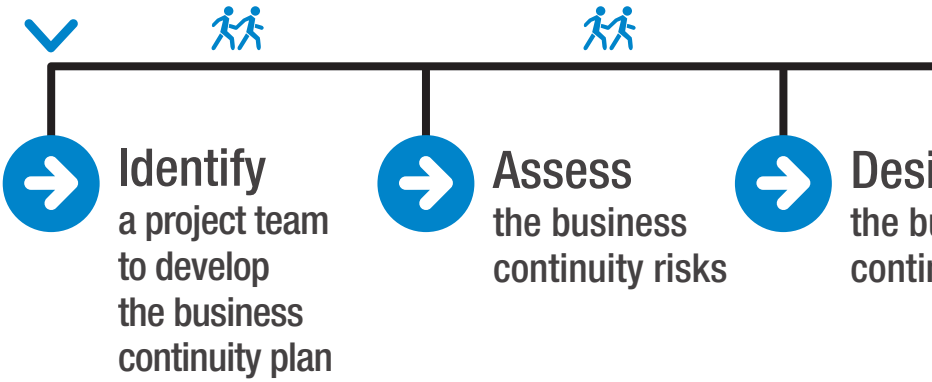
CORPORATE

STEP BY STEP GUIDE

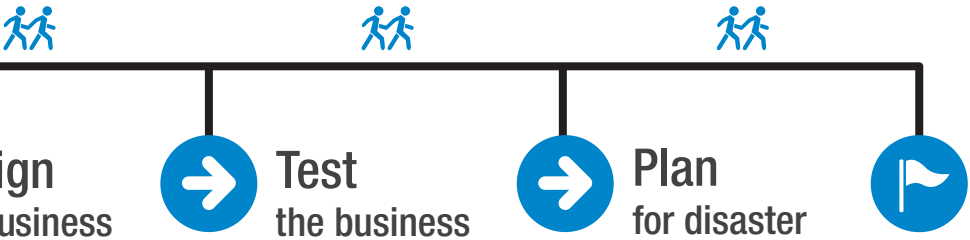
TO DEVELOPING A BUSINESS CONTINUITY MANAGEMENT SYSTEM

REPUBLIC OF IRELAND

YOUR QUICK REFERENCE GUIDE TO THE PROCESS OF DEVELOPING A BUSINESS CONTINUITY MANAGEM



OF
MENT SYSTEM



OUR MISSION

As a mutual, our purpose is to safeguard and protect the insurable interests of our Members. We commit to being our Members' trusted insurance partner providing peace of mind through tailored insurance products, effective risk management supports, Member-focused solutions and equitable claims settlements.

Our long-term sustainability will be assured through continued financial strength while focusing on excellence and continuously providing Members with value for money.

CONTENTS

Introduction P/04

Definitions P/05

Business continuity model P/06

– Identify a project team to develop the business continuity plan P/09

– Assess the business continuity risks P/10

– Design the business continuity plan P/13

– Test the business continuity plan P/14

– Plan for disaster recovery P/17

– Crisis management plan P/18

– Building resilience P/21

Insurance P/22

Claims P/24

References P/24

THIS IS THE START OF YOUR JOURNEY

We will guide you through the process of developing a business continuity management system.

INTRODUCTION

A business continuity management system presents a holistic approach to the planning, implementation, management, recovery and continual improvement of an organisation's systems. As we have learnt from the recent pandemic experience, the impact on business can be immediate and continuity of service is paramount. Business continuity management should be an integral part of the organisation's approach to effective risk management.

Business continuity planning and disaster recovery planning are frequently interpreted as being the same; however, they are different. A business continuity plan provides for the identification of the risks that could result in business interruption. It includes the business impact analysis of the risks that could prevent the continuity of an organisation and the steps to be taken so that if a serious incident were to occur, the organisation would not be adversely impacted.

A disaster recovery plan documents how an organisation would recover the critical components of a business if a serious incident were to occur, how the organisation would manage the incident, and how long the recovery phase would continue so that the organisation would remain viable. It is a key requirement within the business continuity plan. This guidance was developed to help organisations to create both a business continuity plan and a disaster recovery plan. Should a disruptive incident happen, the availability of a previously prepared plan ready for implementation will mean that the organisation is well placed to deal with it effectively.

