# Risk control

## Business Continuity Management


In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

**Risk Management Partners**
rmpartners.co.uk

# Business Continuity Management

## Introduction

Business Continuity can be defined as the 'capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption'.[1]

Business Continuity Management (BCM) can be defined as 'a management process that helps manage the risks to the smooth running of an organisation or delivery of a service, ensuring that it can operate to the extent required in the event of a disruption'.[2]

In recent years, there have been numerous events that have highlighted the importance of BCM including:

- **Global Pandemic**: The global pandemic disrupted businesses worldwide, underlining the need for robust BCM strategies to manage remote work transitions, and supply chain disruptions.
- **Cybersecurity Threats**: Increasing cybersecurity threats, including ransomware attacks on major corporations, have demonstrated the necessity of protecting data integrity and ensuring business operations can continue during and after an attack.
- **Natural Disasters**: Events such as hurricanes, wildfires, and floods have impacted on businesses, emphasising the importance of preparing for and responding to environmental disruptions.
- **Supply Chain Disruptions**: Supply chain disruptions have demonstrated the critical need for managing supply chain risks and ensuring continuity of production and delivery.
- **Geopolitical Instability**: Instances of geopolitical instability in various regions have affected business operations, highlighting the need to address potential disruptions.
- **Technological Failures**: Outages and failures of critical technology infrastructure, such as cloud services and telecommunications, have demonstrated the importance of maintaining business operations and communications.

These events have reinforced the value of BCM in enabling organisations to anticipate, prepare for, respond to, and recover from disruptions, ensuring continuity of operations and minimising impacts.

## Essential Elements

BCM involves several essential elements[1] that collectively ensure an organisation's resilience and ability to maintain operations during disruptions. These elements include:

- **Business Impact Analysis (BIA)**: Assessing the potential effects of disruptive events on critical business functions and processes. BIA helps prioritise recovery efforts by identifying essential operations and the resources required to maintain them.
- **Risk Assessment**: Identifying and evaluating potential threats and vulnerabilities that could impact critical business functions.
- **Strategy Development**: Creating strategies to mitigate risks and ensure continuity. This includes developing plans for resource allocation, alternative work arrangements, and communication protocols.
- **Plan Development**: Documenting detailed Business Continuity Plans that outline procedures for maintaining operations during disruptions. Plans should include roles and responsibilities, crisis management and communication strategies, and recovery actions.
- **Training and Awareness**: Educating employees about BCM plans and their roles in executing them. Regular training ensures that employees are prepared to respond effectively during a disruption.
- **Testing and Exercises**: Conducting regular tests and simulations to evaluate the effectiveness of BCM plans. This helps identify gaps and areas for improvement.
- **Review and Continuous Improvement**: Regularly reviewing and updating BCM plans to reflect changes in the business environment, technology, and emerging threats. Continuous improvement ensures that plans remain relevant and effective.
- **Crisis Communication**: Establishing clear communication channels and protocols to ensure timely and accurate information dissemination during a disruption. Effective communication is crucial for managing stakeholder expectations and maintaining trust.

By integrating these elements, organisations can build a robust BCM framework that enhances resilience, minimises disruption, and ensures the continuity of critical operations.

## Understanding the Organisation

Undertaking a BIA and risk assessment are key foundational elements of BCM, leading to the creation of a deeper understanding of the organisation which then enhances the development of BCM capability[2].

### Conducting a Business Impact Analysis

The purpose of BIA is to identify essential products or services, the critical activities required to deliver these products or services, and the potential impact that a disruption of these products or services would have on the organisation and stakeholders. A BIA also identifies the resources needed to restore these products or services.

A BIA can be completed by following six key steps:

1. **Gather Information**

   Collect data through interviews, surveys, and workshops with key stakeholders and department heads to understand critical business functions and processes.

2. **Identify Essential Products and Services**

   List all the essential products and services that the organisation provides and determine which are critical to operations.

3. **Determine Critical Activities**

   Identify the activities necessary to deliver the essential products and services. Understand any dependencies and interdependencies.

4. **Assess the Impact of Disruptions**

   Evaluate the potential impact of disruptions on each critical activity. Consider factors such as financial loss, customer dissatisfaction, regulatory implications, and reputational damage.

5. **Establish Recovery Time Objectives**

   Determine the maximum acceptable downtime for each critical activity before significant adverse impact occurs. This helps prioritise recovery efforts.

6. **Identify Resource Requirements**

   Document the resources needed to resume critical activities, including people, premises, technology, information, equipment, supplies, and partners.

   To conduct an efficient and effective BIA, it may be necessary to involve various individuals who maintain a detailed knowledge of the specific activities featured in the analysis.

### Conducting a Risk Assessment

A risk assessment seeks to identify the likelihood and impact of a range of risks that could cause a disruption to the critical business activities identified during the BIA.

A risk assessment can be completed by following six key steps:

1. **Gather Information**

   Collect data from various sources, including incident reports, industry trends, and expert opinions. Engage with stakeholders to gain insights into potential risks.

2. **Identify Risks**

   List potential risks that could impact the critical business activities. These may include natural disasters, cyber-attacks, supply chain disruptions, and human errors.

   These risks may affect people, premises, technology, information, equipment, supplies, and partners.

