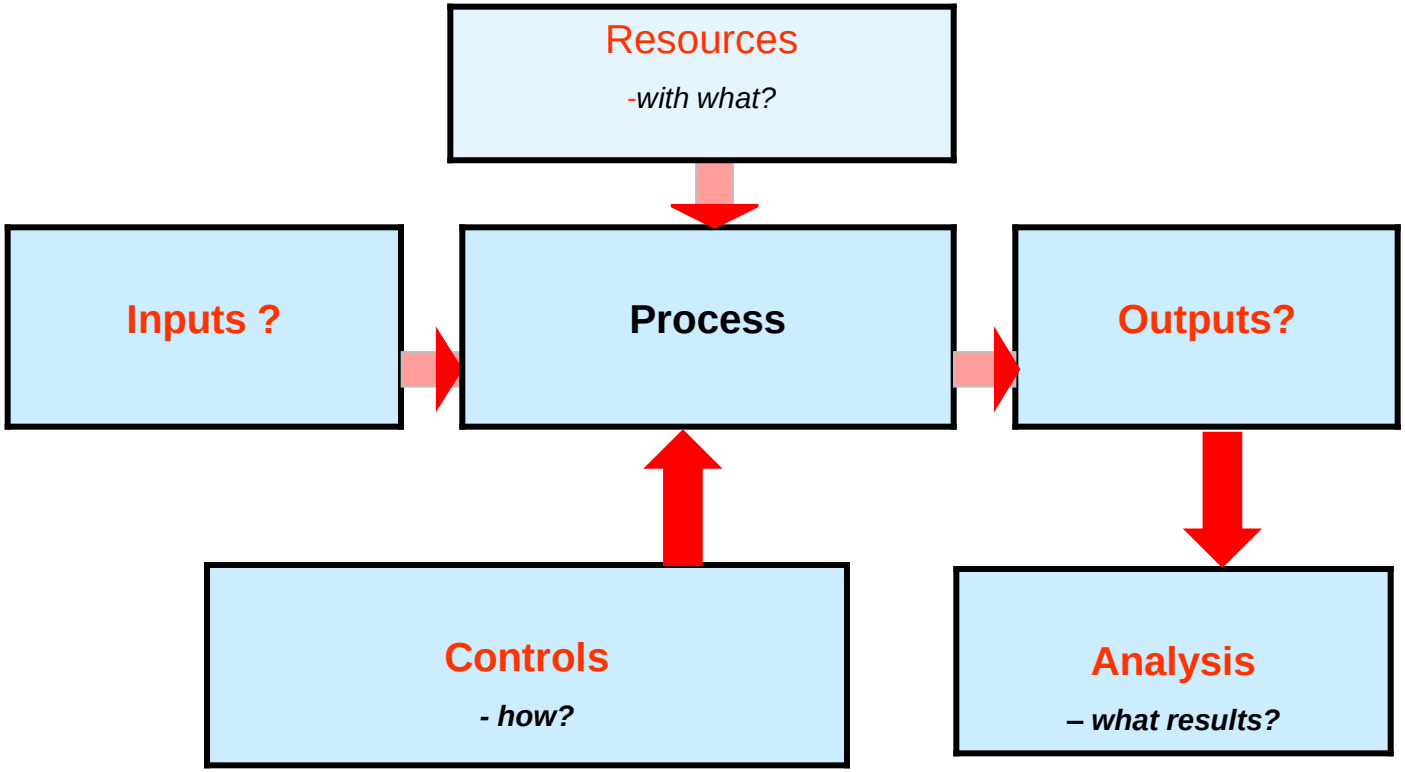
Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)

THE PROCESS – What is a process



Purpose of BCMS

- Introduction to Business Continuity Management
  - The application of ISO 22301
  - The development of BCMS
  - Compatibility with management system standards
  - Legal compliance – management system standards
  - The concepts underpinning BCMS
  - Continuous improvement based on the Plan-Do-Check-Act (PDCA) cycle
  - The benefits of BCMS

Factors affecting bcms

History of ISO 22301 bcms

- **History of ISO 22301:2019**
  - **1999** Survey conducted by **Chartered Management Institute**
  - **2004** UK Civil Contingencies Act
  - **2006 BS 25999-1** issued
    - » Consistence with **ISO 9001**& **ISO 14001** & **ISO/IEC 27001**
    - » Adopted **PDCA** model
  - **2007 Cabinet Office report** on Business Continuity Management
  - **2007 BS 25999-2** issued
  - **2012 ISO 22301:2012issued**
  - **2019 ISO 22301:2019 Issued**

History of ISO 22301 bcms (CONTINUED)

- Aims
  - Provides a specification to assess the organisation's ability to meet regulatory and customer needs
  - Contains those requirements that can be objectively audited
  - Successful implementation can be used to assure interested parties that an appropriate BCMS is in place
  - Utilises *Plan-Do-Check-Act* (PDCA) cycle in developing, implementing and improving the effectiveness of a BCMS

Consistent with other standards

ISO 9001: Quality management systems

ISO 14001: Environmental management systems

ISO Guide 73: Risk management -- Vocabulary

ISO 22300: Societal security -- Terminology

ISO 31000: Risk management -- Principles and guidelines

ISO 22313: Business continuity management systems – Guidance

ISO 27001: Information security management systems

ISO 27031: Guidelines for ICT readiness for business continuity

ISO 24762: Guideline on ICT DR services

Legal compliance

LEGAL COMPLIANCE – MANAGEMENT SYSTEM STANDARDS

The progressive development of customer-driven standards and the increase in world-wide legislation involving BCMS, as well as quality, environmental, and occupational health and safety management systems, is focusing organisations on developing integrated management systems to address legal requirements and process-based management systems.

Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)

How to preserve critical business functions in the face of a disaster.

What is a Business Continuity?

Is the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

(Source: ISO 22313/22301)

What is a Business Continuity Management System?