Please note that this guide is not intended to be a definitive guide on the management of all risks associated with business continuity. This guide is designed to complement the recommendations and advice given in legislation and various publications (some of which are outlined on page 24). Management need to create and update their own policy and procedures for dealing with business continuity and disaster recovery.

DEFINITIONS

Business continuity

The capability of an organisation to continue delivery of products and services within acceptable timeframes at predefined capacity during a disruption (ISO 22301:2019).

Business continuity plan (BCP)

Documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives (ISO 22301:2019).

Business impact analysis (BIA)

The process of analysing the impact over time of a disruption on an organisation. The outcome is a statement and justification of business continuity requirements (ISO 22301:2019).

Disruption

Incident – whether anticipated or unanticipated – that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives (ISO 22301:2019).

Maximum tolerable period of disruption (MTPD)

The timeframe within which the impacts of not resuming activities would become unacceptable to the organisation (ISO 22301:2019). This was previously known as the maximum acceptable outage (MAO).

BUSINESS CONTINUITY MODEL

The decision to develop a business continuity plan should be taken by the executive management team.

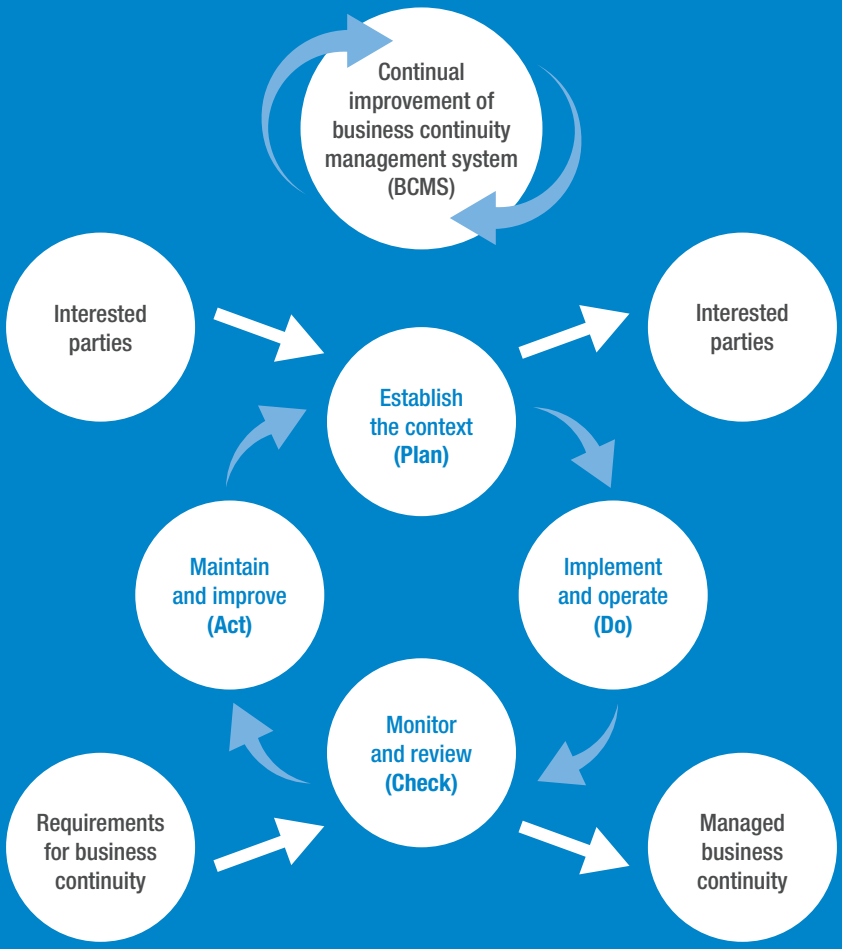
A business continuity plan should be developed following the identification of the business continuity risks as recorded in the organisation's risk register. Reference should be made to ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems – Requirements. The Plan (establish), Do (implement and operate), Check (monitor and review) and Act (maintain and improve) cycle, known as PDCA, is a tool that helps to implement, maintain and continually improve the effectiveness of an organisation's business continuity management system.

