



# **HSE Business Continuity Management Policy 2025**

# Health Service Executive (HSE) Business Continuity Management Policy

International Standard Book Numbering (ISBN)	
Revision Number	Final Draft 1.1 (February 2023)
SMT Review	06 Jan 2025
Revision Number/Date	
SMT Review	

## Table of Contents

<b>Foreword</b>	<b>4</b>
<b>Key Messages</b>	<b>5</b>
<b>HSE Business Continuity Management Policy</b>	<b>6</b>
1.0 Introduction	6
1.1 Policy Statement	7
1.2 Scope	8
1.3 Key Definitions	8
1.4 Key Reference Material	9
1.5 Roles & Responsibilities	9
1.5.1 Board	9
1.5.2 HSE's Audit and Risk Committee (ARC) and other Board Committees	9
1.5.3 Chief Executive Officer (CEO)	10
1.5.4 Regional Executive Officers (REOs) and [other Executive Officers ]	10
1.5.5 Managers	10
1.5.6 Staff	11
1.5.7 Required Roles in BCM	11
1.6 Business Continuity Management Process	12
1.7 Mandatory Requirements	12
1.7.1 Plan (establish)	13
1.7.2 Do (implement and operate)	13
1.7.3 Check (monitor and review)	14
1.7.4 Act (maintain and improve)	15
1.8 Monitoring Implementation of and Compliance with Policy	15
1.9 Implementation Support	15
1.10 Update	16
<b>Appendix 1: Glossary of Terms</b>	<b>17</b>
<b>Appendix 2: Acronyms</b>	<b>19</b>
<b>Appendix 3: References</b>	<b>20</b>

# Foreword

## Bernard Gloster, Chief Executive Officer

As CEO of the Health Service Executive, I am pleased to present the HSE Business Continuity Management Policy and Handbook 2025 which has been approved by the HSE Board. My personal commitment to working to improve the quality of health and social care services to the people of Ireland remains unwavering. Our collective ability to uphold this commitment is significantly bolstered by our focus on being better able to anticipate and prepare for unforeseen threats which could cause disruption to our primary purpose as an organisation, to provide exceptional health and social care services to all those we serve.



In an era marked by rapid advancements in medical technology and evolving population needs, the need for a resilient, adaptable, and integrated healthcare system is more critical than ever. This policy, when used in conjunction with other frameworks and policies in the HSE, aims to continue to support our dedication to respond as effectively as possible when something unforeseen disrupts health and social care services and challenges our resilience as an organisation. Ensuring the effective continuity and timely recovery of critical health and social care services is paramount when such threats materialise into events.

The Business Continuity Management Policy and Handbook 2025 represents a further step, therefore, in standardising and aligning our business continuity strategies today with global best practices. It will help enable us to continue to provide essential health and social care services and support services to our communities, even in the face of unforeseen events. We have, in recent years, proven that we are a resilient organisation, responding when needed to unprecedented events such as the COVID-19 pandemic and the cyber-attack incident. The policy will build on the inherent resilience of our people and our organisation by providing new guidance and a formal, structured approach to deal with threats and events, which can impact the continuity of critical health and social care services.

The policy and accompanying handbook will advise and assist healthcare professionals, managers, and other critical workers across the country on how they can best prepare their functions and services to deal with the impacts of disruptions to patient and service user care while also always maintaining the safety and well-being of our staff as a priority.

The collaborative efforts of several teams have been instrumental in shaping this policy. These teams have come together to develop a comprehensive approach that addresses the unique challenges of our healthcare landscape. With clear roles, responsibilities, and

established communication channels, we are poised to respond more effectively to a range of threat events and scenarios, from natural disasters to cyber incidents. Moreover, our commitment to continuous improvement ensures that this policy will evolve in tandem with Emergency Management and Incident Management policies, procedures and frameworks which exist today in the HSE.

While we cannot predict the future and prepare for every scenario, we can confidently state that the HSE is fully prepared to uphold its duty in the face of adversities, should they occur, to always deliver quality patient care. I endorse the principles outlined in this policy and handbook as a positive contribution to our duty of care.