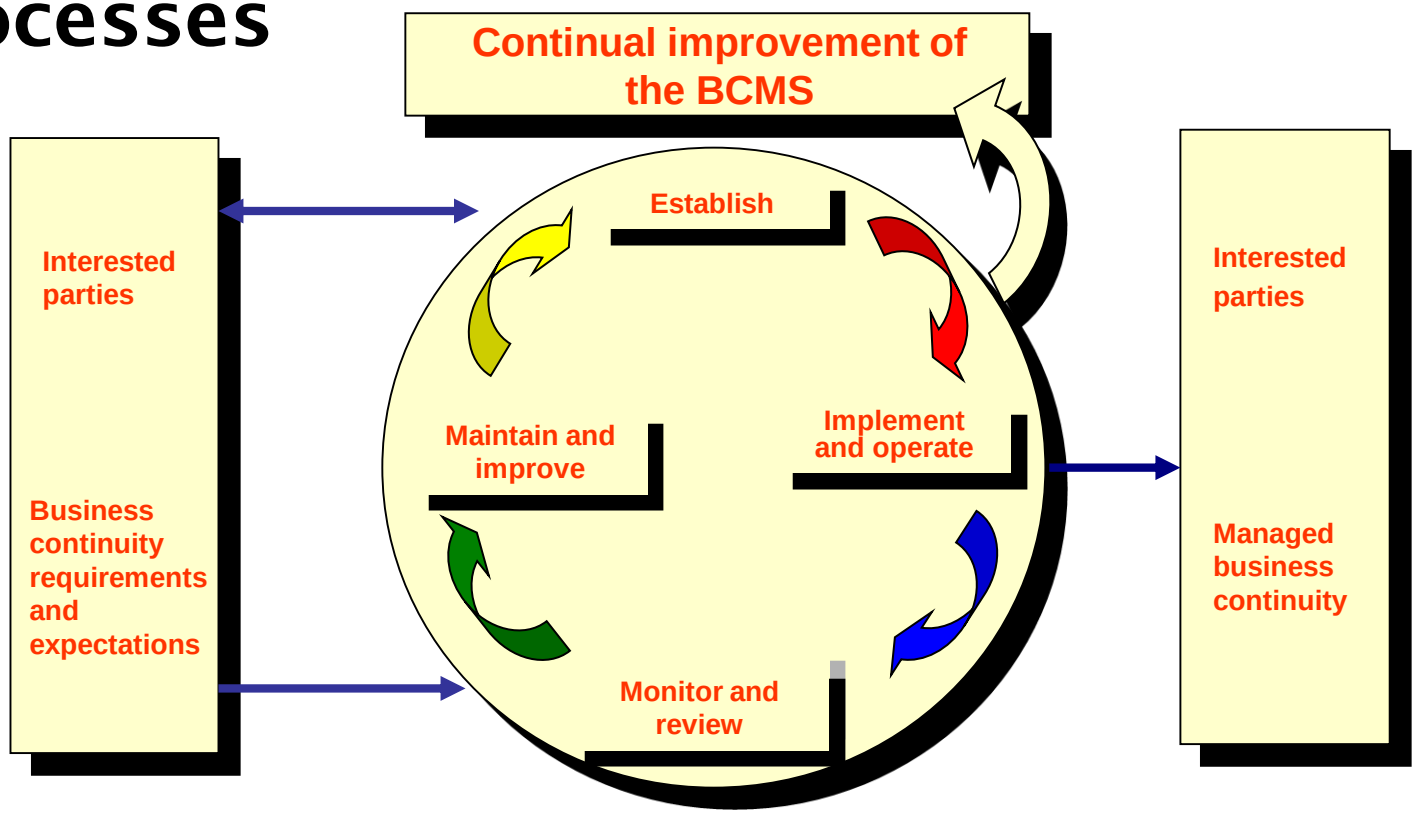
A business continuity management system emphasises the importance of:

- Understanding the organisations needs and the necessity for establishing business continuity management policy and objectives,
- Implementing and operating controls and measures for managing an organisation's overall capability to manage disruptive incidents,
- Monitoring and reviewing the performance and effectiveness of BCMS, and
- Continual improvement based on objective management

What is a Business Continuity Management System?

ISO 22313/ 22301 (2012)

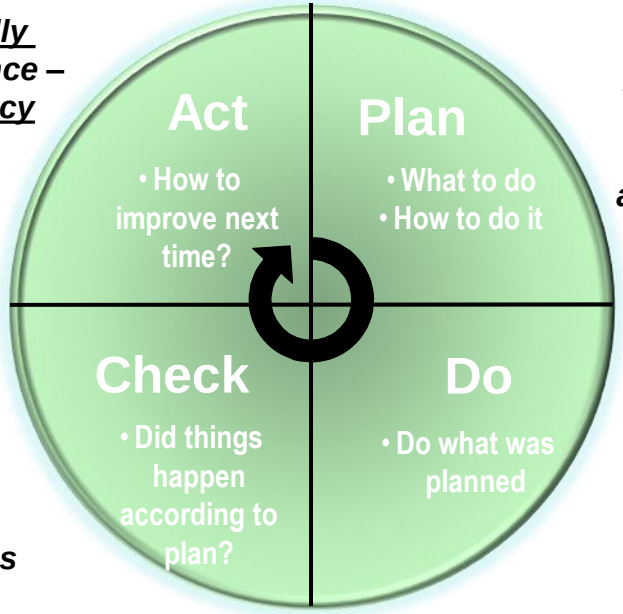
PDCA cycle applied to BCMS processes



PLAN-DO-CHECK-ACT CYCLE & CONTINUAL IMPROVEMENT

Take actions to <u>continually improve</u> process performance – <u>effectiveness</u> and <u>efficiency</u>

Establish <u>objectives</u> necessary to deliver results in accordance with customer requirements and the organisation's policies



<u>Monitor and measure</u> processes and product against policies, objectives and requirements

<u>Implement</u> the processes

Application of the PDCA cycle

- **PLAN**
  - Understand business continuity requirements
  - Demonstrate top management commitment
  - Determine the scope
  - Establish policy and objectives
  - Determine the resources needed
  - Develop necessary documented information and controls

.

Application of the PDCA cycle (continued)

- **DO**
  - Analyse the impacts of incidents and disruptions
  - Identify and assess the risks
  - identify and evaluate options for the treatment of risks
  - select control objectives and controls
  - Prepare business continuity plans
  - Develop a BCM strategy
  - Develop business recovery plans
  - Develop exercise schedules and reports.