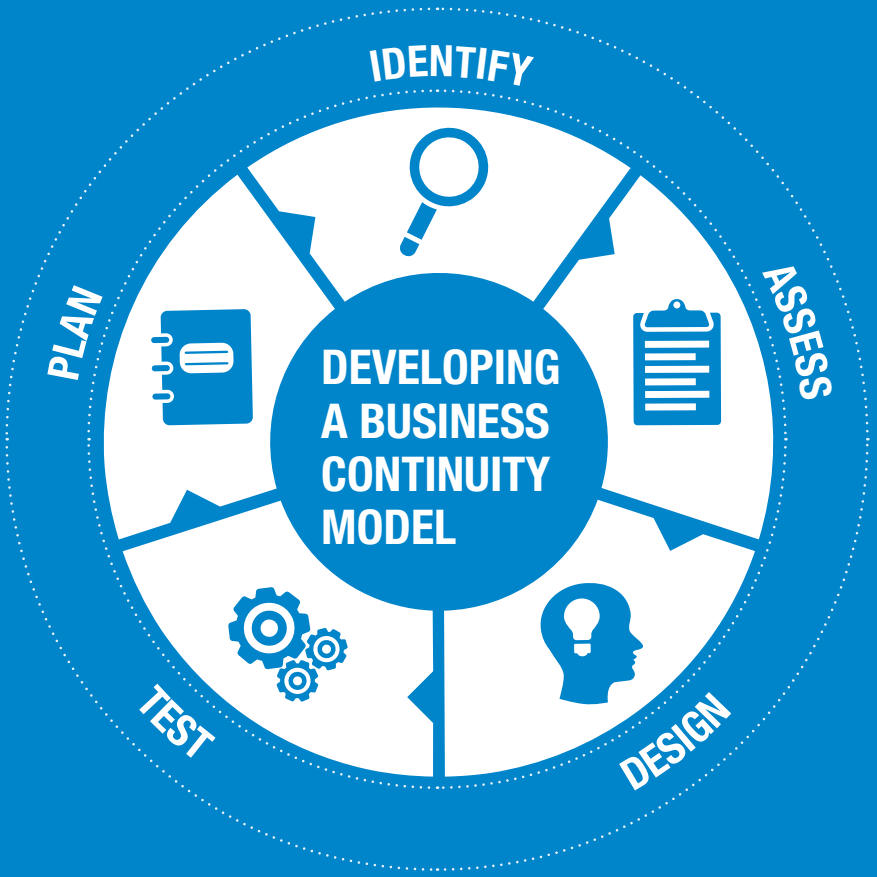
The benefit of applying the PDCA model is that it ensures a degree of consistency with other management systems and standards, such as:

- **ISO 9001**
  (Quality Management Systems)
- **ISO 14001**
  (Environmental Management Systems)
- **ISO/IEC 27001**
  (Information Security Management Systems)

The figure opposite illustrates how a business continuity management system takes interested parties and requirements as inputs for continuity management and, through the necessary actions and processes, produces continuity outcomes (i.e. managed business continuity) that meet those requirements (ISO 22301:2019).

FIGURE 1: PDCA MODEL APPLIED TO BCMS PROCESSES (REFERENCE: ISO 22301)




IDENTIFY
ASSESS
DESIGN
TEST
PLAN
DEVELOPING A BUSINESS CONTINUITY MODEL

"He who fails to plan, plans to fail" – Dr. Esdaille

The organisation's business continuity model should be underpinned by the risk management model already implemented in the organisation. It should include the following steps:

1 Identify a project team to develop the business continuity plan

The members of the team should include a project team leader who is a member of the executive management team and who has decision-making capacity, supported by the heads/managers of the following functions:

- Communications/marketing/PR. This is a key role, the importance of which should not be underestimated
- Information management
- Facilities management, including security
- Representatives from critical business functions across the organisation
- Staff representation.

For business impact analysis (BIA) purposes, the team should have key skills and competencies in the following areas:

- Project/programme planning and management
- Information gathering
- Analysis
- Effective communication and collaboration
- Translating organisational objectives to business continuity requirements and resource needs
- Applying BIA concepts in the specific organisation's context
- Knowledge of the organisation, its products and services, processes, activities and resources (ISO/TS 22317:2015).

