



HSE Business Continuity Management Handbook

Final Draft v1.0

Table of Contents

Introduction	4
Purpose of this Handbook	4
How to use this Handbook	4
Definition of key terminologies	5
1 Context of the Organisation	8
1.1 Organisational Context	9
1.2 Understanding Stakeholder needs	9
1.3 Establishing the Context of a Business Continuity Risk	11
1.4 Establishing Business Continuity Management Processes	12
1.5 Scoping Business Continuity Management	13
2. Leadership and Support	17
2.1 Leadership	17
2.2 Roles and responsibilities	18
3. Risk Assessment	21
3.1 Risk Identification	21
3.2 Risk Analysis and Evaluation	23
4. Business Impact Assessment (BIA)	28
4.1 Step by step guide to performing a Business Impact Assessment	29
4.2 High level example of a BIA for a Radiology Department	31
5. Strategies and Plans	34
5.1 Developing Business Continuity Strategies	34
5.2 Document BCP	38
5.3 Action cards	40
5.4 Communication	40
5.5 Triggering a BCP	41
6. Training, Testing & Exercising	44
6.1 Training	44
6.2 Embedding BCM In Business As Usual (BAU)	46
6.3 Testing the BCP	47
6.4 Interagency Engagement	50
7. Management Reviews	51
7.1 KPIs	54
7.2 Assurance	55
8. Learning and Improvement	56
8.1 Post Event Reporting	56
8.2 Post exercise reporting	59
8.3 Corrective Actions	60
8.4 Plan Review and Update	62
Appendix 1 - Template Checklist	64

Appendix 2 – Business Continuity Plan Template	65
Appendix 3 - Glossary of terms	70
Appendix 4 - Acronyms	72
Appendix 5 - References	73

Introduction

Purpose of this Handbook

This handbook has been developed to guide, you, the Manager, on how to design, implement, and manage your business continuity management programme in line with the HSE Business Continuity Management (BCM) Policy (2025).

The processes outlined in this Handbook will guide you to develop a Business Continuity Plan (BCP) that is aligned with international good practice. A BCP is a proactive strategy that will help your service to anticipate and navigate disruptions effectively, enabling the continuation of key health services and supporting services, focus on patient safety, and enhance the overall resilience of the HSE.

BCPs can be a mixture of threat-based response plans which are designed to specifically target actions in response to an event e.g., major weather events, cyber-attack, fire, flooding, industrial action or they are designed for the continuity of a specific key service or function following the loss or one or more key resources that supports the service, e.g., staff, ICT, estates/buildings, equipment, suppliers etc.

This handbook will outline BCM roles and responsibilities and will detail steps that the different roles must take. Additionally, this handbook aims to educate and raise awareness on some wider BCM concepts to support Managers in their roles.

How to use this Handbook

In alignment with the BCM Policy, the activities in this Handbook have adopted the Plan-Do-Check-Act (PDCA) methodology and all templates provided are based on the guidance of ISO 22301:2019 Security and resilience — Business continuity management systems.

This handbook is designed to be used to support compliance with the HSE BCM Policy 2023. Specific requirements in the policy, designated with the modal verb 'must' take precedence in achieving the objectives of the business continuity activities.

This handbook has been set out with the following details to support easy navigation and use:

- Color coded sections to provide a reminder of where you are in the PDCA process and links between section headers and content pages to support easy navigation:

Plan	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	In Do phase, you will perform implementation activities focused on performing risk and impact analysis, creating strategies, plans and

	<p>actions to aid the timely and safe recovery of impacted resources and services from potentially disruptive events.</p> <p>Plans may vary from the very detailed to easy-to-follow action cards.</p>
Check	<p>In Check phase, you must confirm the effectiveness of the formalised processes by testing and validating them regularly. This phase also includes implementing continuous monitoring structures to help ensure ongoing operating effectiveness of the BCM plans and processes.</p>
Act	<p>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.</p>

- The Handbook provides several templates, to facilitate easy access and completion, including:
 - Stakeholder Analysis Template
 - Service Mapping Template
 - Business Impact Analysis Template
 - BCP Template
 - Event Log example
 - Training Plan Example
 - Test Plan Template
 - Self-Assessment Template
 - After Action Report Assessment Form
 - Lessons Learned Report
 - Corrective Actions Log
- The Handbook also outlines some practical examples to demonstrate the actions that need to be taken.

Definition of key terminologies

Health Services is used throughout this Handbook and should be taken to mean all Health and Social Care Services.

Supporting Services is used throughout this Handbook and should be taken to mean all supporting services used to deliver Health Services. Examples include but are not limited to operations and activities such as Estates, Equipment, ICT, Finance, Procurement, Security, Waste Management, Laundry, Catering, Electrical, Maintenance, Utilities and a wide variety of other supplier provided services.

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.

Business Continuity (BC) Owner is the individual that is responsible for ensuring that BCM processes are scoped, implemented and managed appropriately and in line with the BCM policy in their Region, Corporate Function or Service area.

BC Leader is the individual that is responsible for leading, facilitating and advising on the technical aspects of the BCM processes. They are responsible for the management and administration of the end-to-end BCM processes that are in scope within their area of responsibility.

BC Support Staff are individuals who are assigned to assist the BC Leader with the implementation and maintenance of the BCM processes.

Further detail of BC roles is provided in [Section 2.2 Roles and Responsibilities](#)

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.

Maximum Tolerable Period of Disruption (MTPD) is the time it would take for adverse impacts which might arise because of not providing a service or performing an activity to become unacceptable (ISO 22301:2019).

Recovery Point Objective (RPO) is the point to which information used by a service or activity must be restored to enable the service or activity to operate on resumption (ISO 22301:2019).

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 (ISO 22301:2019).

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.

Triggering is the act of declaring that an organisation's business continuity arrangements need to be put into effect to continue delivery of key services, operations and activities. (ISO 22301:2019).

Managers in this policy refers to Senior HSE Functional Leaders, Regional Executive Officers (REO), Hospital Group Chief Executive Officers (CEOs), Community Health Organisation (CHO) Chiefs and any other delegated persons designated to represent such a role.

Internal Audit is a service 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).

A full list of definitions / glossary is contained in Appendix 3

1 Context of the Organisation

Managers in the HSE will need to take a risk-based approach and define the scope of BCM processes in the context of the key health services and supporting services in their area of responsibility, in line with ISO 22301.

To define the BCM scope, it is envisaged that the BC Owner, working with the BC Leader, will set and agree the key boundaries of services, operations, activities, and stakeholders within their area of responsibility.

To achieve this, BC Owners will need to identify and document the “universe” of health services, operations, activities within their area of responsibility, then decide which key health services, operations and activities should be in scope and applicable for BCM. This is important as it is impractical nor necessary for every service, operation and activity to be in scope for BCM.

Once set and agreed, the scope of BCM may be expanded or changed at any stage in the future based on new threats, available resources, and lessons learned from emergencies, incidents and events.

1.1 Organisational Context

Strategic planning is a process by which an organisation defines its vision for the future and identifies its strategic objectives. The HSE’s vision and strategic objectives are articulated in its Corporate Plan. On an annual basis, the HSE prepares a National Service Plan that sets out the in-year actions to deliver on these objectives. Each area of the health service in turn develops operational plans that reflect the National Service Plan actions for their area of responsibility.

As Managers in the HSE, you make significant decisions which can impact the delivery of strategic objectives. These may relate to areas such as planning choices, strategy development, investment decisions and resource allocation. Managers assess risks at the decision-making stage, and at the commencement of and during the implementation of these decisions.

In making decisions in relation to BCM, you as a Manager will need to consider the context of your organisation, including factors such as changes in the global healthcare environment, emerging threats to public trust and confidence in healthcare, new healthcare technology, changes to staff availability and mobility, and changing expectations within regulatory, legal and political domains. Some changes will bring new threats which can pose a risk to the continuity of our health services (as seen with the pandemic and cybersecurity incident).

Establishing the organisational context for BCM in your area of responsibility, requires you to also identify the external and internal factors that you and your team must consider when managing risks that could lead to a disruption.

Your internal context includes strategic objectives, governance arrangements, infrastructure needs, funding arrangements, legal and regulatory obligations, resourcing priorities, contractual arrangements, and working with key partners in the delivery of health and social care services. It also includes your workforce, capacity and capability, internal policies and procedures including the Incident Management Framework, Enterprise Risk Management Policy & Procedures, and the Corporate Safety Statement etc.

Your external context includes your external stakeholders, for example, other Principal Response Agencies (PRAs), the Department of Health, and other government departments, Regulators, patients, and service users.

1.2 Understanding Stakeholder needs

The HSE recognises the significance of understanding the diverse needs and expectations of stakeholders, including patients, healthcare professionals, regulatory authorities, employees, and the community. As part of implementing and applying effective BCM processes, you need to identify and prioritise these stakeholders based on their influence, interests, and roles in maintaining health and social care services.

The identification of stakeholders for each in scope area requires a concerted view. It is recommended that stakeholder identification is conducted either through workshops with representatives of all teams within scope or through questionnaires that will enable all teams to share their inputs.

The key questions to be answered in the assessment of all relevant stakeholders are:

- Which groups of persons benefits from the services provided by the function/area?
- Which groups of persons are affected by the services provided by the function/area?
- Which groups of persons provide/deliver the services in the function/area?
- Which groups of persons govern or oversee the services provided by the function/area?
- How will these groups of persons identified above be directly impacted by an unwanted threat event and disruption to services?
- How do we ensure that Patient safety is not negatively impacted?
- Have we considered our vulnerable service users?
- How influential or important are these groups in taking decisions to plan for the recovery and continuity of the services?

- To what extent can these groups of persons prevent the effective implementation of the recovery and continuity strategies of the services?
- What is the best approach to engaging individuals and groups to ensure we effectively plan, implement, and manage our business continuity objectives?

The process and outcome of stakeholder analysis should be documented in a template (see Figure 1). The example below uses a stakeholder analysis that is linked to Renal Services. It should be noted that this list is non-exhaustive, and stakeholders need to be considered for each health service and supporting service.

Figure 1: Example of Stakeholder Analysis Template

Stakeholder Group	Impact (How much does the BCM impact them? (L, M, H))	Influence (How much influence do they have over the effectiveness of the BCM? (L, M, H))	What is important to them?	How could they block the effectiveness of the BCM?	Strategy for engaging the stakeholder
Patients and families	H	L	Continuous access to provision of the service as they need it	Lack of flexibility Mobility issues	Clear Communication plan Transportation Plan
Hospital Staff	H	H	Site safety Patient Safety Proper equipment Designated areas	Lack of flexibility in contract terms Lack of BCM training Not following BCM protocols Lack of equipped resources	Clear communications plan Training / Exercises Cross hospital staff sharing protocols
Suppliers (equipment/ water/taxi services)	M	H	Payment Retention of contracts Patient Safety Contractual Obligations Met	No BCM measures in place Sub-contractor failure	Engagement in training/exercising Clear requirements in contracts
Patient Advocate Group	L	M	Patient Safety Patient Experience	Reject BCM strategies or protocols Political Pressure	Consultation on patient communication and transport plan

1.3 Establishing the Context of a Business Continuity Risk

BCM risks are a category of risk within the HSE Risk Management Framework. Continuity of health services, operations and activities are typically impacted by operational risks (e.g., loss of equipment, buildings, IT, staff, supplier) and environmental risks (e.g., major storms, pandemics). Based on the guidance of the HSE Enterprise Risk Management Policy 2023 Section 2.1.4.2, the following major categories of risks have been identified (see Figure 2). Additional information is provided to link the HSE policy or framework that should typically be used to manage each risk impact, including risks which would typically leverage the HSE BCM Policy and Handbook (2023).