Application of the PDCA cycle (continued)

- **CHECK**
  - Monitor, measure, analyse and evaluate performance against the BCMS policy and objectives and the effectiveness of each process
  - Evaluate procedures
  - Conduct Internal audits
  - Establish a management review process

Application of the PDCA cycle (continued)

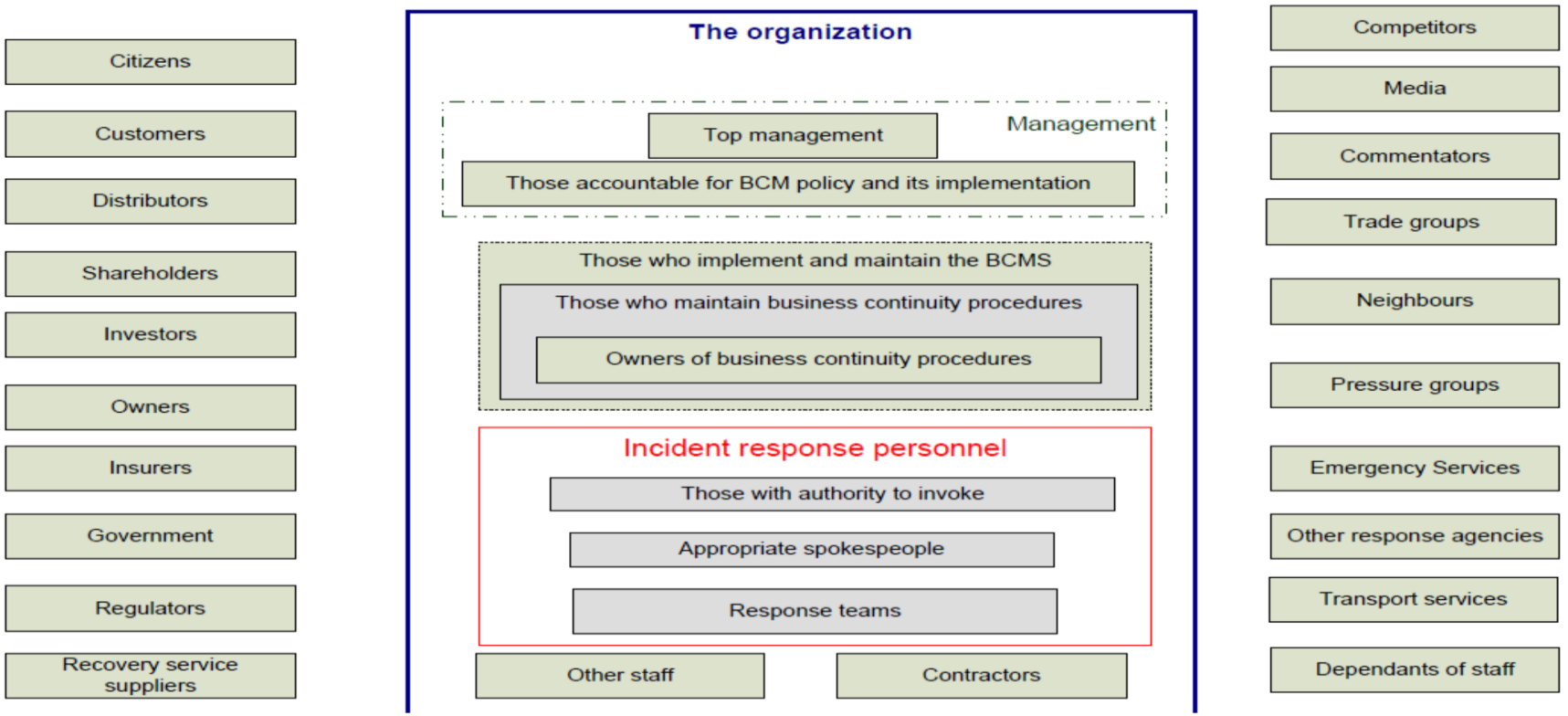
- **ACT**
  - Identify nonconformity and implement appropriate corrective action
  - Continually improve the suitability, adequacy and effectiveness of the BCMS

Elements of Business Continuity Management

ISO22313 (2012)