3. **Assess Likelihood**

   Assess the likelihood of each identified risk occurring. Consider past occurrences and near misses.

4. **Assess Impact**

   Assess the potential impact of each risk on the critical business activities. Impacts may include operational disruption, loss of reputation, and / or regulatory consequences.

5. **Prioritise Risks**

   Prioritise risks based upon their likelihood and impact. Use a risk matrix to visualise and prioritise risks.

6. **Identify Mitigation Strategies**

   Develop strategies to mitigate identified risks. This may include preventive measures, and contingency plans.

   By following these steps, you can effectively conduct a BCM risk assessment to help your organisation prepare for and manage potential disruptions.

## Crisis Management

Effective crisis management[3] ensures that an organisation can continue to operate critical functions during and after a crisis. It includes establishing a dedicated team with clearly defined roles and responsibilities for managing a crisis.

A Crisis Management Plan should be developed which outlines procedures for identifying, assessing, and responding to crises. It should also outline immediate actions to be taken once a crisis has been identified, focusing on safety, containment, and stabilisation.

A decision-making framework within the plan would ensure timely and effective responses, while a Communication Plan will ensure that clear and consistent information is provided to internal stakeholders, and external stakeholders, including customers, partners, regulators, and the media, to maintain trust and transparency.

## Disaster Recovery

Disaster Recovery Planning[4] involves developing recovery strategies to restore critical systems and processes, which may include data backup solutions, alternative communication methods, and temporary relocation plans.

Effective disaster recovery strategies should encompass all critical components of an organisation, including people, premises, technology, information, equipment, supplies, and partners.

Regular testing and exercises are conducted through drills and simulations to ensure the plan's effectiveness and to identify areas for improvement.

Plan maintenance and updates are crucial, as they involve keeping the disaster recovery plan current with changes in the organisation, technology, and potential threats, ensuring it remains relevant and effective.

Communication and training are also key components, ensuring that all employees are aware of the disaster recovery plan and their roles within it.

The ultimate objective of disaster recovery planning is to minimise disruption and data loss, enabling an organisation to quickly resume critical operations.

## Testing and Exercising

Testing and exercising Business Continuity Plans (BCP's) are crucial activities that ensure an organisation is prepared to respond effectively to disruptions.

Testing helps identify gaps, weaknesses, or outdated information in the BCP, while exercises can reveal unforeseen challenges that were not previously considered.

Regular exercises also ensure that employees are familiar with their roles and responsibilities during a disruption, increasing their confidence and readiness.

There are several types of tests and exercises, with each maintaining different purposes and levels of complexity:

1. **Call Tree Testing**

   A test of the communication plan, specifically the call tree, to ensure that all contact information is accurate and that messages can be relayed quickly.

2. **Walkthrough Exercises**

   A desk-top discussion-based exercise where team members walk through the BCP to familiarise participants with the plan and roles.

3. **Simulation Exercises**

   A more interactive exercise that simulates a specific disruption scenario, requiring participants to respond as they would in a real event.

4. **Functional Exercises**

   A hands-on exercise that tests specific functions or components of the BCP, such as IT recovery or communication protocols.

5. **Full-Scale Exercises**

   A comprehensive exercise that simulates real-life disruption, involving all aspects of the BCP and full participation from relevant teams.

## Roles and Responsibilities

Outlining roles and responsibilities within BCM is crucial for ensuring an organised and effective response to disruptions[1]. Clearly defined roles and responsibilities help streamline decision-making, enhance coordination, and ensure that all necessary tasks are completed efficiently. Roles and responsibilities should be defined for the following positions and entities:

- BCM Steering Committee
- Business Continuity Manager / Coordinator
- Departmental Continuity Coordinators
- Crisis Management Team
- Disaster Recovery Team
- Communication Officer / Team
- Facilities Management Team
- Human Resources Team

## Continuous Improvement

Ongoing reviews and updates to the BCP are essential for maintaining its effectiveness and relevance in a dynamic risk environment.

Incorporating lessons learned from exercises and real incidents ensures that the plan evolves to address new challenges and improve organisational resilience.

Continuous review and updates are necessary, along with strategies for incorporating lessons learned.

Failure to review and update the BCP can result in a reduction in the effectiveness of an organisation's ability to operate to the extent required in the event of a disruption.

## Summary

BCM helps minimise financial losses, protect brand reputation, and ensure compliance with legal and regulatory requirements. It also creates stakeholder confidence by demonstrating a proactive approach to risk management and preparedness. Additionally, BCM contributes to the long-term sustainability and success of the organisation.

## References


1. ISO 23301 available at: Security and resilience — Business continuity management systems —Requirements, available at: https://www.iso.org/standard/75106.html
2. How prepared are you? Business Continuity Management Toolkit, HM Government, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/137994/Business_Continuity_Managment_Toolkit.pdf
3. What is crisis management and how to implement it in your business, IMD, available at: https://www.imd.org/blog/management/what-is-crisis-management/
4. Disaster Recovery Planning: A Comprehensive Guide, BCESG, available at: https://bcesg.org/business-continuity-esg-blog/disaster-recovery-planning-a-comprehensive-guide

## Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

## Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

**Risk Management Partners**

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk



FP875-2025