovering within the agreed time frame, all the mission critical business systems as identified by thmiggge BIA
- Compiling the resource requirement for the recovery
- Identifying alternatives available for recovery

- Objective
  - Select strategies for business continuity based on cost benefit analysis and the RTO & RPO

- Business recovery strategies

- Plan Business Recovery Strategies to meet the BIA

- Main categories for strategies
  - Business Recovery
  - Facilities and Support services
  - Personnel
  - Technical / Operational
  - Software / Data
  - Communication

- Plan Business Recovery Strategies to meet the BIA objectives

- Main categories for strategies

  - Business Recovery
  - Facilities and Support services
  - Personnel
  - Technical / Operational
  - Software / Data
  - Communication

- Develop detailed plans for each and every key process identified
- Define how a process will transition from Incident response phase to Business continuity phase
- Define procedures for

  - How to move to alternate locations
  - How to make business operational at main site
  - How to bring a business back to the main site

- Objectives

  Develop detailed plans for all processes and activities related to the

  continuity

- Emergency procedures
  - Actions to be taken
  - Public relations management
  - Effective liaison with public authorities e.g. police, fire dept, local Govt
- Fallback Procedures
  - Moving essential business activities or support services to alternative temporary locations
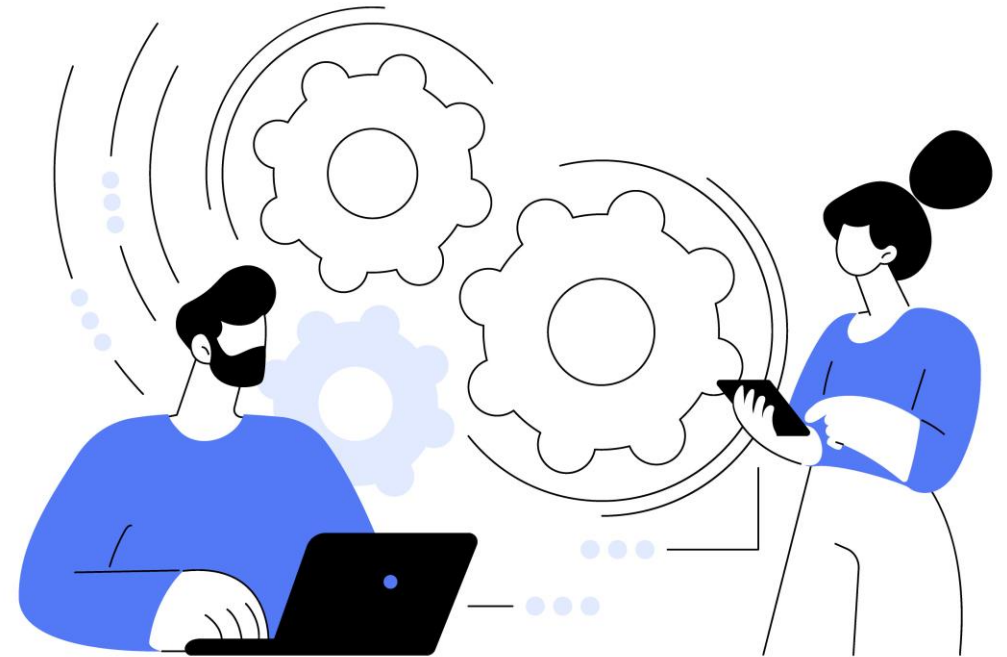  - Bring business process back into operation in required time scale
- Resumption Procedures
  - Actions for returning to normal business operations
- Maintenance Schedule
  - How and when to test the plan
  - How to maintain the plan
- Responsibility allotment

- Objectives
  - Test the BCP for continuous improvement
  - Ensure BCP is up-to-date

**Topics**

- **Testing the BCP**

- **Types of Tests**

- **Maintaining and reassessing the plans**

- Component / Walk-through tests

- Basic: Single Component - to be tested at least once a year

  - Availability of BCP
  - Retrieve vital records from off site
  - Contact staff, suppliers, other contacts
  - Check lead time for critical equipment
  - Check currency of the lists in the plan
  - Confirm alternate site readiness
  - Spot check of vital records
  - Test BCP representatives knowledge of departmental plan

- Telephone notification call tree – Four times a year

- Walk-through – Once a year, or change of plan or member

# Types of Tests

- Integrated test :
  - ❯ Involving integrating any number of components in the order in which they would occur during actual recovery operation

- Incident Simulation :
  - ❯ Involves development and use of pre-written test scenarios or test scripts for disaster events

- Partial Simulation :
  - ❯ Several business units will be involved

- Full Simulation :
  - ❯ This is the ultimate business continuity plan test, which activates the total business continuity plan, also called a Full Interruption Test or Mock Disaster Test.

- Regular review and updates

- Change control procedure

- Situations necessitating updating the plans:

  1. Acquisition of new equipment

  2. Upgrading the operational systems

  3. Changes in:

     › Personnel

     › Addresses or telephone numbers

     › Business strategy

     › Location, facilities and resources

     › Legislation

     › Contractors, suppliers and key customers

     › Processes, or new/withdrawn ones

     › Risks (Operational and Financial)

- Objectives
  - Ensure that all crisis coordination activities are properly planned
  - Establish communication protocols in case of disaster
  - Identify components of proactive public relations program
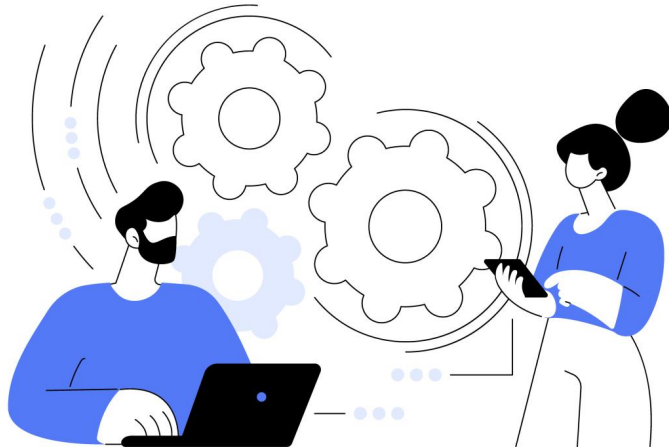


- Internal (Corporate and business level groups)
  - External groups
  - External agencies

- Identify external agencies with which liaison is required
  - Local / State / National
  - Emergency services
  - Civil defense authorities
  - National weather bureau
  - Other Governmental agencies

- Identify stakeholder groups and establish essential communication plans
  - Owners / stockholders
  - Employees and their families
  - Key customers
  - Key suppliers
  - Corporate / headquarters management
  - Other stake holders

- Establish and exercise media handling plans
  - Policies and procedures for media handling
  - Plans and preparation for media handling
  - Implement and exercise media handling plans

- Objectives
  - Train all user on their roles and responsibilities

- Prepare a Corporate Awareness Training Program

- Establish objectives and components of training program

- Identify functional training requirements

- Develop training methodology

- Develop awareness program
  - Management
  - Team members
  - New employee orientation

- Acquire or develop training aids

- Identify external training opportunities

- Identify vehicles for corporate awareness

# About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

## Imprint
© Infopercept Consulting Pvt. Ltd.

## Address
3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

## Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed under standing and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

## Global Office

### United State of America
+1 516 713 5040

### United Kingdom
+44 2035002056

### Sri Lanka
+94 702 958 909

### Kuwait

### India
+91 9898857117