Interested Parties

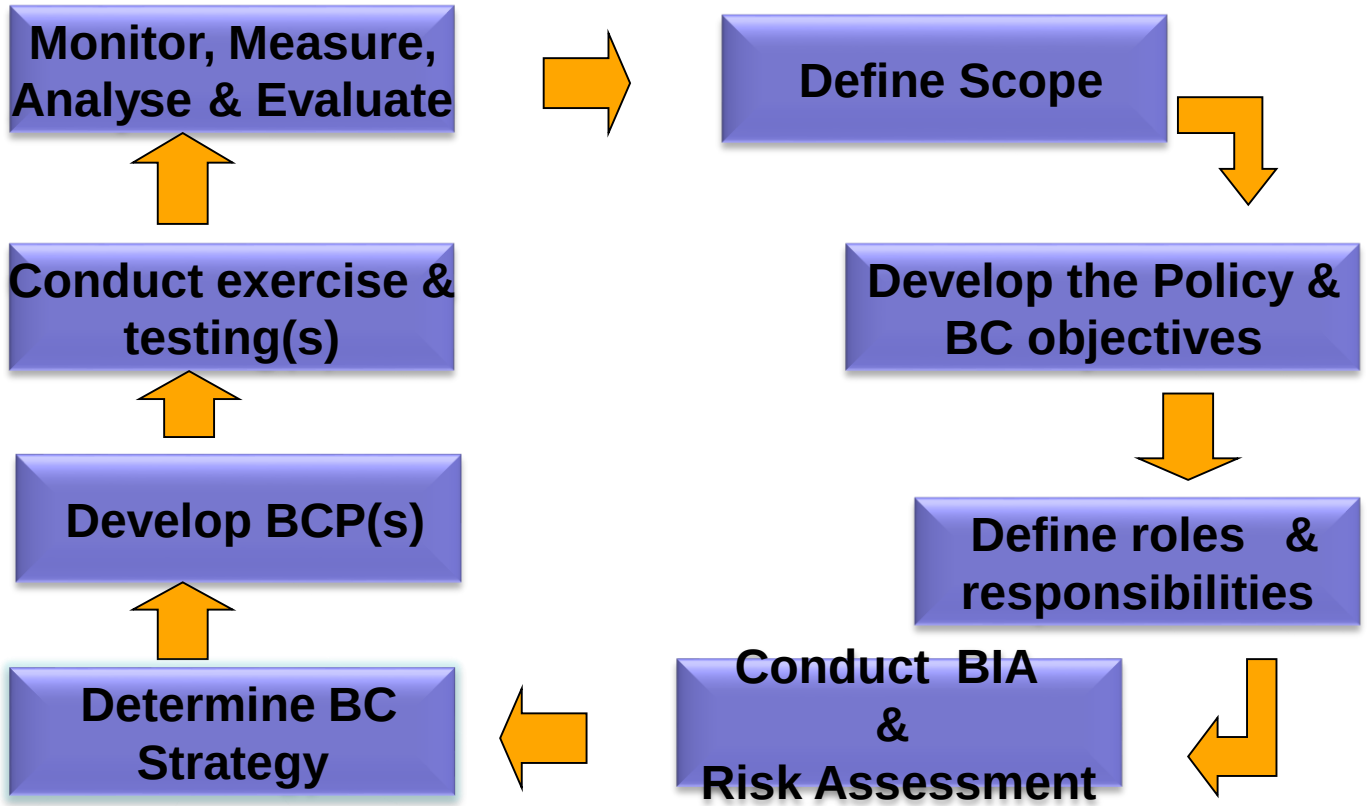
Adapted for the NHS from ISO22313


Citizens
Customers
Distributors
Shareholders
Investors
Owners
Insurers
Government
Regulators
Recovery service suppliers
The organization
Management
Top management
Those accountable for BCM policy and its implementation
Those who implement and maintain the BCMS
Those who maintain business continuity procedures
Owners of business continuity procedures
Incident response personnel
Those with authority to invoke
Appropriate spokespeople
Response teams
Other staff
Contractors
Competitors
Media
Commentators
Trade groups
Neighbours
Pressure groups
Emergency Services
Other response agencies
Transport services
Dependants of staff

Process – Based BCMS

- Establishing a BCMS
- Processes
- BCMS documentation
- Business continuity policy and objectives
- Documented information
- Records
- Control of documented information and records
- Continual improvement
- The purpose of monitoring and improvement
- Implications

To implement an BCMS



Elements of Business Continuity Management 1

ISO22313

Business Impact Analysis

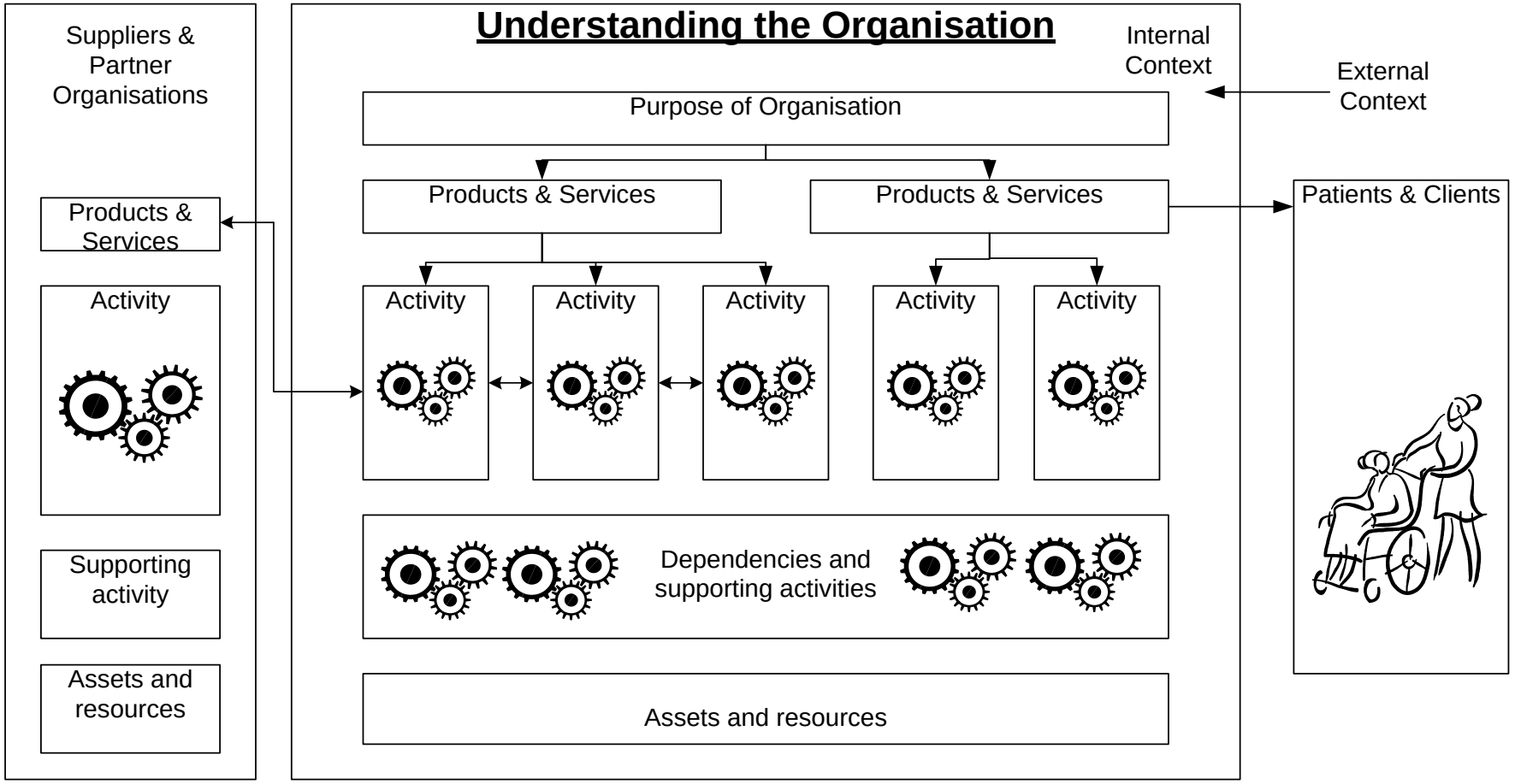
Effective Business Continuity Management (BCM) starts with identifying all functions within and services delivered by the organisation.

A business impact analysis (BIA) is the primary tool for gathering this information and then assigning each with a level of criticality.