## Acknowledgements

*I wish to extend my deepest thanks to the many people who contributed to the HSE Business Continuity Management Policy and Handbook 2025, especially to all the health service staff who took the time to provide invaluable feedback during the consultation phases. I wish also to thank the Senior Leadership Team and the Audit and Risk Committee members who provided advice and feedback on the process and lastly I wish to acknowledge and thank the Directorate for Emergency Management for their leadership in the development of this policy.*

## Key Messages

### Business Continuity Management: Ensuring the continuity of HSE's services

The day-to-day mission of the HSE is to provide, the highest quality health and social care services for the population of Ireland. Furthermore, our longer-term ambition is that our services and the experience of those waiting for, or who are receiving care, become demonstrably better and more resilient to disruptions.

In an ever-changing **threat** and **risk** landscape to the effective delivery of health services, operations and activities, we are very mindful of how easily undesirable and unforeseen incidents or events can throw us off course. Even a minor **incident** or **event** has the potential to evolve into something more serious that prevents or disrupts our ability to deliver quality health services. Through the risk assessment process, we may be able to mitigate risks to prevent an incident or event from occurring.

**Business Continuity Management (BCM)** is a comprehensive process that involves understanding the risks and potential disruptions that an organisation might face, assessing the impact of those disruptions on its services, operations, and key activities and developing strategies and plans to ensure the organisation can continue functioning and recover quickly in the face of these challenges.

The **Business Continuity Management (BCM) Policy and Handbook 2025** is a practical resource for all Managers. It will support all stakeholders in the design and implementation of standardised business continuity management strategies and plans to address a variety of risks across the health system.

### HSE's BCM Approach:

The HSE recognises the need for a structured and standardised approach to developing and implementing BCM processes. The policy and handbook are aligned with guidance from ISO 22301:2019 (Business Continuity Management Systems – Requirements) and adopts the following four key stages:

- **Plan (establish):** In the Plan phase, you will define the requirements and resources to effectively establish and manage a BCM process. Responsible individuals will also establish a clear definition of scope for their area of responsibility (e.g., a Region, Site, Service or Function).
- **Do (implement and operate):** In Do phase, you will perform implementation activities focused on performing risk and impact analysis, creating strategies, plans and actions to aid the timely and safe recovery of impacted resources and services from potentially disruptive events. Plans may vary from the very detailed to easy-to-follow action cards.
- **Check (monitor and review):** In Check phase, you must confirm the effectiveness of the formal plans by testing and validating them regularly. This phase also includes implementing continuous monitoring structures to ensure ongoing operating effectiveness.
- **Act (maintain and improve):** Finally in the Act phase, you must seek continued improvement of the BCM processes through a structured upward feedback spiral focused on learning from events and re-testing changes to help build and improve BCM processes over time.

Refer to Section 1 for Key Definitions and Appendix 1 for a full Glossary of Terms.

# HSE Business Continuity Management Policy

## 1.0 Introduction

This document sets out the policy by which the HSE manages disruptive events that impact on the continuity of patient and service user care and the wider delivery of health services. Some areas within the HSE have historically utilised informal “workarounds” which enable critical services to be delivered at a time of disruption. Business Continuity Management (BCM) is a process that helps the HSE to comprehensively formalise how we prepare, respond and recover from incidents or events that may impact us operationally from delivering key services to patients and service users.

BCM seeks to ensure that all strategies and plans to respond to disruptive events are formalised, designed and implemented in a standardised manner to enable a more

effective response to be deployed to maintain and/or recover key services, operations and activities during disruptive events. The quality of our preparedness can make a material difference between the fast and effective recovery of disrupted services versus a prolonged undesirable disruption to services. BCM processes are therefore aimed at effectively planning for minimal disruption to our services.

The HSE approach to BCM is aligned with the ISO 22301:2019 an international standard for Business Continuity Management (BCM). It provides clear policy direction and guidance to help Managers plan, establish, implement, operate, monitor, review, maintain, and continually improve processes that enhance their ability to respond to and recover from disruptive events.