2 Assess the business continuity risks

Business continuity risks are caused by a disruptive incident, e.g. a fire, flood, power failure, IT interruption, industrial dispute(s), withdrawal of financial support, pandemic, natural disaster, supply chain failure etc.

A disruptive incident will then lead to a reduction in productivity and cause an interruption to your business activity – and is therefore classified as a risk. This may already have been identified on your risk register. It is important to focus on the impact of the disruptive incident rather than the cause. The cause can set off a chain of events that can have multiple impacts. Business impact analysis (BIA) will help to:

- Identify key products and services, and the assets/resources (critical infrastructure) that support these.
- Assess the risks to the key activities and assets, in terms of impact on the organisation.
- Establish the maximum tolerable period of disruption (MTPD) and recovery time objectives (RTO) for each risk.
- Determine appropriate business recovery strategies for each risk.

IPB's Client Enterprise Risk Management Services team has developed a BIA tool that can assist members with this process as part of implementing a business continuity management system. Further information can be found in the Member Risk Area of the IPB Insurance website.

Business impact analysis and risk assessment is a key element in any business continuity plan (and is identified in the NSAI COVID-19 Workplace Protection and Improvement Guide).

Assessing risks is a key step in the risk management process. Its objective is to separate the minor acceptable risks from the major ones and to provide data to assist in the management of risk. It is important to assess both the likelihood and impact of risk occurring, taking into account the mitigating controls or strategies already in place by reference to the risk assessment matrix on the page opposite.

RISK ASSESSMENT MATRIX

LIKELIHOOD	MINOR: 1	MODERATE: 2	MAJOR: 3	SEVERE: 4
ALMOST CERTAIN: 4	4	8	12	16
LIKELY: 3	3	6	9	12
UNLIKELY: 2	2	4	6	8
RARE: 1	1	2	3	4

IMPACT

LOW: 1-3 MEDIUM: 4-8 HIGH: 9-16

A risk is then assessed as being low, medium or high. This is the risk rating (which is Likelihood x Impact).

The result of the risk assessment can be used to produce a risk profile that gives an indication of significance to each risk and provides a tool for prioritising risk treatment efforts. This ranks the relative importance of each identified risk.

The Department of Enterprise, Trade and Innovation published business continuity checklists of preparatory actions in responding to both COVID-19 and an influenza outbreak, and these are useful to consider from a disruptive pandemic incident perspective. See www.dbei.gov.ie/en/Publications/Business-Continuity-Planning-A-checklist-of-Preparatory-Actions-in-Responding-to-the-COVID-19-Outbreak.html

For identified risks requiring treatment, the organisation should consider proactive measures that:

- Reduce the likelihood of disruption
- Shorten the period of disruption
- Reduce the impact of disruption on the organisation's key products and services.

The organisation should then implement appropriate risk management controls in accordance with its risk appetite.

3 Design the business continuity plan

Once the BIA has been completed, you will now able to implement and test the recovery scenarios and draft your business continuity plan.

The business continuity plan should be made available to all employees in hard or soft copy and kept in a secure location that is accessible in an emergency. The level of detail in the plan should be commensurate with the size of the organisation and the number of critical functions to be undertaken. The BCP should contain the following:

- Defined roles and responsibilities for people and teams having authority during and following an incident.
- A process for activating the response.
- Details to manage the immediate consequences of a disruptive incident, giving due regard to:
  - The welfare of individuals.
  - Strategic, tactical and operational options for responding to the disruption.
  - Prevention of further loss or unavailability of prioritised activities.
  - Details on how and under what circumstances the organisation will communicate with employees and their relatives, key interested parties and emergency contacts.
  - How the organisation will continue or recover its prioritised activities within predetermined timeframes.

The BCP should also contain details of the organisation's media response following an incident, which may include a communications strategy, the preferred interface with the media, guidelines or a template for drafting a statement for the media, appropriate spokespeople as well as a process for standing down once the incident is over (ref ISO 22301:2019).

4 Test the business continuity plan

"An untested plan is only a strategy" – Richard Gagnon

Testing is a crucial part of the business continuity management system: rather than wait for the perfect plan, it is advisable to have a good plan, test the plan and then perfect the plan following testing.