Business Impact Analysis (BIA)

- Effective Business Continuity Management (BCM) starts with identifying all functions within and services delivered by the organisation.
- A business impact analysis (BIA) is the primary tool for gathering this information and then assigning each with a level of criticality.
- Prioritisation of activities including Recovery Time Objectives (RTO) and Maximum Tolerable Period of Disruption (MTPD)
- Identify resources required for maintenance of priority services
- RPO – Recovery Point Objective

Understanding the Organisation

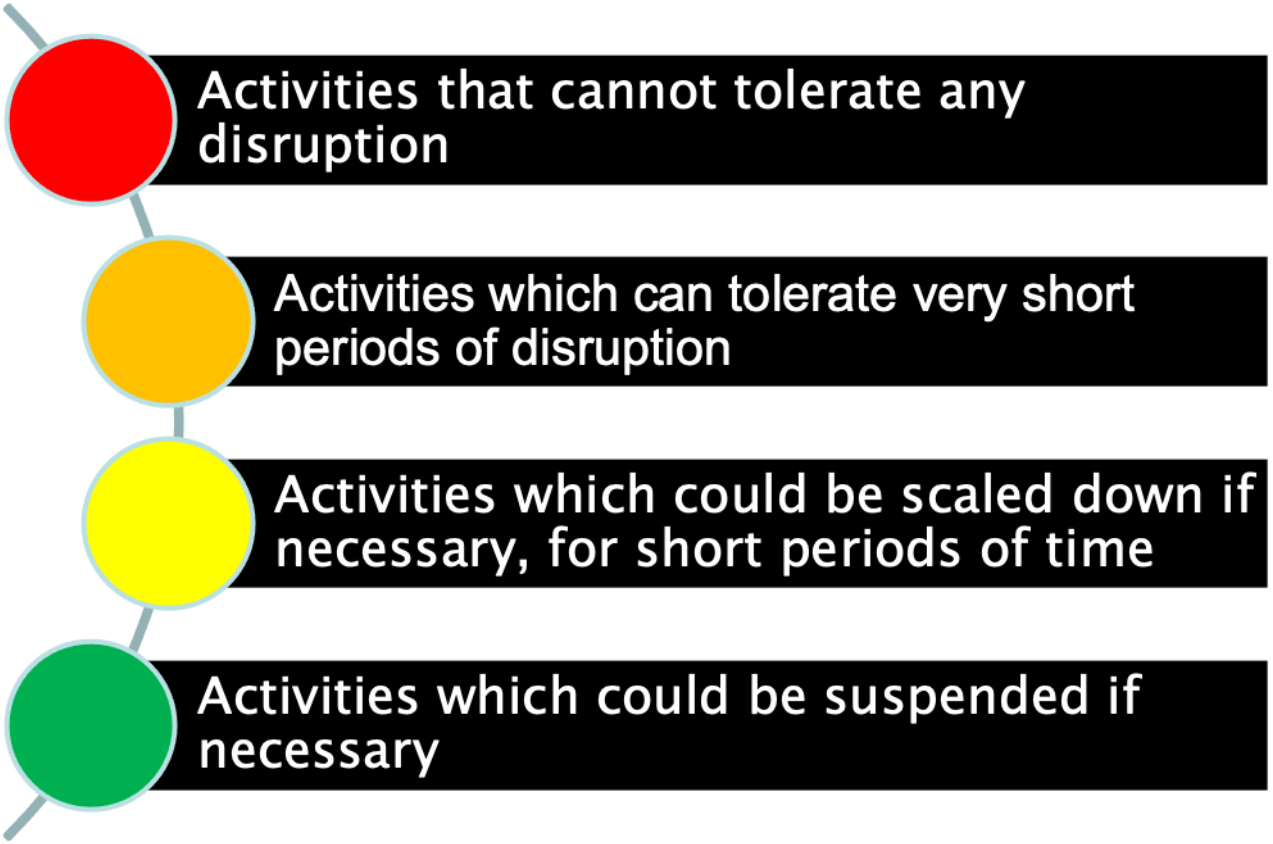


Adapted for the NHS from ISO22313

Business Impact Analysis (BIA) Template

- Risk assessment and treatment
- Prioritisation of activities including Recovery Time Objectives (RTO) and Maximum Tolerable Period of Disruption (MTPD)
- Identify resources required for maintenance of priority services

Business Impact Analysis



Source: ISO 22313

The BCP domain addresses:

- Continuation of critical business processes when a disaster destroys data processing capabilities
- Preparation, testing and maintenance of specific actions to recover normal processing (the BCP)

Disasters – natural, man-made

- Fire, flood, hurricane, tornado, earthquake, volcanoes
- Plane crashes, vandalism, terrorism, riots, sabotage, loss of personnel, etc.
- Anything that diminishes or destroys normal data processing capabilities

Disasters are defined in terms of the business

- If it harms critical business processes, it may be a disaster
- Time-based definition – how long can the business stand the pain?
- Probability of occurrence

Broad BCP objectives - CIA

- Availability – the main focus
- Confidentiality – still important
- Integrity – still important

BCP objective

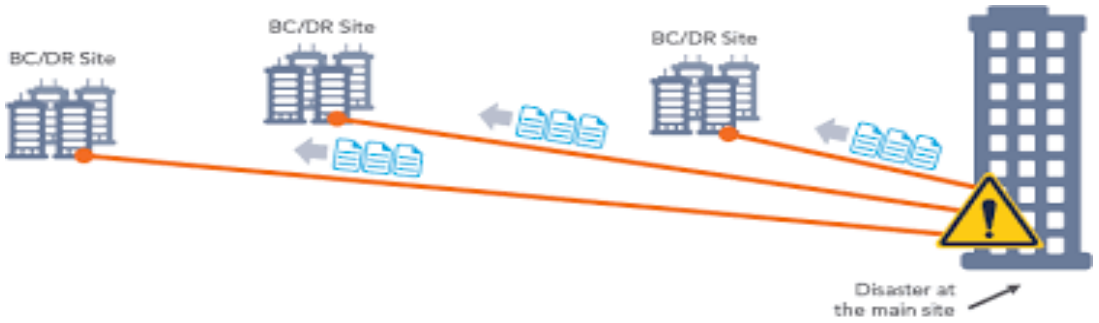
- Create, document, test, and update a plan that will:
  - Allow timely recovery of critical business operations
  - Minimize loss
  - Meet legal and regulatory requirements