Consideration has been given to the HSE's Enterprise Risk Management Policy and Procedures 2023 and the HSE Incident Management Framework 2020 in creating and aligning this policy with relevant reference language and guidance.

## 1.1 Policy Statement

It is the policy of the HSE to minimise disruptive impacts on patient and service user care, staff, and the wider delivery of health and social care services.

The purpose of this policy is to:

- Enable Managers to proactively plan for better organisational and operational resilience from disruptive events by using BCM as one tool in their resilience armoury that guides good practice for the continuity of service provision.
- Assist Managers, and other Stakeholders to understand the need to, and their role in adopting a formal, consistent and standardised approach to planning for and managing business continuity events. This includes aligning any existing BCM processes with the requirements of this policy.
- Provide clear direction of the key requirements for the design, implementation and standardisation of BCM across the organisation. While not prescriptive in terms of a specific course of action for Managers to take, it informs the sequence of activities, quality of work and the support of Management, which will be critical success factors in determining the effectiveness of the BCM processes that are implemented within the HSE.
- Provide HSE management with a structured process for the management of critical infrastructure as defined under the EU CER directive. This legislative requirement behoves the HSE to take specific measures, to ensure that essential services in Health required for the maintenance of vital societal functions and economic activities are provided in an unobstructed manner.

## 1.2 Scope

The content of this policy is mandatory for all Leaders, Managers and Staff across all services, operations, functions, and facilities within the HSE at National, Regional and Local level. BC Owners at all levels, must determine which plans are needed for their site, service and operations and may need to consult with other sites, services and operations, functions etc.

It is essential that HSE funded agencies (Section 38 and Section 39 organisations) have BCM processes in place which reflects best practice. While these organisations manage business continuity risks according to their internal policies, it is recommended that they align to the HSE BCM Policy and associated guidance Handbook. This policy will also support engagement around BCM measures with any other key Stakeholders (see definition) of the HSE to increase wider operational resilience.

The scope of this policy does not address how to respond to a clinical incident. Guidance for this can be found in the Incident Management Framework (2020). It is possible that a clinical incident (e.g., major accident, pandemic) may lead to service continuity risks for the organisation, which may in turn result in certain business continuity plans being utilised.

## 1.3 Key Definitions

**Business Continuity Management (BCM)** is a comprehensive process that involves understanding the risks and potential disruptions that an organisation might face, assessing the impact of those disruptions on its services, operations, and activities and developing strategies and plans to ensure the organisation can continue functioning and recover quickly in the face of these challenges.

A **risk** is the effect of uncertainty on our objectives.

A **threat** is a potential source or event that can cause harm, damage, disruption, or negative impact to an organisation's operations, assets, or objectives.

An **event** is anything that has the potential to disrupt normal service delivery.

An **incident** is an event or circumstance which could have or did lead to unintended and/or unnecessary harm.

**Risk Assessment** is an overall process of risk identification, risk analysis and risk evaluation.

A **Business Impact Analysis (BIA)** is a systematic process used to identify and evaluate the potential consequences of disruptions or incidents on an organisation's services, operations and activities. It forms a foundational part of developing a BCP.

**Business Continuity Plan (BCP)** is a written guide that outlines the steps an organisation needs to take when something unexpected happens that disrupts key services, operations and activities.



A full list of definitions / glossary is contained in Appendix 1.

## 1.4 Key Reference Material

The main guidance for BCM, which also applies to this policy, is contained in:

- ISO22301:2019 – Business Continuity Management Systems – Requirements

Other useful guidance or standards relevant to this policy include:

- HSE Enterprise Risk Management Policy and Procedures 2023 - sets out the policy and procedures by which the HSE manages risk. The approach is aligned with the ISO 31000:2018 Risk Management – Guidelines.
- HSE Incident Management Framework (IMF) 2020 HSE Incident Management Framework (IMF) 2020 - sets out the principles, governance requirements, roles and responsibilities and processes to be applied for the management of adverse events and incidents in all service areas. The IMF is consistent with legislative and regulatory requirements.
- A Framework for Major Emergency Management (MEM) 2006 - sets out common arrangements and structures for front-line public-sector emergency management in Ireland. It is maintained by the Department of Housing, Local Government and Heritage.