Testing the business continuity plan allows identification of the following:

- Appropriateness of the plan in meeting the organisation's strategic objectives.
- Deficits in the planning process, such as absence of a generator in the event of an electricity failure.
- Effectiveness of the means of communication chosen for contacting employees, e.g. the use of mobile phones/landlines/social media.
- Availability of employees to respond to a business interruption.
- Accessibility of the hot site, including the length of time it would take for each employee to respond and relocate to the site following the activation of the business continuity plan.
- Availability of adequate office infrastructure, such as desks/chairs.
- Other issues, such as availability of safe drinking water, food, etc.
- Requirements for overnight accommodation due to the location of a hot site, and the travel distance for employees.
- Capability of software systems to perform when operated remotely.

Testing of the plan should be ongoing, and each time a test is concluded the plan should be revised accordingly. This fits with the Plan-Do-Check-Act (PDCA) model referred to earlier in this guide; this model helps to continually improve the effectiveness of the organisation's business continuity management system.

When testing, consideration should be given to:

- Minimising the risk of disruption of operations.
- Producing formalised post-exercise reports that contain outcomes, recommendations and actions to implement improvements.
- Conducting tests at planned intervals and when there are significant changes within the organisation or to the environment in which it operates.

Certain factors may also trigger testing of the BCP, for example:

- Strategic directional change.
- Regulatory change.
- Customer and/or contractual change.
- Operational change, including new/changed application/ICT, supply chain (insourcing/outsourcing), and site/facility resources.
- Structural change.


Continual improvement of Business Continuity Management System (BCMS)
Interested parties
Interested parties
Establish the BCMS (Plan)
Implement and operate the BCMS (Do)
Monitor and review the BCMS (Check)
Maintain and improve the BCMS (Act)
Requirements for business continuity
Managed business continuity

5 Plan for disaster recovery

The disaster recovery plan should be focused on restoring and returning the business activities from adopted temporary measures to more normal business requirements following a disruptive incident.

The organisation should determine the resource requirements to implement the plan, which should include:

- People
- Information and data
- Buildings, work environment and associated utilities
- Facilities, equipment and consumables
- Information and communication technology (ICT) systems
- Transportation
- Finance.

Decide on the plan of action and timetable for:

- The return of employees to full-time working at the hot site, at alternative work locations or from home. It is important to remember that employers continue to have the same responsibility to employees, such as compliance with safety, health and welfare legislation, even if they are working from home.
- The maintenance of the customer database.
- The return of the original working environment to its pre-interruption condition. Consider if refurbishment will be required or if the site will require clearance and a new build. Perhaps a permanent relocation is needed; if so, identify alternative available sites.
- The maintenance of the organisational infrastructure. Is the current communications and IT infrastructure adequate or has it been damaged? If so, what will be the timetable for replacement and will training for employees be required for the new systems?

Crisis management plan

If a disruptive incident occurs, there will also need to be procedures to ensure stabilisation, continuity of service and recovery as well as management of the disruptive incident. These procedures should:

- Establish an appropriate internal and external communications protocol.
- Be specific regarding the immediate steps that are to be taken during a disruption.
- Be flexible to respond to unanticipated threats and changing internal and external conditions.
- Focus on the impact of events that could potentially disrupt operations.
- Be developed based on stated assumptions and an analysis of interdependencies.
- Be effective in minimising consequences through the implementation of appropriate mitigation strategies.

While there should be emergency response plans in place to manage a fire safety incident in the building, such emergency response plans should be expanded to consider other types of disruptive incidents so that they too are managed quickly and effectively, and are considered collectively as a crisis management plan.

The crisis management plan should include warning and communication procedures in the event of a disruptive incident as well as procedures for:

- Detecting an incident.
- Regular monitoring of an incident.
- Internal communication within the organisation and receiving, documenting and responding to communication from interested parties.
- Receiving, documenting and responding to any national or regional risk advisory system or equivalent.
- Assuring availability of the means of communication during a disruptive incident.
- Facilitating structured communication with emergency responders.
- Recording vital information about the incident, actions undertaken and decisions made.
- Regular testing.