Figure 2: Categories of risk by impact and reference to policy/framework¹

Categories by Risk Impact	Policy or Framework to Manage Risk
Harm to a Person (service user, patient, staff & public)	Incident Management Framework (2020)
Service User Experience	Incident Management Framework (2020)
Business/Service Disruption/Security	Business Continuity Management Policy & Handbook (2023)
Loss of Trust/Confidence or Morale (Public/Staff), including reputational risk	Incident Management Framework (2020)
Organisational Objectives or Outcomes	Enterprise Risk Management Policies & Procedures (2023)
Compliance (legislative, policy, regulatory including data)	Enterprise Risk Management Policies & Procedures (2023)
Financial (including performance to budget, claims, etc.)	Enterprise Risk Management Policies & Procedures (2023)
Environmental/Infrastructure/Equipment	Business Continuity Management Policy & Handbook (2023)

To support the management of different risk categories, there are also different types of plans in place across the HSE that you should be aware of, including:

- Crisis Management Plans
- Crisis Communication Plans
- Emergency Management Plans (EMPs)
- Business Continuity Plans (BCPs)
- ICT Disaster Recovery Plans (DRPs)

¹ HSE Enterprise Risk Management Policy and Procedures 2023, 2.1.4.2 Categorisation by Risk Impact

1.4 Establishing Business Continuity Management Processes

The purpose of BCM is to prepare for, provide and maintain controls and capability for managing the HSE's ability to continue to operate during disruptions. In creating BCM processes the HSE achieves several benefits for patients, staff, and key stakeholders:

1. **Uninterrupted Patient Care:** Effective BCM aims to ensure that key health and social care services remain uninterrupted during unforeseen disruptions such as natural disasters, power outages, or cyberattacks. BCM enables healthcare facilities to continue delivering essential health and social care services and treatments, ideally, without compromising the quality of the services.
2. **Regulatory Compliance:** In every healthcare sector there are strict regulatory requirements which must be always met to ensure patient safety and data security. BCM helps the HSE maintain compliance with healthcare and other regulations by implementing strategies to safeguard patient records, sensitive information, and medical data, even in the face of disruptions.
3. **Operational Resilience:** Standardised BCM processes enhances the operational resilience of healthcare services and facilities by identifying potential risks, vulnerabilities, and key dependencies. By conducting risk assessments and developing robust contingency plans, the HSE can mitigate the impact of disruptions and minimize downtime. This resilience ensures that essential health and social care services are available when needed most.
4. **Reputation and Trust:** The HSE relies heavily on the trust of their patients and the broader community. Implementing and applying BCM processes demonstrates a commitment to patient safety, continuity of care, and ethical practices. By effectively managing crises and ensuring consistent service delivery, the HSE can protect its reputation, maintain patient trust, and foster stronger relationships within communities.

1.5 Scoping Business Continuity Management

As required by the BCM Policy, the BC Owner will define the scope of their BCM to encompass all key health services, operations and activities, within their area of responsibility. The scope will be based on an evaluation of the priority health services, operation, activities and stakeholder requirements in the BC Owner's area of responsibility. This scoping will take account of the planned interdependencies of health and social care processes planned as part of the implementation of Regional Health Areas (RHAs).

BC Leaders, working in conjunction with the BC Owner have several important activities to perform in establishing the scope of BCM for key health services, operations and activities. These include:

1. Clearly **defining the boundaries** of BCM processes, highlighting the interfaces and interactions between health services, operations, activities, and stakeholders.

This definition will ensure that all key elements of the service area are included within the scope and those not considered key are not in scope.

2. Assessing the **potential impact of disruptions** on patient and service user care, health outcomes, and regulatory compliance. Managers will need to identify key healthcare functions, equipment, medical supplies, patient records, and clinical processes that must be prioritised within the BCM to provide uninterrupted services.
3. Identifying and considering all **relevant healthcare regulations**, patient privacy laws, and healthcare industry standards when determining the scope of the BCM. Compliance with legal obligations and regulatory frameworks will be integral to the BCM's design and implementation.
4. Evaluating **internal capabilities, expertise, and resources** necessary to effectively manage disruptions. This assessment will include the availability of healthcare professionals, medical infrastructure, technology systems, and emergency response mechanisms that contribute to the organisation's resilience.

1.5.1 Defining the scope

It will not be possible to apply BCM processes to all services, operations and activities, or to prepare for all potential disruptive events. The scoping of the BCM processes provides you with a clear focus on what is applicable and within the remit of the BCM within your area of responsibility (e.g., a Region, Site, Service, Function etc.).

Identifying the scope of the BCM requires a clear statement identifying the following:

- What health services, operations and activities will be covered by the BCM?
- What support services and functions will be covered by the BCM?
- What locations/sites will be covered by the BCM?
- What external party services are within the scope of the BCM?

What services and functions will be covered by the BCM?

For BCM to be a practical, useful tool to your service, operation or activity, it must be adequately scoped. The identification of key health services, operations and activities to be scoped into the BCM requires the BC Owner and BC Leader to understand the various component parts and stakeholders that contribute to the effective delivery of the service or function.

- For example, each Regional Health Area will have an understanding and priority of the many services, operations and activities provided in that region. It is important that all the services, operations and activities offered are detailed and mapped to associated stakeholders and interdependencies so the scope of the BCM can be properly defined.

- This mapping exercise needs to be evaluated and assessed to identify the key services, operations and activities. For each identified area, there needs to be an identification of the maximum allowable downtime for the service, operation or activity.

Outlined below is a service mapping template which has been completed using an example of Procurement and Logistics, focusing on the service of PPE supply. This template can be used for any health service, operation or activity. For example, Maternity Services in Hospital A would consist of Activities such as Perinatal Care, Labor and Delivery Services, Postpartum Care, Counselling and Family Support. The maximum allowable downtime of each of these sub activities may vary.

Figure 3: Service Mapping Template

Type of Service	Service Description	Activities	Dependent Services/Processes	SERVICE REQUIREMENTS					
				Service Location / facility requirements	Our People requirements	Vendor / Suppliers / Contractors	Financial requirements (€)	ICT requirements	Equipment requirements
<i>Clinical Service/ Corp. Service/ Business Service</i>	<i><Brief description of the service></i>	<i><List of activities that complete a cycle of the service></i>	<i><List of services/processes that rely on the successful delivery of this service></i>	<i><Requirements for facilities or locations to support the service></i>	<i><Specific staff requirements for the successful completion of the service – Indicate the regular and number and minimum number></i>	<i><List of third parties/partners /suppliers who support this service></i>	<i><Service costs – equipment and facilities> < staffing costs></i>	<i><Specifications of information and communication technology that support this service></i>	<i><Specifications of equipment that support this service></i>
Procurement and Logistics	PPE supply	PPE training IPC training AMRIC guidance Microbial resistance Infection Control	All HSE services	Warehouses	Warehousing Staff Logistics People on hospital sites	3 rd party delivery/logistics - goods in and goods out 3 rd party systems on minimum inventory Customs	(Based on demand management)	PPE Ordering system Investment Management system Systems in hospitals Stock/management/demand	Vehicles Warehouse tools Forklifts

What locations will be covered by the BCM?

As a Manager, you will have to consider the key location(s) that are within the scope of the BCM within your area of responsibility, the size of operations, nature of operations and how complex it is to deliver the services and activities from other locations. Specific locations may be excluded from the scope of the BCM, however these will need to be justified, documented and agreed with the BC Owner. Additionally, you may identify other locations, stakeholders or services that your BCM processes will be dependent on. In these case Managers should liaise with the BC Leaders and relevant stakeholders in those locations and service areas to ensure BCPs are aligned.

Note: BC strategies in the HSE will involve relocation of key patient and service user services to other locations for a period and therefore the full extent of locations in scope may not be fully determined until the completion of the business impact assessment and definition of continuity strategies.

What third party/supplier services are within the scope of the BCM?

Suppliers and/or contractors form a significant part of the effective delivery of our services and need to form part and/or subjects of the business continuity response. The key considerations for suppliers and contractors include:

- Risk and Impact Analysis – Managers should assess the role and risk presented by each supplier to the health service, operation or activities and the impact of disruptive events to the continuity of the supplier’s services. Understanding and risk assessing the role played by suppliers will enable Managers to design appropriate responses to supplier service challenges and supply chain disruptions.
- Supplier Business Continuity Plan – All suppliers should have a documented and up-to-date business continuity plan that aligns with the HSE’s policy and unique service requirements. This should be enforced as a requirement for contracting new supplier and contractors and should be phased in, were absent today, as part of contract renewals for existing suppliers.
- Key Points of Contact – As part of designing the service or function’s BCP, key contacts of the supplier should be obtained and verified. These contacts and their alternates should be documented in the BCP and reviewed annually or when the services providers role changes.

Additionally, all relevant communication protocols should be established and documented as part of the contact tree in the BCP to ensure they are readily referable when required.

- Recovery Time Objective and Recovery Point Objectives – Managers should review and establish the RTOs and RPOs of the supplier to ensure they align with HSE service continuity requirements and do not lead to delays in delivery of services.
- Test and validation – As part of periodic testing of the BCP, supplier activations should be agreed and tested to verify their effectiveness.
- Contractual agreements – Service contracts with suppliers and contractors should at a minimum document the following:
 - Supplier roles and responsibility as part of disruption recovery and business continuity management.
 - Contractual consequences for not meeting the continuity requirements.

- Supplier responsibility for ensuring the continued security and privacy of HSE patient and business data accessed during a continuity event.
- Auditability of the supplier's BCM arrangements should be detailed as a requirement to enable the HSE to trust and verify readiness during self-assessments and internal audits.
- HSE contracts with the supplier should mandate the prompt reporting and periodic updates of significant events or near misses within the supplier that could affect or has the potential to affect the delivery of services to the HSE.

You should seek to mitigate single point of supplier failure for key services. This may involve strategic consideration to the procurement of an alternate/multiple supplier model and contracts as part of an overall resilience strategy in the event of a disruption to one key supplier.

2. Leadership and Support

To enable effective BCM processes, senior management of the HSE need to demonstrate a commitment to these processes and key roles and responsibilities must be assigned in line with guidance outlined in ISO22301.

Overall accountability for BCM within the HSE rest with the CEO. The HSE CEO will provide the leadership for deciding accountability and ownership of BCM within the HSE Centre and Regions. Senior leaders both clinical and functional across the HSE will be BC Owners and they in turn may delegate responsibility for management of BCM to other BC Owners and BC Leaders given the complexity of the health and social care system.

It is envisaged that REOs are BC Owners in their own regions and will provide the leadership for implementing accountability and ownership of BCM. Both the HSE Centre and Health Regions must work together on how resources (including people, suppliers, infrastructure, equipment etc.) will be shared, and strategies aligned to achieve the common goals and objectives of the HSE.

Overarching BCM governance structures should be established with a view to assist/help with standardising the overall implementation of BCM across the health system.

What part does everyone play?

Everyone in the HSE or associated with the HSE has a part to play in the effectiveness of BCM processes and activities. This may take the form of communicating incidents and events promptly, participating in test exercises, directing response and recover activities, adhering to response and recovery directives or partaking in after action reviews and lessons learned activities. Staff have a part to play in identifying and communicating any new or emerging threats or risks which if left untreated could result in a disruption to the continuity of key health services, operations and activities. Feedback of this nature should be encouraged in all teams.

2.1 Leadership

In the introduction to the BCM policy the CEO highlighted his commitment to ensuring that Business Continuity Management forms an integral part of the HSE's journey toward a more resilience organisation. The HSE Executive Leadership Team (ELT) will be responsible for providing direction, allocating necessary resources, and communicating the importance of business continuity within the organisation.

The HSE CEO will provide the leadership for deciding accountability and ownership of BCM within the HSE. It is expected that the REOs will provide the leadership for implementing BCM within their respective Health Regions, including assignment of key

roles and responsibilities for BCM. Both the HSE Centre and Health Regions will need to work together on how resources are shared, and strategies aligned to achieve common goals and objectives.

Managers will be made responsible for BCM across the HSE (nationally, regionally and at key locations) and within key operational support functions (e.g., Estates, HR, IT, Procurement). Appropriately, qualified people will need to be appointed as BC Owners, BC Leaders and BC Support Staff for BCM processes to operate effectively.

The effective management of business continuity should be aligned to the activities of existing structures and processes for Emergency Management and Incident Management and Risk Management.