A full list of reference material used in the creation of this policy and guidance material can be found in Appendix 4.

## 1.5 Roles & Responsibilities

Effective BCM requires leadership and governance. Roles and responsibilities have been defined below to support the ownership and commitment to BCM:

### 1.5.1 Board

The Board is the governing body of the HSE and is accountable to the Minister for Health for the performance of its functions. As described in the HSE's Code of Governance, the Board fulfils key functions in respect of the HSE, including the ownership of business continuity risk.

### 1.5.2 HSE's Audit and Risk Committee (ARC) and other Board Committees

The HSE's Audit and Risk Committee (ARC) will provide oversight and advice concerning the operation of the HSE's BCM policy and related activities. Other Board Committees provide oversight of BCM related activities of the HSE as delegated by the ARC Chair.

### 1.5.3 Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) is responsible for executive decision making in the HSE and is the accountable officer for ensuring implementation and compliance with the BCM Policy across the organisation, as well as the dissemination of this policy. They may delegate responsibility for the implementation to other accountable officers that are part of the Senior Management team.

### 1.5.4 Regional Executive Officers (REOs) and [other Executive Officers]

Regional Executive Officers (REOs) and [other Executive Officers], are responsible for implementing BCM processes in their region and ensuring compliance with the BCM policy.

The REOs and [other Executive Officers], as representatives of the CEO, with delegated authority, will make executive decisions including the establishment of nationally consistent standards and policies for the management of their unique risks and will therefore be owners of their regional and/or functional business continuity management processes.

REOs and [other Executive Officers], will appoint responsible Managers and Staff to oversee the implementation and maintenance of BCM processes in their regions. These roles are further outlined below and in the BCM handbook.

### 1.5.5 Managers

Managers are responsible for:

- Implementing and ensuring compliance with the HSE Business Continuity Management Policy and Handbook 2023 in their area of responsibility.
- Ensuring that appropriate and effective BCM processes are in place within their delegated areas.
- Conducting a Risk Assessment covering all likely service continuity risks, both clinical and operational, at least annually.
- Conducting a Business Impact Analysis to identify and assess processes critical to the delivery of services.
- Developing appropriate strategic responses within their service or operational plans which reflect the management of their specific continuity risks.
- Maintaining appropriate documentation that supports BCM and formally reporting on the status of the BCM to the next level of management, up to the Board of the HSE.
- Ensuring that relevant staff are trained on their role in BCM, learning should be included in requirements for relevant staff.

- Ensuring testing is carried out in line with the terms of this policy for their area of responsibility.
- Performing after action reviews and incident reviews in line with the Enterprise Risk Management Policy and Procedures 2023 and the HSE Incident Management Framework 2020. This will result in Business Continuity plans being updated and continuously improved.
- Promoting a culture where all staff are encouraged to be threat aware and to speak up should they spot any type of risks to service continuity.
- Managers that oversee functions where third parties are engaged, are responsible for identifying where a third party is critical and that these third parties can demonstrate effective BCM processes for themselves and their suppliers, which conform with this policy.

### 1.5.6 Staff

Staff are responsible for:

- Identifying and reporting any potential continuity threats or events to their Line Managers.
- Engaging in BCM training appropriate to their designated BCM responsibility. Familiarising themselves with BCPs in their respective areas and partaking in testing and exercising where relevant.
- 1.5.7 Required Roles in BCM

Outlined below are the expected roles which Managers will be assigned, which will underpin the roll out of this policy in National, Regional and Local areas, services and/or operations. They are described in more detail in the handbook.

Role	Definition
Business Continuity Owner (BCO)	<p>Each area should assign a Business Continuity Owner who is responsible for ensuring that business continuity processes are implemented and managed appropriately and in line with the BCM policy.</p> <p>The BC Owner is normally the Senior Executive / Manager of the area, function, service where the business continuity management processes are being applied.</p> <p>At the Regional level this role will be assigned to the REO who may in turn delegate to other BC owners in the region.</p>
Business Continuity Leader (BCL)	<p>The role of the Business Continuity Leader is to support the BC Owner by leading, facilitating and advising on the technical aspects of the BCM processes.</p> <p>They are also responsible for the administration of the end-to-end BCM processes and the provision of status reports to the BC Owner and their Management Team.</p>

They will participate in BCM training and learning activities to support their roles and the roles of the Business Continuity Support Staff (BCSS's) in their area/function.