Scope of BCP

- Used to be just the data center
- Now includes:
  - Distributed operations
  - Personnel, networks, power
  - All aspects of the IT environment
  - Outsourcing and suppliers
  - Production and manufacturing
  - Any other business critical processes and operations

Creating a BCP

- Is an on-going process, not a project with a beginning and an end
  - •Creating, testing, maintaining, and updating
  - •“Critical” business functions may evolve
- The BCP team must include both business and IT personnel
- Requires the support of senior management



The five BCP phases

- Project management & initiation
- Business Impact Analysis (BIA)
- Recovery strategies
- Plan design & development
- Testing, maintenance, awareness, training

I - Project management & initiation

- Establish need (risk analysis)
- Get management support
- Establish team (functional, technical, BCC – Business Continuity Coordinator)
- Create work plan (scope, goals, methods, timeline)
- Initial report to management
- Obtain management approval to proceed

II - Business Impact Analysis (BIA)

- Goal: obtain formal agreement with senior management on the MTD for each time-critical business resource
- MTD – maximum tolerable downtime, also known as MAO (Maximum Allowable Outage)

II - Business Impact Analysis (BIA)

- Quantifies loss due to business outage (financial, extra cost of recovery, embarassment)
- Does not estimate the probability of kinds of incidents, only quantifies the consequences

II - BIA phases

- Choose information gathering methods (surveys, interviews, software tools)
- Select interviewees
- Customize questionnaire
- Analyze information
- Identify time-critical business functions

II - BIA phases (continued)

- Assign MTDs
- Rank critical business functions by MTDs
- Report recovery options
- Obtain management approval

Elements of Business Continuity Management 2

ISO22313

III – Recovery strategies

- Recovery strategies are based on MTDs
- Predefined
- Management-approved

Business Continuity Strategy Options

Business Continuity Strategy Options

People	Premises	Technology	Information	Suppliers and Partners
· What number of staff do you require to carry out critical activities? · What is the minimum staffing level you will need to deliver these · What skills/level of expertise are required to undertake these activities?	· What locations do your prioritised activities operate from? · What alternative premises do you have? · What machinery, equipment and other facilities are essential?	· Is the service dependant on electrical medical equipment? · What IT is essential to carry out your prioritised activities? · What systems and means of communication are required to carry out your prioritised activities	· What Information is essential to carry out your prioritised activities? · How is this information stored?	· Who are your priority suppliers? · Are key services contracted out? · Do both you and your suppliers/ partners have mutual aid arrangements in please

III – Recovery strategies

- Different technical strategies
- Different costs and benefits
- How to choose?
- Careful cost-benefit analysis
- Driven by business requirements

III Recovery strategies

- Different technical strategies
- Different costs and benefits
- How to choose?
- Careful cost-benefit analysis
- Driven by business requirements

III – Recovery strategies

- Strategies should address recovery of:
  - Business operations
  - Facilities & supplies
  - Users (workers and end-users)
  - Network, data center (technical)
  - Data (off-site backups of data and applications)

Strategies should address recovery of:

- Business operations
- Facilities & supplies
- Users (workers and end-users)
- Network, data center (technical)
- Data (off-site backups of data and applications)

Technical recovery strategies – subscription service sites

- Hot – fully equipped
- Warm – missing key components
- Cold – empty data center
- Mirror – full redundancy
- Mobile – trailer full of computers

III – Recovery strategies

- Technical recovery strategies - scope
  - Data center
  - Networks
  - Telecommunications

III – Recovery strategies

- Technical recovery strategies – methods
  - Subscription services
  - Mutual aid agreements
  - Redundant data centers
  - Service bureaus

III – Recovery strategies

- Technical recovery strategies – subscription service sites
  - Hot – fully equipped
  - Warm – missing key components
  - Cold – empty data center
  - Mirror – full redundancy
  - Mobile – trailer full of computers

III – Recovery strategies

- Technical recovery strategies – mutual aid agreements
  - I'll help you if you'll help me!
  - Inexpensive
  - Usually not practical

III – Recovery strategies

- Technical recovery strategies – redundant processing centers
  - Expensive
  - Maybe not enough spare capacity for critical operations

III – Recovery strategies

- Technical recovery strategies – service bureaus
  - Many clients share facilities
  - Almost as expensive as a hot site
  - Must negotiate agreements with other clients

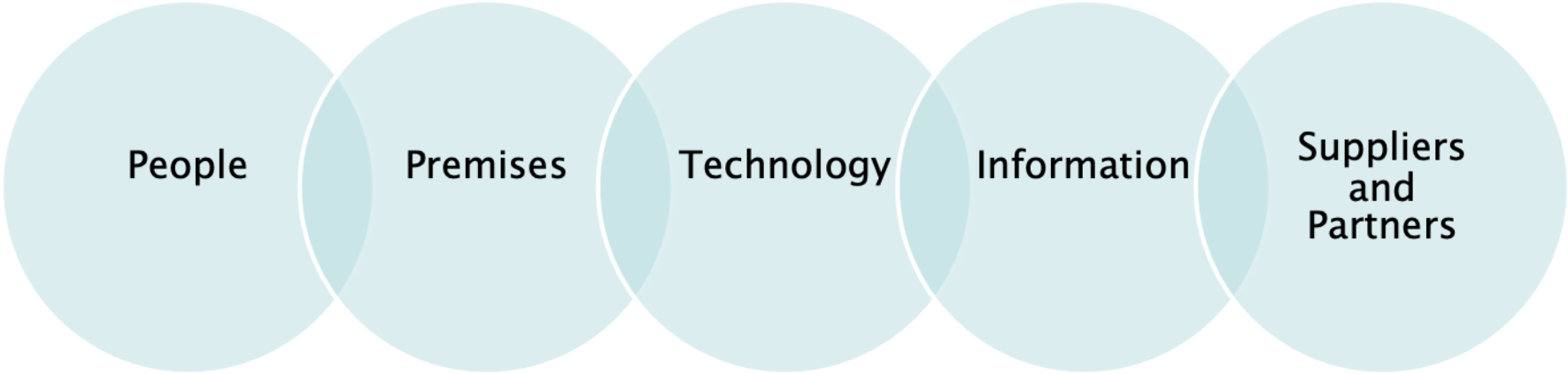
III – Recovery strategies

- Technical recovery strategies –data
  - Backups of data and applications
  - Off-site vs. on-site storage of media
  - How fast can data be recovered?
  - How much data can you lose?
  - Security of off-site backup media
  - Types of backups (full, incremental, differential, etc.)