2.2 Roles and responsibilities

Everyone in the HSE or associated to HSE has a part to play in the effectiveness of their BCM activities. This is either through communicating incidents and events promptly, participating in test exercises, directing response and recover activities, adhering to response and recovery directives or partaking in after action reviews and lessons learned activities. Staff also have a part to play in identifying and communicating any new or emerging threats or risks which if left untreated could result in a disruption to the continuity of key health services, operations and activities.

The table below provides further details on the key roles and responsibilities:

Figure 4: Roles and Responsibilities

Role	Definition	Key Activities
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>	<ul style="list-style-type: none"> ▪ Assign roles and responsibilities for BCM in their area of responsibility, including BC Leaders and BC Support Staff ▪ Ensure the establishment of BCM processes in line with the policy ▪ Review and approval of BCM budget ▪ Review and approval of the BCP ▪ Approving the triggering and standing down of the BCP ▪ Periodic communication of the importance of the BCM to all staff and key stakeholders (Communication may be sent on behalf by BCM Leader) ▪ Supporting and participating in BCM test exercises and training events ▪ Ensuring the intended outcomes/KPI's for BCM are achieved in their area.
Business Continuity	<p>The role of the Business Continuity Leader is to support the BC Owner by leading, facilitating and advising on the</p>	<ul style="list-style-type: none"> ▪ Implementation and maintenance of BCP and supporting artefacts (Risk

Role	Definition	Key Activities
Leader (BCL)	<p>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> <p>They will participate in BCM training and learning activities to support their roles and the roles of the BCSS's in their area/function.</p>	<p>Register, BIA, Strategies, Plans, Test Exercises, Lesson Learned log)</p> <ul style="list-style-type: none"> ▪ Implementation and maintenance of Threat & Risk Assessment and BIA ▪ Must engage with Subject Matter Experts (SMEs) as outlined below. ▪ Managing the triggering and standing down of the BCP ▪ Actively engaging in test exercise programs and planning training events ▪ Review and sign off BCP test reports ▪ Ensure continuity of staff within the BC roles and ensure adequate training is performed when there is staff change over ▪ Integrating BCM activities in daily operations of the areas/function ▪ Maintaining relationships and communication channels with other BC Leaders in other locations/functions ▪ Situational awareness of other functions that deal with crisis's and emergencies ▪ Ensuring BCM improvement actions are implemented in a timely manner
Business Continuity Support Staff (BCSS)	<p>Business Continuity Support Staff should be identified to assist the BC Leaders with the implementation, coordination and maintenance of the BCM processes in their area/function.</p>	<ul style="list-style-type: none"> ▪ Supporting the BC Leader in all aspects of their role ▪ Coordinating interactions with other BC teams, SMEs and external stakeholders ▪ Planning for test exercises and training events ▪ Assisting with execution of BCP's ▪ Managing corrective actions/lessons learned logs ▪ Monitoring of new threats and risks ▪ Reviewing supplier BCP's ▪ Maintaining records of all BCM activities in their area/function
Business Continuity Action Owner	<p>An Action Owner is accountable to the BC Owner and is responsible for ensuring delivery of a BCM related action assigned to them and reporting on progress relating to the achievement of that action.</p> <p>Actions will be closed once completed and operating effectively.</p>	<ul style="list-style-type: none"> ▪ Agreeing with the action wording, priority and due date ▪ Executing assigned tasks in the BCM actions log to completion ▪ Reporting on the status of actions to the BC Support Staff periodically

In addition to the formal roles outlined above, you as a Manager, will need to engage with Subject Matter Experts (SMEs) when creating your BCP and when considering any training or test exercise activities. The role of the SME is to advise and assist the BC Owner and BC Leaders with the design, implementation, and maintenance of BCM processes in their area/function. SMEs may be used for:

- Identifying and analysing specific threats and risks
- Leading the assessment of likelihood and impact of disruptive events within their area
- Consultative advice on strategies, resources, funding, systems, procedures, regulations, legal and safety concerns etc.
- Monitoring of event triggers
- Participation and leadership of triggered BCP's

There are many SMEs in the HSE. These include but are not limited to resources working in – Clinical, Health & Safety, Occupational Health, Estates, Data Protection, HR, Finance, Risk, IT, Digital and Cybersecurity, Quality and Patient Safety Staff etc.

Note: Additional external support may also be sought from time to time to assist with review, implementation and improvement activities associated with BCM.

3. Risk Assessment

Managers must conduct a risk assessment (recommended at least annually), to identify and verify potential threats, risks, associated causes and impacts on health and social care services and functions in their area of responsibility. Typically, the BC Leader will be responsible for managing the annual BCM risk assessment exercise.

Why carry out a risk assessment within the BCM process?

1. It is an important and effective tool to help identify and possibly prevent or reduce the impact of potentially disruptive events on services. It needs to be performed at an appropriate granular level to be useful and to stand up to scrutiny.
2. Prevention and reduction of potential impacts of disruptive events and incidents represents an opportunity for the HSE and is a core objective of risk management processes.
3. The BCM risk assessment is designed to help prioritise the “risks that really matter” to the organisation based on potential likelihood of the threat or risk occurring and the potential disruptive impact on health services, operations, and activities. Once priority is agreed, you as a Manager can decide how best to use our limited resources to prioritise risk mitigation and business continuity management processes.

3.1 Risk Identification

Identifying what could disrupt our services:

In such an ever-dynamic environment, identifying disruptions requires both a bottom up and top-down approach. Identifying threats or causes of disruptions is a pivotal step towards improving the HSE's resilience. By diligently assessing internal and external factors, as recommended by ISO 22301, an organisation can pinpoint potential disruptions that could undermine services, operations, and activities.

Threats or causes of disruptions encompass a wide spectrum, ranging from natural disasters to cyberattacks, supply chain interruptions to workforce disruptions. A comprehensive threat identification process enables the HSE to tailor response strategies and allocate resources effectively to address the most important threats and risks to services. Through this proactive approach, we can create a more resilient organisation that is not only prepared for foreseeable challenges but also equipped to navigate the unforeseen with greater agility and confidence.

Risk identification is the process of finding, recognising, and describing risks. Risk identification is an ongoing activity of all Managers and their teams and must be performed annually at a minimum. While performing risk identification, the BC Leader should engage all teams, departments, and specialties through workshops or other means.

To perform an effective risk identification, the BC Leader will need to perform research in their areas of responsibility and review the following:

- Events that have disrupted HSE's operations in the past (examples include the COVID pandemic, industrial disputes, cybersecurity attacks, major weather events).
- Events that have affected other national health service providers across the globe.
- Changes in records of extreme weather, climate and natural disasters that are retained by the Environmental Protection Agency of Ireland.
- Records of past building and facility incidents (e.g., fires, flooding, equipment damage).
- Technology related threats and events recorded in Ireland and across global health service providers.
- Analysis of surges that have caused significant challenges in the demand and availability of health services, staff, or facilities at cyclical times over the years.

A sample of common causes and impacts of disruptive events have been detailed below for consideration. It should be noted that while it may be useful for Managers to consider the below events and impacts, they will not need a plan for each scenario outlined.

Figure 5: Common Causes & Impacts of disruption

Common Causes	Impacts (on services, operations, activities)
<ul style="list-style-type: none"> ▪ Weather Events (e.g., Storms) ▪ Epidemic illness ▪ Industrial Action ▪ Pandemic illness ▪ School closures ▪ Sudden onset / surge demand ▪ Transport disruptions 	<p><i>resulting in</i></p> <ul style="list-style-type: none"> ▪ critical service delay or closures
<ul style="list-style-type: none"> ▪ Cyber Attacks ▪ Introduced Virus ▪ Destruction of paper files ▪ Network Failure ▪ Full scale loss of connection ▪ Deliberate staff interference 	<p><i>resulting in</i></p> <ul style="list-style-type: none"> ▪ Data stolen/lost ▪ Failure of back up or failsafe ▪ Lack of Access to data and ICT
<ul style="list-style-type: none"> ▪ Damage to internal telephone network ▪ Damage to the data network ▪ Destruction of active directory ▪ Localised hardware failure ▪ Loss of major application ▪ Loss of minor application 	<p><i>resulting in</i></p> <ul style="list-style-type: none"> ▪ critical service closure/delay

Common Causes	Impacts (on services, operations, activities)
<ul style="list-style-type: none"> ▪ Loss of mobile/telephone phone networks ▪ Loss of switchboard ▪ Server failure ▪ Staff tampering 	
<ul style="list-style-type: none"> ▪ Contamination ▪ Crime Scene ▪ Disruption to direct medical gas ▪ Disruption to water supplies ▪ Electric Supply Disruption ▪ Failure of fixed equipment ▪ Fire ▪ Flooding ▪ Introduction of cordon ▪ Loss of heating/cooling ▪ Structural Defect/Failure ▪ Terrorist Attack 	<p><i>resulting in</i></p> <ul style="list-style-type: none"> ▪ Loss of access to operating premises
<ul style="list-style-type: none"> ▪ Contamination/product quality ▪ Management Failure Breach ▪ Industrial action by drivers ▪ Unofficial Industrial action in supplier ▪ Supplier goes into administration ▪ Supply/Procurement chain collapse 	<p><i>resulting in</i></p> <ul style="list-style-type: none"> ▪ Contract Breach ▪ Failure to fund/supply

3.2 Risk Analysis and Evaluation

3.2.1 Risk Analysis

Risk analysis is a process of determining how the identified threats or risks can affect the HSE and estimating the level of risk attached to it. To establish the level of exposure to the identified risks we assess the likelihood and impact. This requires the person/team assessing the risk to rate the risk across two dimensions, that of Likelihood and Impact. The HSE has developed a Risk Assessment Tool for this purpose, which can be found in Appendix 2 of the HSE's Enterprise Risk Management Policy and Procedures 2023.

The process for rating risk is:

- 1) Using the Likelihood Table, see Appendix 5, identify, and assign the likelihood score of the risk occurring on a scale of 1 to 5;
- 2) Using the Risk Impact Table, see Appendix 5, identify the primary impact category and assign the impact score of the risk on a scale of 1 to 5; and
- 3) Multiply the two scores, to get the risk score. Risk Score = Likelihood score x Impact score

4) Then using the HSE Risk Rating Matrix, align the score to a risk rating of High, Medium, or Low

Likelihood Rating

Included in the Risk Tool is the below Likelihood table to assist with the rating of likelihood. Assess and assign the likelihood score of 1-5 from the most appropriate dimension used for likelihood of a risk, that is, probability or frequency.

Figure 6: Likelihood Scores

Score	Likelihood	Probability of Occurrence	Frequency
5	Almost certain	≥ 90%	At least monthly
4	Likely	60% to 90%	Bi-Monthly
3	Possible	30% to 60%	Occurs every 1 to 2 years
2	Unlikely	> 5% to 30%	Occurs every 2 to 5 years
1	Rare	≤ 5%	Occurs every 5 years or more

Impact Rating

The HSE has identified several risk impact categories to be managed which are detailed in the HSE Risk Impact Table. One category is '*Business/Service disruption/Security (unauthorized and/or inappropriate access to systems/assets including data)*' which is described as '*issues that would affect an organisation's ability to provide service e.g., deregistration, fire, flood, ICT or electric outage, industrial strikes, lack of access to systems/assets.*'

Having decided on the primary impact category, ask yourself what would be the impact if this risk was to occur? How would you describe this impact should it occur? Then, using the Risk Impact Table, assign a score of 1 to 5 to the impact that best aligns with the descriptions provided.

When scoring, a 1 would indicate that the risk impact is negligible, conversely a 5 would indicate that the risk impact would be considered extreme.

Further detail is included in section 3.3 Procedure: Risk Analysis (including Risk Rating) of the Enterprise Risk Management Policy and Procedures 2023.

How to get a Risk Score

Simply, having established the likelihood and impact scores, these scores should be multiplied to get the risk score.