Building resilience

Implementing a BCP in your organisation is important and can have many benefits such as:

- Minimising the effect of a disruption on the business.
- Reducing the risk of financial loss.
- Retaining company brand and image.
- Providing employees, clients and suppliers with confidence in the organisation's products and services.
- Enabling the recovery of critical systems within an agreed timeframe
- Meeting legal and statutory obligations.
- Testing of BCPs allows for continual improvement to minimise the impact of a disruptive incident.

Being resilient is also very important and this should be built into your business continuity management system. This will enable the business to implement, maintain and improve its management system to protect against, reduce the likelihood of occurrence of, prepare for, respond to and recover from disruptions when they arise. The Irish Management Institute recommends an example of how to build organisational resilience in three stages:

1. Coping (taking actions during the unexpected event).
2. Adaptation (after the event; reactive action).
3. Anticipation (before the unexpected event; proactive action).

The PDCA cycle earlier in this guide encourages businesses to identify, assess, design, test and plan their business continuity plan. This plan is an integral component of good corporate governance and an important aspect of emergency preparedness and organisational resilience.

A core principle of risk management is to learn from experience and improve; there will be lessons from the experiences of dealing with the challenges of disruptive incidents and these lessons will result in improved resilience and better risk management in the future (Institute of Risk Management 2020).

INSURANCE

Insurance should be viewed as a key component of any business continuity plan, providing an organisation with the ability to transfer risks of damage and interruption to the business should there be a loss. IPB Insurance has extensive experience in dealing with our customers following losses to their assets and interruption to their business.

Property Insurance

Property insurance covers damage to property following an insured event and seeks to replace/repair or reinstate the property in the quickest time possible in order to minimise any disruption to the organisation. To ensure the smooth handling of any property claim following any loss, reinstatement/replacement values must be considered prior to setting up or renewing any of your property insurance policies.

Are all buildings/structures/assets insured for their current reinstatement value?

The cost of reinstatement of the property should take into account the cost of rebuilding the premises to a condition equivalent to, or substantially the same as, but not better or more extensive than, its condition when new. Consider the following items when finalising valuations:

- The additional cost of reinstatement to comply with public authority requirements or European legislation.
- Professional fees, e.g. architects, engineers, etc.
- Debris removal costs to clear the site following loss.

Members should also ensure that their asset register is related to their insurance schedule so that none of the property or its contents are overlooked or uninsured. Members should consult with their insurance advisor prior to arranging property valuations.

Business Interruption Insurance

In the event of damage to a property, the insurance will, if the values are correct, ensure that there is sufficient money available to repair/replace the damaged property. However, repairs or replacements could take time and could impact financially

on the organisation through lost income or through extra incurred costs in order to keep the organisation running (e.g. rental on other premises, machinery hire, additional overtime and travel expenses for employees).

Increased cost of working (ICOW) insurance is provided by insurers to help organisations cover the increased costs necessarily and reasonably incurred by the organisation in order to minimise any interruption or interference with the running of the organisation during the period following damage.

To obtain details of cover in your property or business interruption policy, please refer to your IPB Insurance property policy and schedule. You should also discuss the adequacy of your cover with your insurance advisor.

CLAIMS

If an incident occurs that threatens the viability of your organisation or that could result in any level of interruption to your business, you should contact claims@ipb.ie

REFERENCES

Institute of Risk Management, May 2020, COVID-19 Global Risk Management Response: Resilience, Risk and Recovery

ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements.

ISO/TS 22317:2015 Societal Security – Business Continuity Management Systems – Guidelines for Business Impact Analysis (BIA)

NSAI COVID-19 Workplace Protection and Improvement Guide 2020

The Department of Enterprise, Trade and Innovation – Business Continuity Checklist of Preparatory Actions in Responding to COVID-19 (April 2020)

The Department of Enterprise, Trade and Innovation – Business Continuity Checklist of Preparatory Actions in Responding to an Influenza Outbreak (February 2020)

The Irish Management Institute (2020) – Building a Resilient Organisation.

Designed by **FUDGE Creative** | fudgecreative.ie

IPB Insurance
1 Grand Canal Square
Grand Canal Harbour
Dublin D02 P820
Ireland

Tel: +353 1 639 5500
Email: info@ipb.ie
www.ipb.ie

PUBLISHED/UPDATED JUNE 2020