Elements of Business Continuity Management 3

ISO22313

Activity 4
Continuity Requirements



BCP development / implementation

- Detailed plan for recovery
  - Business & service recovery plans
  - Maintenance
  - Awareness & training
  - Testing

Terms

RTO – Recovery Time Objective

Definition: period of time following an incident within which; product or service must be resumed, or activity must be resumed, or resources must be recovered

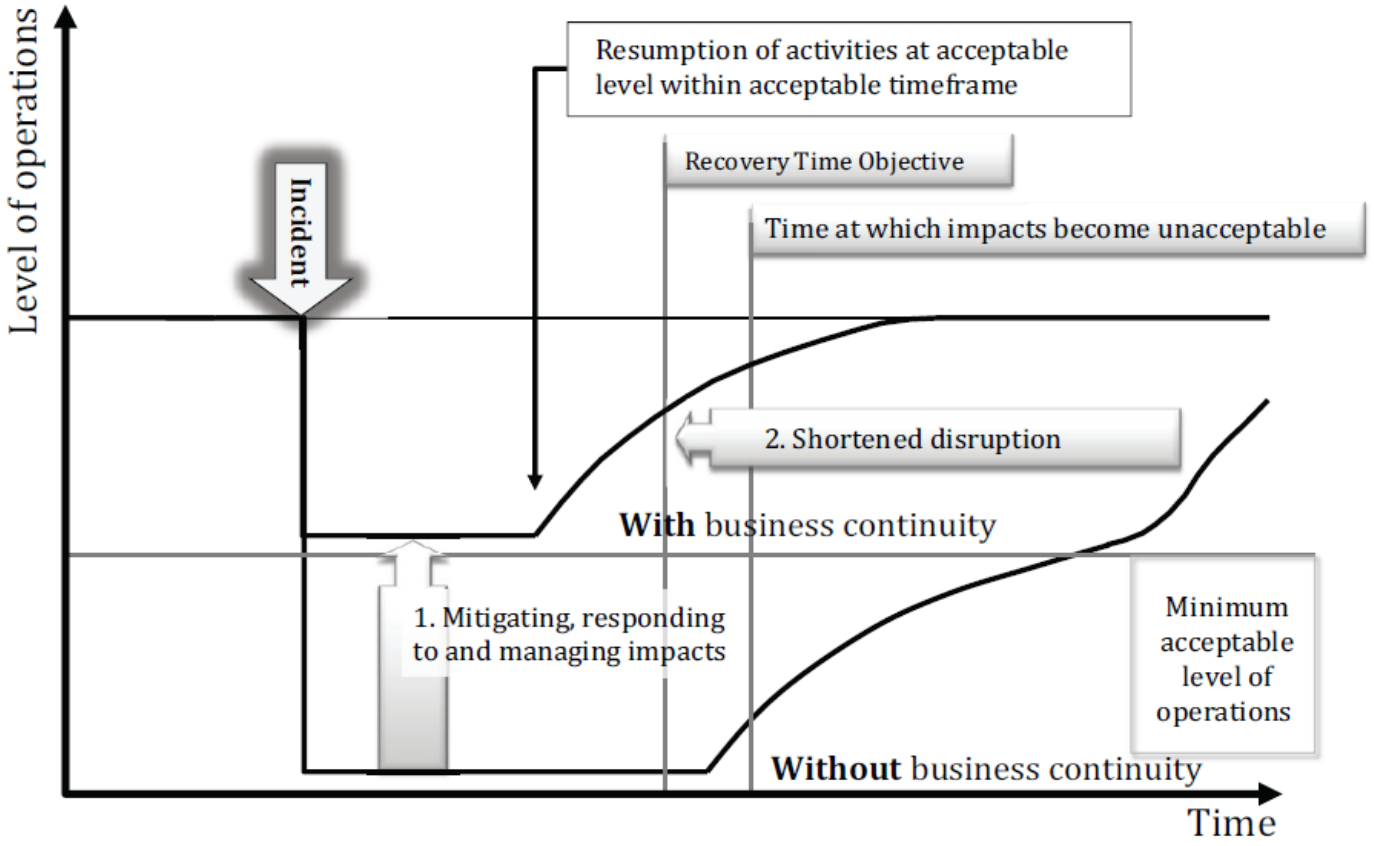
NOTE: For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/ service or performing an activity to become unacceptable.