As stated before; **Risk Score = Likelihood score x Impact score**

Figure 7: Risk Scores

Risk Scoring Table

5 Almost Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Likely	2	4	6	8	10
1 Rare	1	2	3	4	5
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Extreme

How to get a Risk Rating

Now with the risk score to hand, as can be seen from the HSE Risk Rating Matrix shown in Figure 8 below, the following are the groupings of risk ratings, dependent on the score:

- High risks are scored between 15 and 25 and coloured Red.
- Medium risks are scored between 6 and 12 and coloured Amber.
- Low risks are scored between 1 and 5 and coloured Green.

Following the calculation of the above score, giving the inherence risk level, BC Leaders need to:

- Document and assess the existing controls in place to mitigate the risk.
- Re-assess the likelihood and impact of the threat after considering the existing controls, giving the residual risk level.
- Assess which of the risks are acceptable or the desired target risk rating, and do or do not require further corrective action.
- Determine the follow up actions that need to be taken to further mitigate or manage the risk.

Risk Evaluation

The purpose of risk evaluation is to make decisions based on the residual risk rating to determine whether the risk requires further management action e.g., specific BC plan.

The required action will depend on the risk rating as outlined below:

Figure 8: Risk Rating

Risk Rating	Acceptable/ Not acceptable	Action
High (Red)	Not acceptable	Risks identified within this range require strategic responses and supporting mitigating activities that ensure that the potential impact is appropriately reduced. The actions required must be assigned to action owners and their completion should be monitored by Business Continuity Support Staff.
Medium (Amber)	Acceptable / Not acceptable	Such risks require consideration by the assessment team on whether appropriate strategic responses are required. In most cases, where the potential impact is acceptable, the assessment team would need to consider designing response plans for the management of stakeholder expectations.
Low (Green)	Acceptable	Such risks do not require tailored strategic responses. Quarterly monitoring, review, and/or testing of controls will be in place to ensure that controls remain effective to manage the risk and reduce its potential impact.

- Clearly, the most effective approach to mitigate any risk or threat is to take actions that prevent it from becoming an issue or an event in the first instance. Where all available prevention and detection actions have been taken, Managers need to decide where formal response actions need to be taken should the risk or threat occur. This is where BC Leaders decide which risks or threats warrant an action such as the development of a specific business continuity plan or action cards etc.
- An example of such threat-based actions may include:
 - We need to develop a major weather event response plan for a site.
 - We need to develop action/battle cards to rapidly contain a new cyber-attack.
 - We need to develop a severe flooding response plan in a hospital location where flooding risk is rated High and/or increasing due to climate change.
- Where a BC Leader and BC Owner have decided to develop a specific threat-based response plan or action cards they will document that decision here in the Risk Assessment stage of the overall BCM process. Managers can proceed to Section 5 “Strategies & Plans” to obtain guidance on how to develop these plans and they do not need take these decisions through the BIA process.
- The BIA process is focused on how broader services, operations or activities will be impacted by any type of disruption (irrespective of the cause) and requires a more holistic approach and assessment before you as a Manager can progress to Section 5 “Strategies & Plans”. It is anticipated that BCM plans for your area of responsibility will contain a hybrid of “threat or cause based response and recovery plans” and “service, operational or activity” based response and recovery plans.

- In line with the HSE risk management process, significant changes in the service operations and environment, presenting new potential disruptions to health services, should result in an out of schedule re-assessment of threats and risks.

Full guidance on how to complete a Risk Assessment is provided for in the **HSE Enterprise Risk Management Policy and Procedures (2023)** available at the following link:

[HSE Enterprise Risk Management Policy and Procedures 2023](#)

4. Business Impact Assessment (BIA)

Understanding how we could be affected:

Managing a complex organisation such as the HSE involves the allocation of limited resources. Evaluating health services, operations and activity impacts within a BCM context is essential in assessing the potential consequences of major disruptions. Drawing on ISO 22301's guidance, the Business Impact Assessment (BIA) process involves a comprehensive analysis of how a variety of threats and risks could impact key health services, operations and activities.

By quantifying potential operational, societal, and financial impacts the BC Owners and BC Leaders can prioritise their response efforts and allocate the HSE's limited resources strategically. The BIA evaluation provides a deeper understanding of the impacts of different scenarios, enabling you to devise clearer mitigation strategies and more effective business continuity recovery plans.

A thorough evaluation of key health services, operations and activity impacts will also equip you the Manager with the insights needed to make informed decisions that strengthen resilience and assist with maintaining service continuity during major disruptions.

Why carry out a Business Impact Assessment within the BCM process?

1. A Business Impact Assessment (BIA) is a critical component of the BCM process and involves a comprehensive assessment of the processes and dependencies that are key to the delivery of health services, operations, and activities.
2. The BC Leader, working in conjunction with other Managers, will be responsible for coordinating and leading the BIA exercise. When executed well, it enables Managers to quantify the potential impacts of major disruption and to prioritise where recovery strategies and plans are needed the most.
3. The BIA will help you as a Manager to understand firstly the operational implications of a disruption to a service, operation or activity and other impacts such as financial, reputational or regulatory implications.

Note: Determining the impact of disruptions on key health services, operations and activities will often require the input of Subject Matter Experts (SME's) (refer to the [roles and responsibilities](#) section). The BIA exercise also works best when it involves cross team participation. A cross team approach enables better context setting, discussion and prioritization, especially when it leverages the voice, experience and knowledge of relevant stakeholders.

4.1 Step by step guide to performing a Business Impact Assessment

The BC Leader, working with other Managers, Staff and SME's, will assess and prioritise the criticality of the health and social care services, operations and activities provided in their area of responsibility by performing and documenting these steps:

- **Step 1.** Identify and verify the universe of health and social care services, operations, activities, and stakeholders within scope (this may have been completed in the PLAN phase => refer to section [1.2 Understanding Stakeholder Needs](#) and [1.5 Scoping Business Continuity Management](#)).
- **Step 2:** Assess if the health and social care service, operation, or activity is a Priority 1, 2 or 3 in line with Figure 9. Agree with the BC Owner which Priority services are in scope for the next steps in the BIA.
- **Step 3.** Identify and document the activities or processes fundamental to support the selected in scope priority² health and social care services, operations, and activities.
- **Step 4.** Identify and document the dependencies and interrelationships with and between other health and social care services, processes, and support functions for the selected priority services, operations and activities within scope.
- **Step 5.** Determine and document the duration within which a disruption of an identified in scope key health and social care service, operation and activity may cause irreparable damage (Maximum Tolerable Period of Disruption – MTPD). This assessment will be based on the core activities/processes identified in Step 1 and 2.
- **Step 6.** Determine and document the duration within which it is required to restore the in-scope key health and social care service, operation, and activity (Recovery Time Objective – RTO).
- **Step 7.** Determine the point to which system-based information used by an in-scope service, operation or activity must be restored to enable the service, operation or activity to operate effectively on resumption (Recovery Point Objective – RPO).

² Priority health and social care services, operations and activities will differ between services, and these will be determined in the scoping phase and through the BIA process.

Figure 9 - Priority Rankings Table

- Step 8. Following these steps, the BC Leader should now be able to determine

Disruption impact and recovery objectives		
Priority 1	Priority 2	Priority 3
<p>0 – 24 Hours</p> <p>Services, operations, or activities that cannot tolerate any disruption beyond the maximum of 1 day. If activities are not resumed immediately it may result in significant negative impacts on patient or service users, our staff and/or other HSE services.</p> <p>Priority 1 items may need a high-level BC Strategy and a detailed BC Plan. This will be agreed between the BC Owner and BC Leader.</p>	<p>> 24 hours</p> <p>Services, operations or activities which can tolerate a very short period of disruption and must be resumed within 24 hours to a maximum week before a failure to return to BAU starts to materially compromise health and social care services.</p> <p>Priority 2 items may need a high-level BC Strategy and a Plan on an exception basis. This will be agreed between the BC Owner and BC Leader.</p>	<p>>7 days</p> <p>Services, operations, or activities that can be delayed for more than a week given our Priority 1 and 2 objectives. They can tolerate a >7 days disruption before a failure to return to BAU starts to materially compromise health and social care services.</p> <p>Priority 3 items may need a high-level BC Strategy but unlikely to need a BC Plan. This will be agreed between the BC Owner and BC Leader.</p>

which health services, operations and activities will be proposed as in scope for development of BC Strategies and BC Plans based on the priority ratings.

- This may mean that Priority 1 items will require a detailed BCP in place, whereas a Priority 3 may have a high-level strategy. The BC Owner should be informed and advised by the BC Leader, based on the BIA analysis, where new BC Strategies and BC Plans should be developed or refreshed and, where importantly, they are not required.

Section 5 ([5. Strategies and Plans.](#)) details the approach for developing strategies and plans. The additional information captured in the BIA will also become relevant in the next stage of BCM.

4.2 High level example of a BIA

Two example BIAs are documented below. One for a Radiology Department and one for a Community Nursing service. This is non-exhaustive list and is provided for illustration purposes. You as a Manager, will be required to follow the steps outlined above for your own area of responsibility and will likely need to consult with a range of other stakeholders and SME's to complete the BIA process.

Figure 10: Example of a Business Impact Assessment for a Radiology Department

Type of Service/Operation	Core Activity Description	Dependent Services/Activities	Maximum Tolerable Period of Disruption (MTPD)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Priority Ranking
Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
<Corporate / Clinical / Support Service>	<Brief description of activities/processes>	<List of services/activities that rely on the successful delivery of this area>	<Specification of the Maximum Tolerable Period of Disruption for Core Activity – Step 2>	<How long it should take to restore the service /operation>	<How far back ICT data is needed to effectively perform the services after an event>	<Ranking of activity based on figure 9>
Radiology Department	X-ray Imaging	Emergency Services Orthopaedics Gastroenterology Cardiology	16 hours	Within 1 day	<1 hour	1
	CT Scan	Emergency Services Neurology Oncology Diagnostic Imaging	16 hours	Within 1 day	<1 hour	1
	MRI	Neurology Orthopaedics Oncology	72 hours	Within 1 day	<1 hour	2
	DXA Scan	Orthopaedics Endocrinology Rheumatology	72 hours	Within 1 day	<1 hour	2
	Radiation Therapy Planning	Neurology Oncology	72 hours	Within 1 day	<1 hour	2
	Radiation Safety and Dosimetry	All radiology services	6 hours	Within 1 day	<1 hour	1
	Weekly team meetings	All radiology services	7 days	Within 3 days	<1 day	3

In this example you will note that X-Ray Imaging, CT scans and Radiation Safety and Dosimetry are ranked as Priority 1's as the MPTD is less than 24 hours. MRI, DXA Scans and Radiation Therapy Planning are ranked as Priority 2 with a MPTD of greater than 24 hours but less than 1 week. The Radiation Team Meeting is a Priority 3 as the MPTD is longer than a week.

Using this information, the BC Leader is now able to consider where the focus for developing BC Strategies and Plans should be within the Radiology Department.

Figure 11 - Example of a Business Impact Assessment for a Community Nursing Service

Type of Service/Operation	Core Activity Description	Dependent Services/Activities	Maximum Tolerable Period of Disruption (MTPD)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Priority Ranking
Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
<Corporate / Clinical / Support Service>	<Brief description of activities/processes>	<List of services/activities that rely on the successful delivery of this area>	<Specification of the Maximum Tolerable Period of Disruption for Core Activity – Step 2>	<How long it should take to restore the service /operation>	<How far back ICT data is needed to effectively perform the services after an event>	<Ranking of activity based on figure 9>
Community Nursing	Support for vulnerable populations	Mental Health Service Primary Care Centre Community Pharmacy Nursing Staff Patient Data Accessibility of patient home Palliative Care Newborn Blood Spot Screening Programme	8 hours	Within 1 day	Full restoration of information	1
	Home Health Care	Primary Care Centre Community Pharmacy Nursing Staff Patient Data Accessibility of patient home	8 hours	Within 1 day	Full restoration of information	1
	Chronic Disease Management	Primary Care Centre Community Pharmacy Nursing Staff Patient Data Accessibility of patient home	8 hours	Within 1 day	Full restoration of information	1
	Clinics	Nursing Staff Patient Data	24 hours	Within 1 day	Full restoration of information	2
	Weekly team meetings	Community Health Teams	7 days	Within 3 days	<1 day	2

In this example you will note that Support for vulnerable populations, Home Health Care and Chronic Disease Management are ranked as Priority 1's as the MPTD is less than 24 hours. Clinics are ranked as Priority 2 with a MPTD of greater than 24 hours but less than 1 week. The Weekly team meeting is a Priority 3 as the MPTD is longer than a week.