Business Continuity Support Staff (BCSS)

Business Continuity Support Staff (BCSS) should be identified to assist the BC Leaders with the implementation, coordination and maintenance of the BCM processes in their area/function.

## 1.6 Business Continuity Management Process

The HSE's approach to BCM leverages the Plan-Do-Check-Act process (as illustrated below) which acts as a tool for end-to-end delivery of effective BCM processes. This is in alignment with the model of the International Standard for Business Continuity Management Systems – Requirements (ISO 22301:2019).

Plan-Do-Check-Act provides a simple and effective approach to implementing and applying BCM in the HSE. This policy and the associated handbook will provide Managers with guidance to develop and implement each stage outlined below.

**Figure 1 – HSE BCM Process**

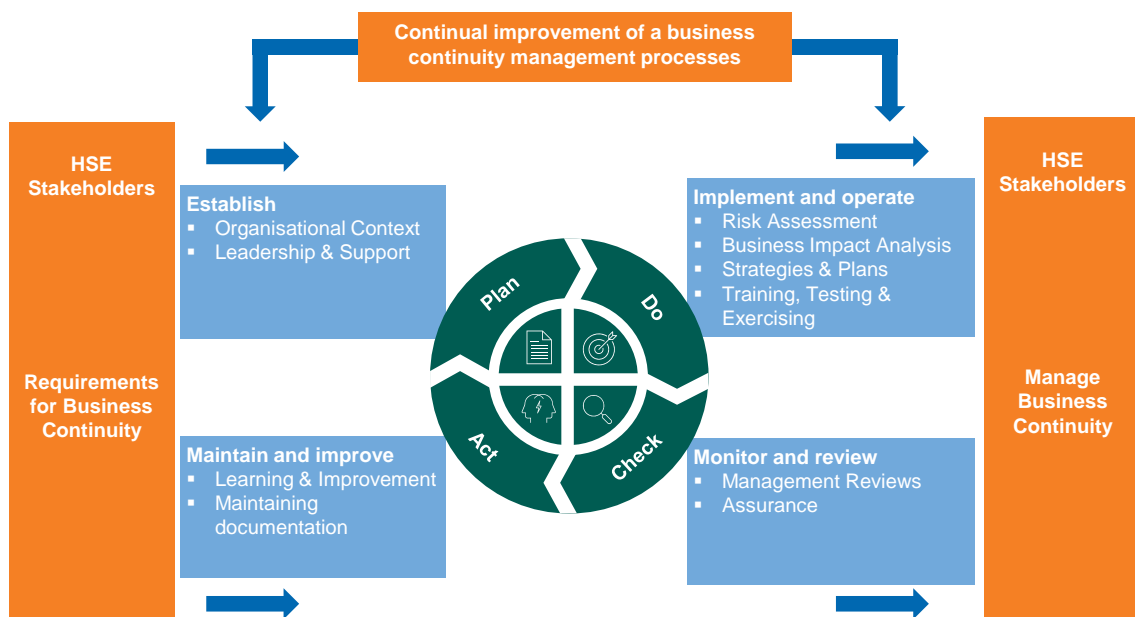


Figure 1: Adapted from ISO 22301

## 1.7 Mandatory Requirements

Outlined below are the mandatory requirements for implementing and applying BCM in the HSE and ensuring compliance with this policy.

The Policy, Handbook and Training materials form a package of tools designed to assist Managers in preparing BCM materials for parts of health and social care services where BCM does not currently exist as a process or where the current process needs to be

updated and aligned with this policy. It is recommended that Managers use the guidance provided by the BCM Handbook when completing these steps.

### 1.7.1 Plan (establish)

Managers must establish and manage BCM processes in the areas they are responsible for.