MTPD- Maximum Tolerable Period of Disruption

Definition: time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

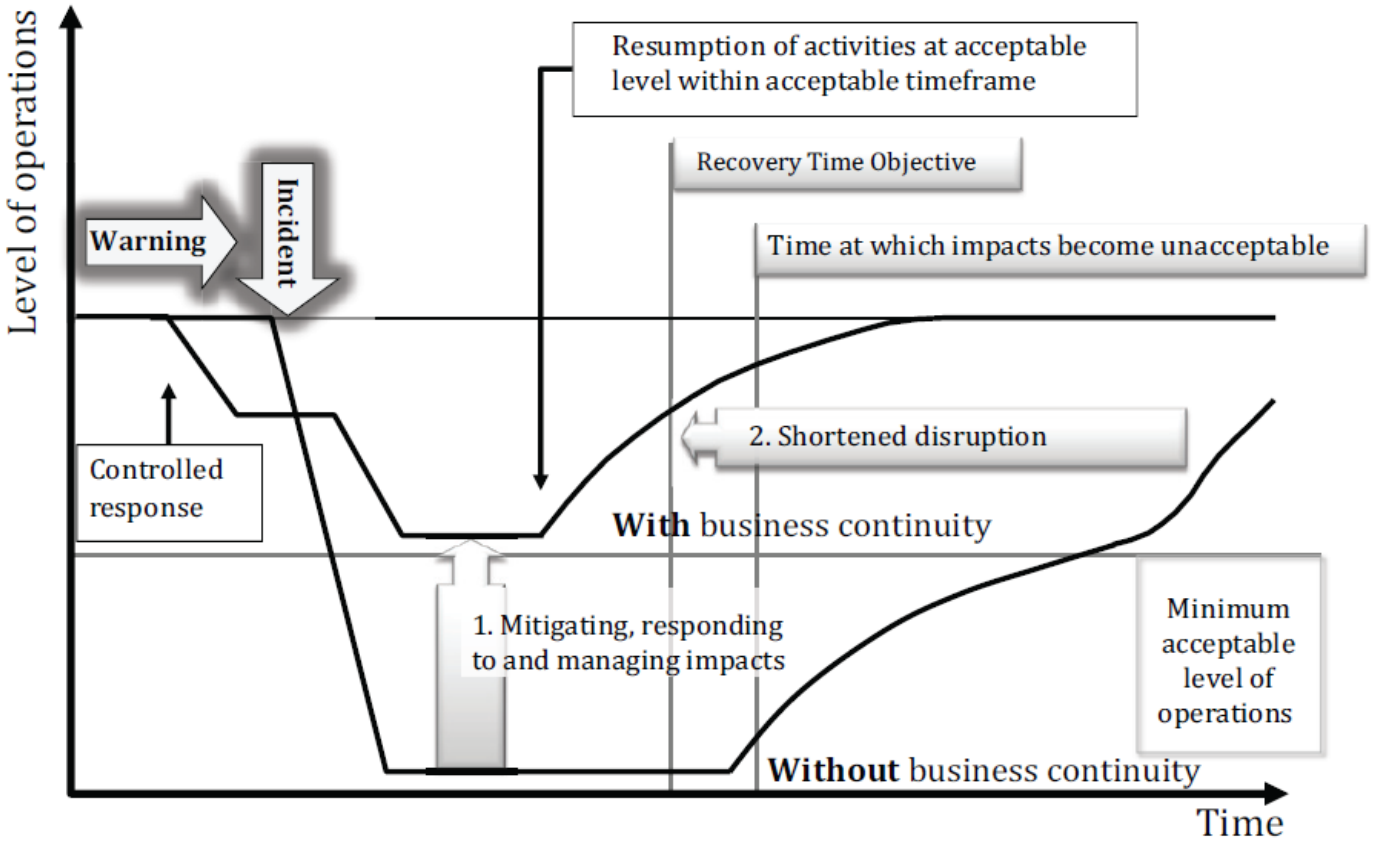
Source: ISO 22301

Mitigating Impacts through effective Business Continuity: sudden disruption



ISO22313

Mitigating Impacts through effective Business Continuity: gradual disruption



Incident Timeline

What mechanism could be used to ensure that during and following an incident the matter is escalated to the appropriate level in the organisation?

What are your organisational command and control arrangements?

BCP development / implementation

- Sample plan phases
  - Initial disaster response
  - Resume critical business ops
  - Resume non-critical business ops
  - Restoration (return to primary site)
  - Interacting with external groups (customers, media, emergency responders)

Business Continuity Response Plans

Organisations may have numerous plans.

These may include:

- Strategic organisational Incident Response Plan (IRP)
- Department/service response plans
- Building or site response plans
- Technical response plans for IT or clinical systems

Business Continuity
Incident Response Plan Content

- Document Control
- Purpose and Scope
- Document owner and maintaine
- Roles and responsibilities
- Plan activation
- Contact details
- Incident management structure and plan
- Action Cards

Business Continuity
Incident Response Plan Content cont.

- The plan should:
  - Set out the prioritised activities to be recovered, the timescales in which they are to be recovered and the recovery levels needed
  - Detail the resources available at different points in time to deliver the prioritised activities
  - Outline the process for mobilising the necessary resources
  - Include actions and tasks needed to ensure the continuity and recovery of prioritised activities
  - Be stored in a place that's easily accessible for all…consider storing on a shared drive

Elements of Business Continuity Management 4

ISO22313

BCP final phase

- Testing
- Maintenance
- Awareness
- Training

Exercising and Testing

- Exercises are there to test plans to give an idea how our plans would stand up in a disruption
- Ensures that plans are fit for purpose
- Identify gaps and learning actions
- Continuous updating of core information i.e. contact lists

Types of Business Continuity Exercises

It is important for those who are responsible for Business Continuity to know which type of Business Continuity exercise is appropriate for what they wish to achieve before planning it. This is because exercises vary in levels and resources required.

There are five main types of exercise and these are summarised below:

1. Discussion based exercise
2. Table top exercise
3. Command post exercise
4. Live exercise
5. Test

Why undertake a Business Continuity exercise?

Exercises are undertaken with three main purposes:

- **Validation** - to validate and identify improvement opportunities in existing arrangements
- **Training** - to develop staff competencies and confidence by giving them practice in carrying out their roles in a incident
- **Testing** - to test existing procedures, plans and systems to ensure they function correctly and offer the degree of protection expected

Embedding your Business Continuity Plan

To embed business continuity within you must ensure that business continuity plans are:

- communicated to staff, and
- that those staff understand their roles and responsibilities.

Exercising and Testing

- Exercises are there to test plans to give an idea how our plans would stand up in a disruption
- Ensures that plans are fit for purpose
- Identify gaps and learning actions
- Continuous updating of core information i.e. contact lists

BCP final phase - testing

- Until it's tested, you don't have a plan
- Kinds of testing
  - Structured walk-through
  - Checklist
  - Simulation
  - Parallel
  - Full interruption

BCP final phase - maintenance

- Fix problems found in testing
- Implement change management
- Audit and address audit findings
- Annual review of plan
- Build plan into organization

Maintaining Business Continuity

A clearly defined and documented maintenance programme for the business continuity management should be established.

This programme should:

•Ensure that there is an on-going programme for business continuity training and awareness
•ensure that any changes that impact on BC are reviewed
•identify any new products and services, and their dependent activities that need to be included in the BCMS;
•ensure that the business continuity plans remains effective, fit-for purpose and up-to-date; and
•enable existing exercise schedules to be modified when there has been a significant change in any of the business continuity processes.

BCP final phase - training

- BCP team is probably the DR team
- BCP training must be on-going
- BCP training needs to be part of the standard on-boarding and part of the corporate culture

Record Keeping Discussion

Logs vital information about the incident

Documents decisions made

Documents a timeline of the incident

Documents decisions not made and why

Why is record keeping so important?

Helps keep track about financial impact

Details of casualties or near misses that occur

Legal follow up

Clarifies communication channels if protracted incident

Questions