Using this information, the BC Leader is now able to consider where the focus for developing BC Strategies and Plans should be within the Radiology Department.

The BC Leader should then make a recommendation to the BC Owner based on the results of the BIA, available resources and management appetite and experience to deal with different disruptions. For example, the BC Leader may recommend to the BC Owner that the area creates strategies and a detailed plan for all Priority 1 activities, high level strategies only for Priority 2 activities and they may decide to risk accept that no BC strategy or plan is required for Priority 3 ranked areas.

5. Strategies and Plans

Selecting business continuity strategies and plans:

Selecting which areas are in scope for business continuity strategies and plans is a pivotal decision-making process within BCM that stems from ISO 22301's guidance.

Across the HSE today there are many examples of formal strategies and plans in place to assist you as Managers in dealing with a range of disruptive events. This includes plans to manage major weather events, emergency department surge events, major accidents. In addition, many areas of the HSE (including national/regional/site health and social care services, corporate Centre operations and clinical locations) have agreed continuity strategies, plans or protocols to deal with a variety of disruptive scenarios to services, operations and activities.

BC strategies are “What” statements, which outline at a high level what is proposed to minimise a disruption to a specific health and social care service, operation or activity. BC plans follow the strategy and detail “How” these strategies will practically and effectively operate should they be needed. The outcome from the BIA should be used to determine which service, operation or activity need a Plan and which need a Strategy.

As highlighted in Section 3. Risk Assessment, BC strategies and plans (including action cards) can be threat or cause based e.g., designed to address threats or causes of events such as major weather events, cyber-attack, fires, floods. They can also be designed around continuity of a key service, operation or activity which may suffer severe disruption at any stage due the loss or one or more key resources (e.g., People, Premises, Providers, Processes, Systems).

In the earlier example, the Radiology Department may decide to develop a set of strategies and plans, for example, what to do in the event of a) a sudden unanticipated depletion of staff b) a major ICT service disruption c) a complete or partial loss of estates/buildings d) failure of key radiology equipment or a key radiology supplier.

5.1 Developing Business Continuity Strategies

Following approval of the BIA by the BC Owner, BC Leaders and Managers should document all agreed prioritised business continuity strategy statements which are applicable to their areas of responsibility. All documented strategies will adhere to the following key principles:

Figure 12: Key Principles for Continuity Strategies

Key Principles for Continuity Strategies
Aligned with HSE's values of Care, Compassion, Trust, and Learning
Ensure patient safety obligations at all times
Meet the requirements to continue and recover prioritised activities within the identified time frames and agreed capacity
Protect prioritized activities and legal and regulatory obligations
Reduce the likelihood of disruption
Shorten the period of disruption
Limit the impact of disruption on the HSE's services
Provide for the availability of adequate resources
Represent a reasonable combination of cost and benefits to the HSE
Can be matched with implementation resources (people, systems, infrastructure, equipment, logistics, finance and / or suppliers)

A template has been provided below that guides the documentation of BC strategies and plan options.

The examples below continues the Radiology and Community Nursing examples to show some illustrative strategies. These are simply examples, and it is up to the BC Leader and other Managers to consider and document the most acceptable strategies for your service, operation or activity.

Figure 13: Recovery Strategy example for a Key Hospital Service

Key Service	Priority Rating	Trigger Threshold	Trigger Risk Event	Strategy to Respond	Action Plan	Ownership
<Service / Operation/Activity description>	<Priority Rating from BIA>	<At what threshold should the BC Plan/Strategy be invoked>	<What types of risks for this service/operation would cause us to trigger BCP>	<What are our response strategies for each risk>	<Action 1><Date> <Action 2><Date> <Action 3><Date>	<Action 1 Owner> <Action 2 Owner> <Action 3 Owner>
RADIOLOGY						
X-ray Imaging	1	Complete loss of service anticipated for >12 hours	Complete or partial loss of our real estate/clinical work area.	All services for priority 1's move to Hospital B and C	1.We need to contact Hospital B and C to understand their capacity to continue patient services for our priority 1 areas. 2.We need to agree and align our hospital transfer protocols with other areas impacted. 3.We need to understand and agree transport requirements for our patients.	BC Leader Head of Estates Head of Estates

CT Scan	2	Loss of service anticipated for >72 hours	Sudden loss of our primary equipment.	Leverage every other instance of key technologies held across our site.	1.We need approval for emergency spending in the event of sudden failure of equipment 2.We need to have rapid repair/purchase agreements in place for new equipment	Hospital CFO Head of Procurement
Radiation Safety and Dosimetry			Sudden depletion of our staff	Appoint skeleton staff to operate the department on rotas starting with priority 1 services. We will stop all non—essential sub services /activities (Priority 2/3's) until they reach their MTPD triggers.	1.We need to define and agree what are our minimal staffing levels and what skills are needed to operate services safely. 2.We need to create and maintain a rota for skeleton staff and skills requirements.	Head of Department Head of Department
MRI			Complete or partial loss of our real estate /clinical work area.	All services for priority 2's move to Hospital B and C	As above.	As above.
DXA Scan	2	Loss of service anticipated for >72 hours	Sudden loss of our primary equipment.	Leverage every other instance of key technologies held across our site.		
Radiation Therapy Planning			Sudden depletion of our staff	Appoint skeleton staff to operate the department on rotas starting with priority 1 services.		
Weekly team meetings	3	N/A	N/A	Weekly meetings to resume following stand down of BCP.	N/A	N/A

Figure 14 - Recovery Strategy example for a Key Community Service

Key Service	Priority Rating	Trigger Threshold	Trigger Risk Event	Strategy to Respond	Action Plan	Ownership
<Service / Operation/Activity description>	<Priority Rating from BIA>	<At what threshold should the BC Plan/Strategy be invoked>	<What types of risks for this service/operation would cause us to trigger BCP>	<What are our response strategies for each risk>	<Action 1><Date> <Action 2><Date> <Action 3><Date>	<Action 1 Owner> <Action 2 Owner> <Action 3 Owner>
COMMUNITY NURSING SERVICE						

Support for vulnerable populations	1	Complete loss of service anticipated for >12 hours	Inability for nursing staff to travel due to a severe weather event	Utilise National Ambulance Service (NAS) and other emergency response services to get nursing staff to patients.	<ol style="list-style-type: none"> 1.We need to contact the Area Emergency Planning Group to understand the emergency service contacts in the Area. 2.We need to agree and align with NAS and other relevant services. 3.We need to understand and agree the highest priority patients in the area to prioritise where staff go. 	BC Leader
			Home Health Care	Sudden depletion of our staff	Appoint skeleton staff to operate the service starting with priority 1 services. We will stop all non—essential sub services /activities (Priority 2/3's) until they reach their MTPD triggers.	<ol style="list-style-type: none"> 1.We need to define and agree what are our minimal staffing levels and what skills are needed to operate services safely. 2.We need to create and maintain a rota for skeleton staff and skills requirements.
Chronic Disease Management	2	Loss of service anticipated for >72 hours	Complete or partial loss of our real estate /clinic work area.	All services for priority 2's move to nearby Community Health Centre.	<ol style="list-style-type: none"> 1.We need to contact the Community Leads in our area to understand where movement would be possible. 	As above.
			Sudden loss of our primary equipment.	Leverage every other instance of key technologies held across our site.	<ol style="list-style-type: none"> 1.We need to define what technologies we have across the community and how we can re-deploy these. 	
Clinics	3	N/A	N/A	Weekly meetings to resume following stand down of BCP.	N/A	N/A
Weekly team meetings						

There are many options to consider as strategies for reducing the impact of disruptive events. The figure below provides some practical areas to consider.

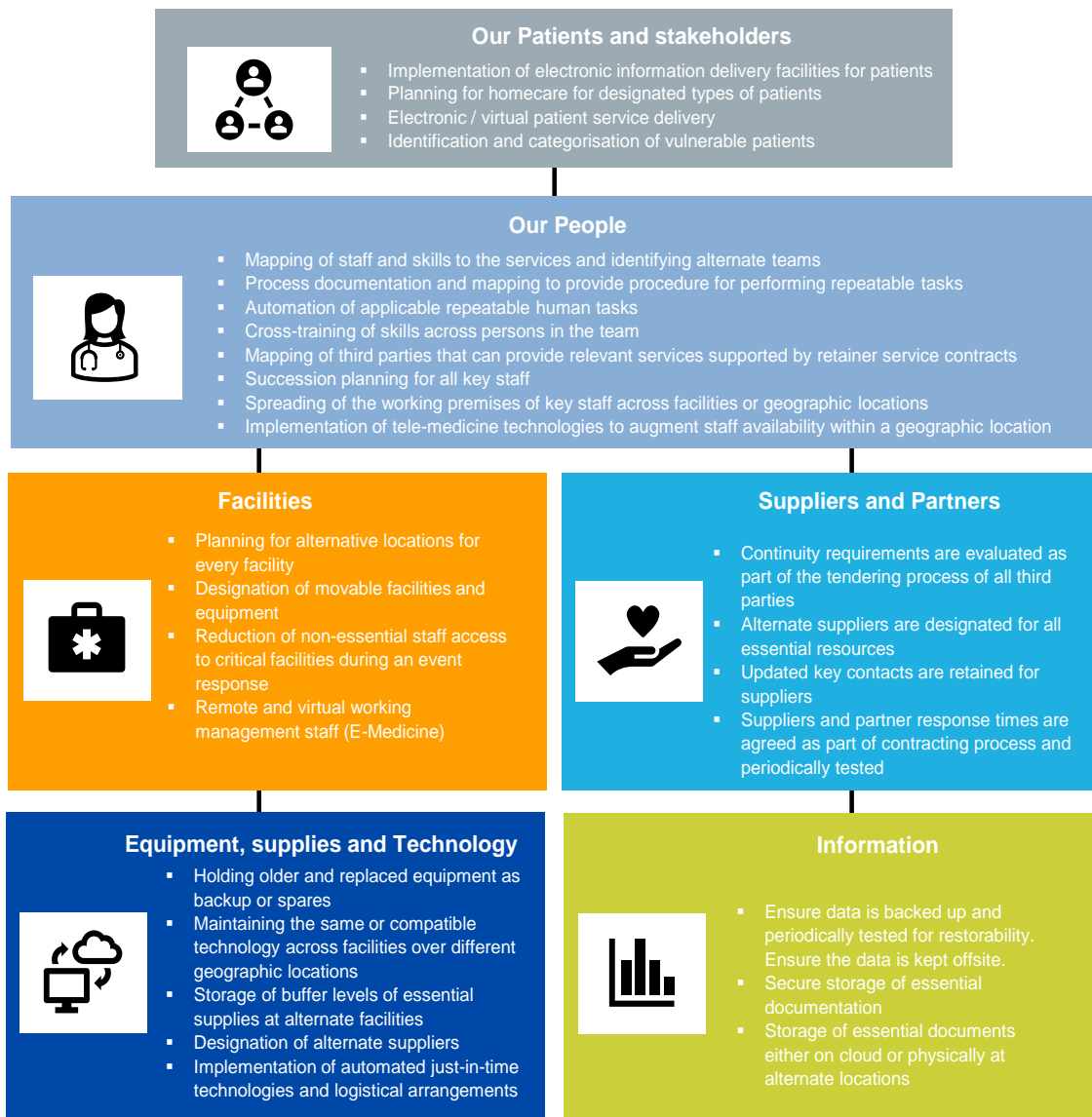


Figure 15: Strategies for reducing the impact of events

5.2 Document BCP

Within the HSE today there are many plans in place to deal with a range of possible adverse events and incidents. These plans include:

- Crisis Management Plans
- Crisis Communication Plans
- Emergency Management Plans (EMPs)

- Incident Management Response Plans
- Business Continuity Plans (BCPs)
- ICT Disaster Recovery Plans (DRPs)

For the avoidance of doubt, this handbook only covers a standardised approach to developing Business Continuity Plans (BCPs). BC Owners and BC Leaders will need to satisfy themselves that any other plans in existence today are current, aligned and integrated as needed when considering requirements for any new or updated BCP's for their area of responsibility. If any current BCP's could benefit from being updated and aligned with the new BCM Policy and Handbook guidance, this should be discussed and agreed with the BC Owner.