This comprises of the following mandatory requirements in this phase:

- **Context of the organisation** – Managers must ensure they are considering the context of the organisation and their areas of responsibility when determining the scope of BCM processes in their area.
- **Leadership & Support** – Managers must define clear roles and responsibilities as outlined in this Policy and the Handbook for BCM implementation and ensure adequate management support, resources, skills, awareness, and communication are in place.

### 1.7.2 Do (implement and operate)

In the Do cycle, Managers must identify, assess, and plan responses and actions, to ensure the timely and safe recovery from potentially disruptive events.

This comprises of the following mandatory requirements, in their areas of responsibility.

- Complete a **Risk Assessment**, to identify and verify potential threats, risks, associated causes and impacts on identified key services, operations, and activities to ensure all potential disruptions are considered at an appropriately granular level. This should include consideration of mitigations to prevent incidents and events from occurring. To complete a Risk Assessment a Manager must:
  - At least annually, complete identification, analysis, and evaluation of risks to service, operations and activity continuity, using the HSE Enterprise Risk Management Policy & Procedures (2023) as a guide to this process.
- Complete a **Business Impact Analysis (BIA)** to provide a comprehensive analysis linking the impact of threats and risks to service impacts and where to prioritise recovery efforts. To complete a BIA Managers must:
  - Identify and verify key services, operations, activities and stakeholders within scope.
  - Identify and document the processes fundamental to support the health services, operations, and activities within scope.
  - Identify and document the dependencies and interrelationships with and between other health services, processes, and support functions.
  - Determine and document the duration within which a disruption of an identified key health service, operation and activity may cause irreparable damage.

- Determine and document the duration within which it is required to restore the key health service, operation and activity.
- Determine the point to which system-based information used by a service or activity must be restored to enable the service or activity to operate effectively on resumption.
- Assess the priority of the health service, operation, or activity.
- Establish **Strategies & Plans** to outline approaches that will be taken to minimise service, operation or activity disruption in the event of a business continuity disruptive event. Strategies and plans may be adopted to address a specific threat (e.g., cyber-attack, surge events, localised flooding, major weather events, industrial action etc..) or they may be developed around continuity of a specific critical service, function, or process.
- Develop Business Continuity Plans (BCPs) as needed to enable continuation of their key health and social care services, taking into consideration third parties and suppliers where relevant. When developing BCPs Managers must:
  - Ensure the BCP is fully aligned with the requirements outlined in this policy and the accompanying handbook.
  - Ensure that plans can be used in parallel and do not contradict each other or other National/Regional guidance or other plans that exist in their areas.
  - Allocate roles and responsibilities in line with this policy.
  - Use appropriate communication and coordination tools to facilitate the effective management of business continuity activities.
  - Use appropriate documentation and recordkeeping processes to ensure the traceability and integrity of business continuity-related information.
- Perform appropriate **Training, Testing & Exercising** to support the cultural change needed to enable the success of BCM. This also includes assessing and identifying gaps in BCM processes, including BCPs, and highlighting areas for improvement. When performing training, testing & exercising Managers must:
  - Develop training plans for identified staff to support them in the delivery of their roles and responsibilities.
  - Hold desk-based functional continuity related exercises annually, with larger full-scale drills/exercises to be performed every three years.
  - Perform tests and exercises in line with the effective exercising guidelines outlined in the Handbook.

### 1.7.3 Check (monitor and review)

In the Check cycle, Managers will undertake a systematic observation of the performance of BCM processes, ensuring that they remain aligned with established objectives and strategies. This comprises of the following requirements:

- **Management Review** – On an annual basis, Managers must perform a self-assessment of their achievement of the objectives of the BCM using the guidance outlined in the BCM Handbook.
- **Assurance** – Managers must comply with any Assurance activities performed to evaluate the effectiveness and adherence of their area to this policy. Assurance reviews may be performed from a variety of sources including HSE Internal Audit, Department of Health or Regulatory Bodies (e.g., HIQA).