It is envisaged by the BCM Policy, that Managers within HSE National, Regional and Local levels will need to develop BCP's to support and lead the continuation of key health services, operations and activities in their areas of responsibility. In Section 3. Risk Assessment, we also noted that recovery and response strategies and plans (including action cards) may also be developed for high-impact threats and risks to the organisation.

The three levels are defined as follows for the purpose of this handbook:

- HSE Centre and National Services
- Regional – All Regional Health Areas (RHAs)
- Local – Any site / facility (e.g., any hospital or community care facility) deemed in scope by the BC Owners.

BCPs at a minimum must include:

- The purpose, scope, and objectives of the BCP
- The roles and responsibilities of the BCP team
- Details of the key recovery strategies for priority services/operations/activities
- Detailed plans for the implementation of each recovery strategy
- Supporting information for the activation, operation, coordination, and communication of recovery actions
- Internal and external interdependencies affecting the BCP
- The process for triggering and standing down the BCP
- The resources required to manage and execute the BCP
- The reporting requirements during and after a BCP event

Plans will only work when they are **well designed, accessible, up to date** and **practical to use**.

An example of a BCP template has been detailed in Appendix 2.

Managers must use appropriate documentation and recordkeeping processes to ensure the traceability and integrity of business continuity-related information. BC Plans and action cards should be accessible at all time, both online and in print.

5.3 Action cards

Action cards (sometimes referred to as battle cards) detail high level but practical steps that are planned for use by staff members in the event of a specific event. Action cards can be very useful as they provide rapid, step-by-step actions to follow should a certain type of event occur, e.g., a suspected cyber event in a site, a flooding incident, a power outage, a hostage situation etc.

Action cards should always be documented and printed (e.g., laminated in folders) in busy environments to aid staff with key prevention, containment, and response activities. By taking rapid and precise action when an event occurs, staff and Managers have the potential to significantly reduce the impact of the event on health and social care services and the wider community. Action cards and training associated with these cards are proven to be highly effective tools within an end-to-end BCM process.

A template for documenting **action cards** has been provided within the BCP Template in Appendix 2.

5.4 Communication

It is the expectation of the BCM Policy that Managers will be made responsible across the HSE and will document and communicate the approach to operate the BCM within their area or responsibility. It is encouraged that both digital and printed versions of the plans are made available and easily accessible for referencing in a disruption. It is also expected that a program of testing, training, lessons learned, and maintenance activities will be performed on a regular basis.

Plan Communication

BCP's must be made available to all relevant managers and staff in both hard and soft copy. Managers and staff should be informed of changes and updates to BCPs. Records of the storage locations of the BCP's should be retained including a change log as part of BCP control management processes.

In many hospital and social care settings certain BCPs and/or Action Cards should be readily available (e.g., printed in binders and in approved digital locations) in key locations to facilitate ease of access if needed. Managers and staff will need to be trained and made aware of the location of the plans on a regular basis.

Refer to the Appendix 2 for a sample of the storage and distribution log, which is provided as part of the BCP Template.

Periodic updates of BCPs can be communicated to staff through channels such as posters in the premises, email banners or electronic posters to ensure understanding of key areas.

Event Communication

A BC communication plan will be documented and kept updated as part of the BCP.

The communication plan will detail:

- Who to contact?
- When to contact the person / role?
- How to contact the person / role?
- What message to deliver?

A sample communication table has been documented in Appendix 2 as part of the BCP template.

5.5 Triggering a BCP

Response to key health service, operation or activity disruptions requires a coordinated, approved, and planned approach that identifies who has authority and is responsible for making key decisions, when they can make these decisions, and in what order they are required.

Every BCP should clearly set out the roles and responsibilities of those tasked with triggering and managing the plan during a disruptive event. A structured and well-defined triggering (sometimes referred to as 'invocation') approach helps ensure effective and timely response activities.

The decision process for triggering a BCP will typically include the following:

1. **Has a disruptive event occurred?** The BCM Policy defines an event as "anything that has the potential to disrupt normal service delivery"
2. **Can this event be handled by BAU in a reasonable period?** This decision should be made by the responsible Manager in consultation with the BC Leader depending on the situation.
3. **What is the potential of this event to significantly disrupt normal service delivery?** The responsible Managers, BC Leader and BC Support Staff should determine the likely impact of the event.

4. **Should the BCP be invoked?** Considering all known information, the BC Owner and BC Leader should determine whether BCP should be triggered (and which BC Plan should be triggered).

If the BCP is invoked the following steps need to be performed by the BC Leader or delegate:

- Communicate the triggering of the BCP in line with the agreed communication plan.
- Establish the agreed forums and clearly set out the situation and procedures that will govern operation of the BCP.
- Agree and perform periodic checkpoint reviews to confirm the status of the event and the response actions.
- Consider other responses such as Major Emergency (MEM) or Incident Management.
- Consider other forums such as National, Area and Local Crisis Management Groups.
- Document and maintain a log of actions and decisions made using the below event log (see example in Figure 16).

The event log below is populated with some examples of key actions and decisions that may be noted during the triggering of a BCP. Please note that this is non-exhaustive and for illustration purposes only.

Figure 16: Event Log example

Ref.	Date	Time	Details	Action / Decision	assigned to	Statue
001	01/01/23	11.00am	BCP Triggered	Decision to Trigger BCP actioned due to anticipated loss of service for >12 hours	BC Owner	Complete
002	01/01/23	11.01am	Hospital B contact	Contact Hospital B to arrange for patient transfers	BC Leader	Complete
003	01/01/23	11.01am	Initiate Crisis Comms	Initiate Crisis Comms Plan per the BCP	BC Leader	Underway
004	01/01/23	11.15am	Arrange Patient Transport	Contact ambulance service to arrange Patient Transport to Hospital B	BC Leader	Complete

Ref.	Date	Time	Details	Action / Decision	assigned to	Statue
005	01/01/23	12.00pm	Initiate Patient Transport	Patients to be moved to Hospital B to allow for services to be delivered at that location	Ambulance Service	Underway

If a checkpoint review identifies that services levels have been restored, declare the stand down or completion of the business continuity response activities, and revert to business as usual.

Managers should perform an After-Action-Review on a timely basis, reporting and formally identifying areas of improvement from the business continuity response (refer to the Act Section for further detail).

6. Training, Testing & Exercising

6.1 Training

ISO 22301 highlights the need for establishing, implementing, and maintaining processes to ensure that personnel are aware of their roles and responsibilities during incidents and are trained to perform these roles effectively. This includes preparing and conducting training programs and exercises to enhance personnel's awareness, skills, and readiness for potential disruptions.

Training is an important activity to drive cultural awareness, support and knowledge of the importance of BCM within the HSE. Training also enables leadership to ensure that Managers and staff are competent to perform the roles and responsibilities required of them within BCM processes.

BC Leaders should consider the following guidance when implementing training in their area of responsibility:

- Training and awareness plans should be targeted and developed based on the unique needs of identified Managers and staff. Training and awareness programmes should be designed to support Managers and staff in the competent performance of their roles and responsibilities within the BCM processes.
- Specific technical training programmes, e.g., eLearning or classroom based, will be required for assigned BC roles (BC Owners, BC Leaders and BC Support Staff). The use of external parties to provide training and certification/qualification services should be considered. Other stakeholders should be considered as appropriate, e.g., external agencies, key partners, key suppliers.
- Leadership within the function or area should actively support and be involved in training initiatives where appropriate. BC Owners may be the appropriate leaders in this context.
- Regular training maintenance activities should be undertaken to ensure the BCM remains designed and operating effectively.
- BCP exercise, drills and simulations should be considered as additional formats to the formal training programme of Managers and staff allowing them to practice risk management, response and recovery procedures.
- Training programmes should be documented and formally evaluated. The measurement of the effectiveness of the training could be through assessments, tests, or feedback from participants to ensure that training objectives are being met.

- Training evaluations and learning from past training events should be applied in improving subsequent training events.

Types of training that may be appropriate for establishing, managing, and maintaining the BCM processes are as follows:

- Understanding your BCM roles and responsibilities
- Setting up and managing BCM processes
- Conducting a business impact analysis
- Conducting a threat and risk assessment
- Developing and implementing business continuity strategies and plans
- Maintaining documentation
- Preparing for and running a BCP test exercise programme
- Conducting after action reviews and continuous improvements
- Communication skills
- Project management

The BC Leader should develop and implement an annual training and awareness plan of activities using the suggested template below. The training plan and activities will be reviewed as part of the performance evaluation and continuous improvement process.

Examples are provided below on what could be in a training plan, this list is non-exhaustive and is for illustration purposes only.

Figure 17: Training Plan Example

Date	Training Type/Name	Training Objective	Involved stakeholders / Focus Group
01.12.23	Intro to BCM	<p>Purpose: To introduce employees to the concept of business continuity, its importance, and their roles in maintaining continuity during disruptions.</p> <p>Content: Overview of BCM, organisational BCM policy, basic principles, and general response procedures.</p>	<p>BC Leaders</p> <p>BC Support Staff</p> <p>Staff with a role in BCP</p>
01.03.24	Incident Response/BCP Training	<p>Purpose: To educate staff on how to respond effectively during different types of BCP incidents and disruptions.</p> <p>Content: BCP/incident response strategies, plans, communication</p>	<p>BC Leaders</p> <p>BC Support Staff</p>

Date	Training Type/Name	Training Objective	Involved stakeholders / Focus Group
		protocols, immediate actions, and coordination procedures.	Staff with a role in BCP
01.06.24	Exercising Training	<p>Purpose: To instruct individuals on how to plan, conduct, and evaluate tests, drills, and exercises to validate the effectiveness of the BCP.</p> <p>Content: Designing scenarios, conducting tabletop exercises, evaluating outcomes, and implementing improvements based on exercise results.</p>	<p>BC Leaders</p> <p>BC Support Staff</p> <p>Head of IT</p> <p>Emergency Service Lead</p>
01.07.24	Crisis Communication Training	<p>Purpose: To equip individuals with effective communication skills during crises and to manage stakeholder communications.</p> <p>Content: Crisis communication strategies, media handling, stakeholder engagement, and messaging during disruptive events.</p>	<p>BC Owner</p> <p>BC Leader</p> <p>Hospital CEO</p> <p>Hospital Comms team</p>

Training delivery options may include:

- Professional training and certifications – The BC Owner/Leader may approve the use of professional training institutions to improve the capability of key Managers and staff within the BCM team.
- External facilitator led classroom training – The BC Owner/Leader may consider the engagement of a third-party training organisation to conduct workshop-based training sessions for identified staff groups.
- Internally led trainings – The BC Owner/Leader may consider the selection and delivery of train-the-trainer courses for identified staff. These trained facilitators will take up the role of conducting classroom-based workshops and training sessions for groups of staff and stakeholders.
- Self-driven training sessions – The BC Owner/Leader may consider the provision of electronic training facilitates (e-learning) to support self-training by staff.

6.2 Embedding BCM In Business As Usual (BAU)

Embedding BCM processes in the HSE requires executive sponsorship, strong leadership and an ongoing commitment to several areas including ongoing training, test exercises, regular awareness and communications programmes.

BC Owners should seek to embed a culture of business continuity awareness into business-as-usual activities through awareness campaigns targeted at relevant Managers, staff and key stakeholders.