#### 1.7.4 Act (maintain and improve)

Through the activation of plans and exercising performed in the Do and Check cycles, gaps will be identified. In the Act cycle, Managers address these gaps to promote continuous improvement in their BCM processes. This comprises of the following requirements:

- **Learning & Improvement** – Following the activation of plans or tests/exercises, Managers must appraise all aspects of the response and perform a re-assessment of risks. This appraisal should be performed in line with the guidance outlined in the BCM Handbook.
- **Maintain documentation** – All BCM documentation must be maintained and kept current to remain effective during a disruptive event.

### 1.8 Monitoring Implementation of and Compliance with Policy

BC Owners will be responsible for the implementation of, and monitoring of compliance with, this policy within their area of responsibility.

BCM audits, compliance checks or reviews will be carried out by designated internal or external representatives of the CEO, REOs, the Internal Audit function, Senior Managers or other parties (e.g., DOH, Regulatory Bodies). Section 7 of the Handbook, Management Review, provides further guidance on self review checklists and KPIs for BCM relevant to the policy.

It is anticipated that the Critical Entities Resilience (CER) Directive came into legal effect in October 2024 and will bring legislative requirements to support the resilience of National Critical Infrastructure within the Health sector and many other sectors. Any future regulatory based audits in relation to the CER Directive will be carried out by a competent authority, which will be HIQA for the HSE.

Reports and recommendations arising from audits or reviews will be reported to the relevant Senior Accountable Officer, the HSE's Executive Management (EMT) and the Audit and Risk Committee (ARC).

### 1.9 Implementation Support

To support services in the application of the Policy, a Handbook has been developed and made available on HSE.ie.

## 1.10 Update

It is anticipated that the BCM Policy and Handbook (Version 1.0) will require review and update as lessons are learned from the adoption and implementation of the policy and associated guidance across the HSE.

Review and update to this policy and the supporting handbook will be made in compliance with the requirements of the HSE National Framework for developing Policies, Procedures, Protocols and Guidelines (PPPGs).



## Appendix 1: Glossary of Terms

Term	Definition
Business Continuity Management (BCM)	Business Continuity Management (BCM) is a comprehensive process that involves understanding the risks and potential disruptions that an organisation might face, assessing the impact of those disruptions on its services, operations, and activities and developing strategies and plans to ensure the organisation can continue functioning and recover quickly in the face of these challenges.
Business Continuity Plan (BCP)	A Business Continuity Plan (BCP) is a written guide that outlines the steps an organisation needs to take when something unexpected happens that disrupts key services, operations and activities.
Business Impact Analysis (BIA)	A BIA is a systematic process used to identify and evaluate the potential consequences of disruptions or incidents on an organisation's services, operations and activities. It forms a foundational part of developing a BCP.
Event	An event refers to a specific occurrence, incident, or happening that has the potential to impact or disrupt normal operations, health and social care services, or the overall functioning of the HSE. Events can be planned or unplanned and can range in severity from minor incidents to major disruptions. They can encompass a wide variety of situations, actions, or circumstances that require attention, response, or management within the healthcare environment.
Incident	An incident is an event or circumstance which could have or did lead to unintended and/or unnecessary harm. Incidents include adverse events which result in harm; near misses which could have resulted in harm, but did not cause harm, either by chance or timely intervention; and staff or service user complaints which are associated with harm. Incidents can be clinical or non-clinical.
Internal Audit	An audit conducted by or on behalf of the organisation itself for management review and other internal purposes, and which might form the basis of an organisation's self-declaration of conformity (ISO 22301: 2019).
Maximum Tolerable Period of Disruption (MTPD)	Maximum Tolerable Period of Disruption (MTPD) determines how long an organisation can sustain a disruption before the consequences become too damaging.
Monitor	To check, supervise, observe critically, or record the progress of an activity, action, or system, regularly to identify change.
Recovery Point Objective (RPO)	Recovery Point Objective (RPO) defines the point in time to which data needs to be recovered after a system failure or incident.
Recovery Time Objective (RTO)	Recovery Time Objective (RTO) defines the timeframe within which an organisation aims to resume its critical services, operations and activities after a disruption.
Risk	A risk is the effect of uncertainty on our objectives. In the context of the HSE and its services, it is any condition, circumstance, event, or threat which may impact the achievement of objectives and/or have a significant impact on the day-to-day services, operations or activities of the HSE. This also includes failing to maximise any opportunity that would help the HSE, or service meet its objectives.