Awareness campaigns or processes may include the following techniques:

- Communication of BCM procedures via posters, emails, and other internal channels.
- BCM capability and skills in relation to recruitment and selection of relevant roles
- Discussing BCM in staff workshops, journals, newsletters, and briefings (especially Health and Safety briefings)
- Inclusion of BCM materials on relevant intranets and digital platforms
- Involvement of BCM as a topic in BAU staff and management team meetings
- Visits to designated alternative locations (e.g., a recovery site)
- Regular communication with key suppliers to ensure they understand HSE's business continuity requirements

6.3 Testing the BCP

Validating our strategies and plans:

Validating continuity strategies and plans is a critical process aligned with ISO 22301's principles. It involves subjecting developed business continuity plans to rigorous testing and assessment. By simulating real-world disruptions and executing these plans, we can gauge their effectiveness, identify gaps, learn, and refine our strategies and plans to be more effective and meaningful in a real-life disruption.

Validation encompasses various techniques, from tabletop exercises to full-scale simulations, each designed to uncover vulnerabilities and enhance response capabilities.

This process not only fosters confidence among stakeholders but also ensures that the plans are adaptable and aligned with evolving risks. Through validation, we gain insights that empower Managers to make informed decisions, fine-tune responses and put in place additional mitigations that may prevent or minimise the impacts of disruptive events.

Effective testing and exercising are used to assess and identify gaps in BCM processes, including BCPs, and highlight areas for improvement. A testing and exercising programme will also provide training to staff and can help improve

management decision making during an incident. The ongoing viability of BCM processes can only be determined through continuous tests and improvements.

In accordance with the Policy, a cycle of exercising will be introduced, BC Leaders will be required to hold desk-based functional continuity related exercises **annually**, with larger full-scale drills/exercises to be performed every **three years**.

BC Leaders are responsible for preparing for and conducting testing and exercising, utilising the guidance provided in this policy and associated handbook. Effective testing and exercising will include the following:

- Securing an appropriate budget to operate an effective test programme.
- Development and maintenance of test plans for each BCP in the Managers area of responsibility.
- Appropriate, well-planned tests and exercises based on appropriate scenarios with clearly defined aims and objectives.
- Involvement of all relevant staff and stakeholders who have a part to play in testing the effective recovery of services.
- Consideration of all key dependencies to the success of the test plan.
- Formalised post-exercise reporting with outcomes, recommendations, and actions to implement improvements.

Outlined below are examples of testing Managers should consider:

- Talk-through – A workshop driven scenario-based simulation focused on exploring the understanding of key stakeholders on their roles and responsibilities in the BCP.
- Walkthrough – A walkthrough of the business continuity plan and related documentation without active simulation or a full-scale exercise.
- Functional/Service testing – Conducting simulations based on specific function or service continuity scenarios in a controlled environment focused on exploring the effectiveness of a section of the BCP. This may include for example, simulating a test of the continuity and recovery of a key patient service, operational area or key activity based on the simulated loss of a key resource e.g., Staff, ICT, Equipment, Supplies, Estate.
- Full scale exercise – A comprehensive test of a complete business continuity event or scenario involving several functions or teams and external stakeholders. This is focused on assessing the function's overall readiness for a significant disruptive event and should be conducted at least once every 3 years.

BC Leaders may consider the involvement of external stakeholders, suppliers, emergency service providers and other related parties as necessary for the effective execution of the any test or exercise based on the requirements of the BCP's.

Figure 18 - Test Plan Template

The table below will be used to document a testing plan. This example outlines a Talk-through style test following the scenario of a fire in the kitchen of a hospital. This is for example purposes only and test scenarios should be developed that are relevant to the area you are responsible for.

<FUNCTION/SERVICE> TEST PLAN FOR A BCP EXERCISE

PLANNED TEST DATE: 20/02/20XX

COMPLETED BY: BC Leader

APPROVED BY: BC Owner

COORDINATOR: BC Leader

INTERNAL STAKEHOLDERS: Kitchen staff, Ward Manager, Nurse Manager, Hospital Manager, Head of Patient Safety, Head of Health and Safety, Head of Communications, Fire Warden

EXTERNAL STAKEHOLDERS: Fire Service, Food Supplier

ROLES AND RESPONSIBILITIES –

Incident Leader: [BC Leader]

Communication Lead: [Head of Comms]

Staff: [As per their designated roles in the BCP.]

Test Objectives and Scope:

- Validate the organisation's response procedures, communication strategies, and recovery processes outlined in the BCP.
- Assess the effectiveness of coordination, roles, and responsibilities among designated teams and personnel.
- Identify strengths and weaknesses in the BCP to drive continuous improvement and enhance overall resilience.

Test Type Talk-through

Test Scenario: Response to a fire in the kitchen of a hospital disrupting operations and threatening patient and employee safety.

Required Resources:

White board

Meeting room

PC/Laptop for notes

Communication Plan:

Communication plan should be followed as outlined in the BCP

Test Script / Schedule:

Test time – 90mins

Debriefing time – 30mins

Introduce participants to the existing BCP

Initial Notification and Activation – Notify Response team of fire incident and activate the BCP

Assessment and Situation Analysis - Conduct an initial assessment of the incident's impact on patients, staff, facility, and critical operations. Determine the severity of the fire and potential harm to individuals.

Communication - Activate the emergency communication system to alert all staff about the fire incident.

Patient and Staff safety - Simulate evacuation of patients and staff following predetermined routes to safe assembly areas.

Assess Damage to Kitchen area

Recovery Site Set up - Establish recovery site to allow lost services to resume partial/full operations. This action may also involve activating an alternative site to resume operations.

Communication and Media - Communicate the incident response and recovery status to patients, staff, stakeholders, and the media as per the communication plan.

Evaluation and Lessons Learned - Conduct a debriefing session with key stakeholders to evaluate the response, identify areas for improvement, and capture lessons learned.

Document the test results, observations, and recommendations for further refinement of the BCP.

A report of key activities performed, results and lessons learned must be completed for each test, and shared across the network of BC Leaders and BC Owners within the health system. Notable actions from the test will be incorporated into the planning of any subsequent review of the plan and supporting activities. Further details on completing this are provided below in the “Act” [Section 8.2 Post Exercise Reporting](#).

6.4 Interagency Engagement

The Regional Emergency Management teams are in place to ensure the effective coordination of collaboration with other Principal Response Agencies (PRAs). During planning and exercising, BC Leaders should consult the Emergency Management Team to ensure efficient collaboration with these groups. BC Leaders should ensure that they are communicating regularly with these teams and associated governance structures as and when required, especially during events and training/testing.

7. Management Reviews

Checking the effectiveness of the plans

Monitoring and reviewing BCM processes are a cornerstone of effective resilience, in accordance with ISO 22301 principles. Managers can only test and re-check BC strategies and plans. They cannot have definite certainty that plans will work but they can be reasonably assured they may work through training, test exercises and lessons learned from previous occurrences.

This ongoing process of monitoring and review involves systematically assessing the BCM performance in each area to ensure it remains aligned with objectives and continuously improves. Regular monitoring detects deviations from established plans, while reviews dive deeper to evaluate the BCM effectiveness in real-world scenarios.

By analysing data, gathering feedback, and measuring outcomes, Managers can identify areas for enhancement, gauge the system's responsiveness, and ensure that it evolves alongside an ever-changing threat and risk environment. Monitoring and reviewing BCM processes are not just a requirement; it's a proactive strategy that fosters adaptive preparedness, enabling Managers to navigate disruptions with more confidence.

Monitoring and reviewing are integral components of robust BCM processes aligning with the guidance set out in ISO 22301. The process of monitoring involves a systematic observation of the BCM activity's performance, ensuring that it remains aligned with established objectives and strategies.

BC Leaders should undertake regular reviews of plans, to identify opportunities for improvement and to verify compliance with the BCM policy. The review should include:

- Conformance with defined KPIs (Key Performance Indicators).
- Status of actions and outcomes from any recent review.
- Action logs/assumptions in relation to BIA are being addressed and managed.
- Updates on identified lessons learned from activation of BCP's or from test and training exercising.
- Consideration of changes to the internal or external environment that may affect BC materials.
- Identification of trends from reviews.
- Update of BCPs and other BCM process documentation following the review.

On an annual basis, the BC Owner with the support of the BC Leader/Support Staff should perform, certify, and file a self-assessment of their achievement of the objectives of BCM using a template like the one detailed below:

Figure 19: Self-Assessment Template

FUNCTION/SERVICE			
ASSESSMENT PERIOD			
OVERALL COMPLIANCE RATING (C/P/N)			
PLAN			
Ref	Objective	Compliance (Compliant / Partial / Not)	Comment / Action plan
1	A Business Continuity Policy is available documenting the purpose, context, scope, and governance requirements.		
2	The policy been reviewed and updated in line with policy requirements.		
3	The policy is supported, approved, and owned by senior management with effective governance, leadership and resourcing.		
4	The scope of the BCM covers the identified key services and business support components.		
5	A team has been established to oversee and manage the BCM within the function/area and an approved charter detailing the key roles and responsibilities is in place.		
6	BCM status and key actions are proactively discussed and tracked at Senior Leadership team meetings.		
7	BCM is discussed and supported as part of periodic staff briefings.		
DO			
Ref	Objective	Compliance (Full / Partial / Not)	Comment
8	A detailed threat and risk assessment has been formally performed (Risk Assessment Templates).		
9	The impact of threats and risks has been formally assessed across the service/operation/activity area? (BIA Templates)		
10	The Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) are documented, where applicable. (BIA Templates)		
11	Planned strategic responses, actions and assumptions have been developed for each prioritised area emerging from the BIA (Strategic Plan Templates).		
12	A budget has been approved to support the implementation of the strategic actions and assumptions that covers all the required activities.		

13	BCP's (including action cards) have been developed and approved to address the key strategic response areas.		
14	BCP's include requirements for training and awareness		
15	Training programmes have been developed based on an approved training plan.		
16	All the approved training has been scheduled and held for key Managers and staff.		
17	Learnings from training evaluations are conducted and included in corrective actions log.		
18	BCP's includes requirements for periodic testing and validation of the plans.		
19	Test exercise programmes have been developed based on an approved test plan.		
20	All the approved test activities have been scheduled and completed as planned.		
21	Test exercise results are formally documented and reported to the appropriate governance forums.		
22	Learning sessions from test exercises are conducted and included in a corrective action plan.		
23	Corrective action plans relating to test exercises are tracked and reflected in updated BCP's and processes.		

CHECK

Ref	Objective	Compliance (Full / Partial / Not)	Comment
24	Self-assessment reports are completed within the agreed period (bi-annually).		
25	Internal audit or external reviews are performed within the timeframes agreed with management.		
26	Managers fully cooperate and engage in any reviews or audits of BCM processes in their area.		
27	Internal audits or any other review reports covering BCM are agreed, and the findings and recommendations are included in a corrective action plan.		
28	Corrective action plans related to audits or reviews are tracked and reflected in updated BCP's and processes.		



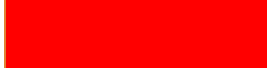
ACT

Ref	Objective	Compliance (Full / Partial / Not)	Comment
29	Action owners and actions dates have been documented in consolidated corrective actions log and are managed to completion by the BC Owners and BC Leaders.		
30	Learnings from all prior business continuity tests, audits and reviews have been verified as incorporated into updates to the BC plans.		

31	What is in 30 has been shared across the system		
----	---	--	--

The assessment of BCM compliance is defined as follows:

Figure 20: Compliance Rating

Rating	Definition	Colour
Compliant	The function/area is materially compliant in achieving most of the key objectives, with some partial compliance objectives noted.	
Partially compliant	The function/area is mostly partially compliant in meeting all the key objectives.	
Not compliant	The function/area does not meet most of objectives described in the self-assessment.	

7.1 KPIs

Effective monitoring and ongoing review of BCM requires clearly identified benchmarks or key performance indicators which will act as a guide for Managers. These key performance indicators should be objective based and aligned with the requirements of the HSE.

KPIs provide a clear and measurable way to monitor the performance of BCM activities, demonstrating alignment with corporate goals, identifying areas for improvement, and highlighting a commitment to improve resilience to key stakeholders.

The CEO will define KPIs that will guide the evaluation of its BCM activities and provide guardrails for its improvement.