Term	Definition
Stakeholder	<p>A person or organisation that can influence or be affected by business continuity activities. This corresponds to the application of interested parties in ISO 22313. Within the HSE, this includes but is not limited to:</p> <ul style="list-style-type: none"> <li>▪ The Department for Health</li> <li>▪ The Health Information and Quality Authority (HIQA)</li> <li>▪ The National Cyber Security Centre (NCSC)</li> <li>▪ The Board and its sub-committees</li> <li>▪ Other Hospitals, Hospitals Groups and Community Health Organisations</li> <li>▪ HSE funded services</li> <li>▪ Patient Advocacy Groups</li> <li>▪ Third Party Suppliers and Contractors</li> <li>▪ The Public</li> </ul>
Threat	<ul style="list-style-type: none"> <li>▪ A threat is any potential or imminent event, circumstance or condition that could disrupt or compromise the normal functioning of the health system, its operations, patient care, data security, or overall safety or objectives. Threats can take various forms and originate from internal or external sources, posing risks to a healthcare facility, staff, patients, and assets.</li> </ul>

## Appendix 2: Acronyms

Acronym	Definition
ARC	Audit and Risk Committee
BAU	Business As Usual
BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CEO	Chief Executive Officer
CHO	Community Health Organisation
CPD	Continuous Professional Development
DoH	Department of Health
EMP	Emergency Management Planning
EMT	Emergency Management Team
ERM	Enterprise Risk Management
HSE	Health Service Executive
ICT	Information and Communication Technology
IMF	Incident Management Framework
ISBN	International Standard book Number
ISO	International Organisation for Standardisation
KPI	Key Performance Indicator
MEM	Major Emergency Management Framework
MTPD	Maximum Tolerable Period of Disruption
OCR	Operational and Clinical Resilience
RPO	Recovery Point Objective
RTO	Recovery Time Objective
WHO	World Health Organisation

## Appendix 3: References

- ISO 22301:2019 – Societal Security – Business Continuity Management Systems - Requirements
- ISO 22313 – Societal Security – Business Continuity Management Systems - Guidance
- ISO 22399:2007 – Societal Security - Guideline for Incident Preparedness and Operational Continuity Management
- British Standard BS25999-1:2006 Code of Practice for Business Continuity Management
- Health service continuity planning for public health emergencies: a handbook for health facilities. Interim version for field testing. Geneva: World Health Organization; 2021.
- Vale of York, Clinical Commissioning Group: Business Continuity Policy, 2018.
- Business Continuity Management Policy Directive, NSW Health, North Sydney, Australia, 2018.
- Business Continuity Management Policy, Department of Health Policy, Government of Western Australia, Australia, 2022.
- Business Continuity: A framework for NHS Scotland. Strategic Guidance for NHS Organisations in Scotland, Government of Scotland, Scotland – United Kingdom, 2022.
- Business Continuity Policy & Plan 10.0, Cambridgeshire Community Service NHS, Cambridgeshire – United Kingdom, 2022.
- Trust wide Business Continuity and Contingency Planning Policy 11.1, Portsmouth NHS Trust, Portsmouth – United Kingdom, 2022.
- RDaSH Business Continuity Policy, RDaSH NHS Foundation Trust, Rotherham Doncaster, and South Humber – United Kingdom, 2022.
- Business Continuity Policy and Business Continuity Plan, NHS Sheffield Clinical Commissioning Group, Sheffield – United Kingdom, 2022.
- Business Continuity Policy 6.0, Isle of Wight NHS Trust, Isle of Wight – United Kingdom, 2022.
- Emergency Resilience and Response and Business Continuity Policy, NHS Kernow Clinical Commissioning Group, Cornwall – United Kingdom, 2021.



**Contact Details**

Health Service Executive  
Dr. Steevens' Hospital  
Steeven's Lane  
Dublin 8  
D08 W2A8

Phone: 01 635 2230

Publication Date: 28 February 2025