Figure 21: KPIs

Ref	KPI / Objective	Metric	Information Source / Evidence
1	Adequate leadership and resourcing	<ul style="list-style-type: none"> ▪ Leadership for the BCM has been clearly defined and communicated in a charter, the plan or job details. ▪ The BC Owner demonstrates ownership and commitment to staff through periodic communication about the relevance of the BCM. ▪ Accountable roles and responsibilities have been assigned and are monitored as detailed in the BCP. ▪ An annual budget has been developed for BCM activities 	BCP
2	Adequately developed business continuity plan	<ul style="list-style-type: none"> ▪ An approved BCP is in place. ▪ The plan has identified and assessed all the key services in the function or service area. ▪ Response plans and Action Cards have been developed for the identified events. ▪ Contact details in the plan are up to date 	BCP

Ref	KPI / Objective	Metric	Information Source / Evidence
3	Adequately tested business continuity plan	<ul style="list-style-type: none"> Testing has been conducted and documented within the last 12 months. Full scope testing has been performed within the last 36 months 	BCP Test Plan BCP Test Reports
4	Adequate communication and stakeholder engagement is performed	<ul style="list-style-type: none"> BCP has been made accessible to staff and relevant stakeholders. BCP materials are accessible offsite or in an immutably accessible digital format. Periodic BCM training and awareness is provide to Managers and staff. A BCM communications plan is in place. 	
5	Plan Maintenance and Review	<ul style="list-style-type: none"> Business continuity plan has been reviewed and updated within the past 12 months. Learnings from BCP Test Reports, Audits, Reviews and Incident Logs have been incorporated into updated BCP's 	BCP Document History Log BCP Test Reports AAR Reports

7.2 Assurance

The HSE will seek to obtain assurance that the BCM policy is being complied with. This could take the form of Internal Audit or other forms of independent reviews. These reviews will be performed to evaluate the effectiveness and adherence of the function to the BCM policy, and this associated handbook.

Findings and recommendations will be documented and shared with relevant Managers for corrective action and continuous improvement and tracked for resolution. These could be tracked by the BC Leader in the Corrective Action log outlined below in the Act Section ([Figure 24 - Corrective Actions Log](#)).

Assurance can be provided by an **external body or** through the **internal audit function**.

8. Learning and Improvement

Improving and maintaining our plans

ISO22301 notes the importance of continually monitoring, measuring, analysing, and evaluating the performance and effectiveness of the BCM processes to identify opportunities for improvement.

By consistently updating plans to address emerging risks, incorporating, and sharing lessons learned from test exercises and real-life incidents/events, and staying abreast of best practices, we can further strengthen HSE resilience over time.

Through this dedicated focus on maintenance and improvement, Managers across the HSE can not only safeguard key patient and service user services and operations but also foster a culture of continuous enhancement to overcome new resilience related challenges.

Following the activation of plans or tests/exercises, BC Leaders must appraise all aspects of the response. This appraisal should:

- Capture best practice and identify opportunities for continual improvement.
- Capture outcomes and lessons learned.
- Be conducted in an open and honest and constructive manner.
- Be formally documented in a post incident/exercise report.
- Be shared with network of BC Leaders
- Be shared with stakeholders/BCP participants.

Significant changes to internal and external structures must prompt a review of the whole or part of the policy and plans.

8.1 Post Event Reporting

Post event reporting is the process of documenting and analysing the organisation's response and recovery efforts following a disruptive event or crisis, when the BCP has been triggered. It involves capturing information about what occurred, the actions taken, the outcomes, lessons learned, and areas for improvement.

Post event reporting helps continuous learning, future planning and supports accountability, and ensures that the BCM program evolves based on real-world experiences to enhance resilience.

After the restoration of BAU after a business continuity event, the function will perform an After-Action Review (AAR) workshop with key stakeholders. It focuses on identifying unexpected events both positive and negative, exploring the reasons of its occurrence, and learning what can be avoided or aimed for in the future.

It is recommended that the facilitation of the workshop is conducted by an experienced individual and may be conducted either in-person, hybrid or virtually. This session aims at creating a comfortable and open atmosphere for everyone to freely share their views and experience.

During the AAR, the team should complete the below assessment form. This has been completed using the example of a Cyber Attack on a Payroll system for illustrative purposes only.

Figure 22 - AAR Assessment Form

INCIDENT – Cyber Attack on Payroll system

INCIDENT DATE: 29/09/20XX
REPORT DATE: 31/09/20XX
COMPLETED BY: BC Leader
APPROVED BY: BC Owner

FACILITATOR: BC Leader

ATTENDEES: Head of IT, Head of Payroll, Hospital Manager, BC Co-Ordinator, Senior IT Manger

Summary of the incident: An attacker infiltrated our network through a phishing email. The attacker deployed ransomware to encrypt files and systems associated with the payroll process and render the payroll data and systems inaccessible to the organisation.

Question	Response
What occurred?	In a ransomware cyberattack on the payroll system, an attacker infiltrated our network through a phishing email. The attacker deployed ransomware to encrypt files and systems associated with the payroll process and render the payroll data and systems inaccessible to the organisation.
What was the timeline over which this occurred? What was the continuity response planned for such as event?	9.05am – Cyber Attack detected 11.30am – Payroll BCP Invoked by BC Owner/Leader 12.30pm – Activated BCP Team Engaged SMEs (internal & external cyber support), Isolated Affected System Notified Key Stakeholders Activated our payroll secondary site Assessed business impacts Reported incident to Exec & relevant authorities Restored payroll systems and date from back ups to secondary site

<p>What was the actual response by the function?</p>	<p>The BCP was activated by the Head of Payroll and the affected system was isolated. The team moved to a 3rd party secondary site where access was provided for key staff to do their role. SMEs were engaged to assess the damage and impact and support on next steps.</p> <p>Payroll was run from the prior month detail using encrypted memory sticks to the bank files.</p> <p>The attack was reported to Authorities.</p> <p>Etc..</p>
<p>Why there was a difference between planned and actual (if any)?</p>	<p>As responding to the incident was priority, key stakeholders were not informed in a timely manner and per the communications policy. In addition, the news was leaked to social media in advance of official comms.</p> <p>The secondary site was not ready on time as the 3rd party was not contacted in a timely manner as the contact details in the BCP were out of date.</p> <p>The payroll had to be run from last month's payroll, not accounting for shift work, as RPO was incorrectly documented in BCP Plan.</p> <p>Etc..</p>
<p>What was the impact on Staff/Patient Safety?</p>	<p>N/A</p>
<p>What was the financial impact of the response?</p>	<p>150k</p>
<p>What were the individual roles in the response process?</p>	<p>Incident Response Lead – Head of Payroll Incident Co-Ordinator – Senior Payroll Manager System Administrator – Senior IT Manager Malware Analyst – Cybersecurity Manager 3rd Party Vendor Liaison – Senior Payroll Manager</p>
<p>What variations were noted in the roles and responsibilities?</p>	<p>Head of IT was out sick so Senior IT Manager had to perform the systems role</p>
<p>What learnings were noted from the event (positive and negative)?</p>	<p>Positive:</p> <p>Documented BCP provided an organised response.</p> <p>Recent testing of payroll outage proved vital in timely response.</p> <p>Clearly defined roles and responsibilities allowed for clear leadership of crisis.</p> <p>Secondary site had the required technology to run payroll.</p> <p>Negative:</p> <p>As responding to the incident was priority, key stakeholders were not informed in a timely manner and per the communications policy. In addition, the news was leaked to social media in advance of official comms.</p> <p>The secondary site was not ready on time as the 3rd party was not contacted in a timely manner as the contact details in the BCP were out of date.</p>

	The payroll had to be run from last month's payroll, not accounting for shift work, as RPO was incorrectly documented in BCP Plan
What follow up actions will be taken on these learnings?	<p>Action: Crisis Comms training to be organised for all staff listed in the BCP: Owner: BC Leader</p> <p>Action: Contact details in BCP for 3rd Parties to be updated Owner: BC Co-ordination</p> <p>Action: Update RPO in BCP with agreement between IT and Payroll: Owner: Head of IT</p>

8.2 Post exercise reporting

Post exercise reporting involves documenting the outcomes, observations, and lessons learned from conducting a simulation or exercise of the organisation's response and recovery plans.

Post exercise reporting helps validate the effectiveness of the plans, enhances team coordination and communication, provides a basis for refining response strategies, and ensures that the HSE is better prepared to manage actual disruptions in the future.

After the testing is performed, the function should document a detailed report of the activities and continuous improvement actions.

Outlined below is an example Lessons Learned Report which has been completed for possible lessons learned through the "Fire in the kitchen Talk-through" exercise outlined in the example above in the Check Section.

Figure 23 - Lessons Learned Report

Exercise Date and Name	Key Activities	Lessons Learned	Actions Required and Owner
20/02/2024 Talk-through exercise of a kitchen fire	<p>Introduce participants to the existing BCP</p> <p>Initial Notification and Activation</p> <p>Assessment and Situation Analysis</p> <p>Communication to staff and patients</p> <p>Patient and Staff safety -</p>	<p>Early Detection and Alarm Systems are Critical: The effectiveness and early activation of fire detection and alarm systems are essential in promptly notifying staff about a fire, allowing for quicker response and evacuation.</p> <p>Effective Use of Fire Suppression Equipment: Familiarity with the location and proper use of fire extinguishers and other fire suppression equipment can mitigate a fire's initial spread and severity, limiting damage and potential injuries.</p>	<p>Action 001 – Update Contact Details in BCP Owner – BC Support Staff</p> <p>Action 002 – Schedule Test of Fire Detection and alarm systems within 30 days Owner – Head of Facilities</p> <p>Action 003 – Schedule Fire Suppression Equipment Training for Kitchen Staff within 60 days Owner – Hospital Manager</p> <p>Action 004 – Review Evacuation Plan with local</p>

Exercise Date and Name	Key Activities	Lessons Learned	Actions Required and Owner
	Assess Damage to Kitchen area	<p>Criticality of a Well-Defined Evacuation Plan: A well-established evacuation plan with clear routes, assembly areas, and assigned responsibilities during an evacuation is essential for a quick and organized exit from the affected area.</p> <p>Role Clarity and Leadership: Clearly defined roles and responsibilities ensure efficient decision-making and coordination, reducing confusion and promoting effective response efforts.</p> <p>Emergency Contact and Communication List Accuracy: Regularly updating and validating emergency contact information for staff, stakeholders, and emergency services is essential to ensure accurate and timely communication during a crisis.</p> <p>Review and Update of Business Continuity Plan: Conducting desktop exercises highlights areas of improvement within the BCP. Regular reviews and updates of the plan based on lessons learned from exercises ensure its relevance and effectiveness.</p>	<p>Fire Service and other SMEs within 60 days</p> <p>Owner – Hospital Manager</p>
	Recovery Site Set up		
	Communication and Media		
	Evaluation and Lessons Learned		

8.3 Corrective Actions

Corrective actions refer to steps taken to address identified weaknesses, deficiencies, or gaps in the organisation's business continuity process.

Corrective actions help avoid reoccurrence of the same issue and facilitate continuous improvement.

Post-event and post-exercise reports may identify areas of improvement or corrective actions that need to be implemented for an effective BCM process.

These learnings or corrective actions will be documented in a BCM activities log or corrective actions log or plan. This will form a vital agenda item for the function BCM team's meetings and will detail at a minimum:

- Observation - What was identified?
- Source of item – Identify whether the item arose from results of testing, an event, an audit, or a self-assessment?
- Root cause of item – What is the root cause of the item in the log?
- Action item or activity – What corrective actions have been mapped to the item?
- Responsible person – Who is responsible for the resolution of the corrective actions?
- Target date – By which date should the item have been resolved?
- Resolution date – When was the item resolved?
- Status – What is the status during each review?

It is recommended that entries in the log are retained after resolution.

The below Corrective Action Log shows examples that are taken from the [AAR](#) and the [Exercise Lessons Learned Activities](#) carried out below. It also includes examples of Internal Audit Findings. All actions from all sources should be noted in this log and tracked for resolution.

Figure 24 - Corrective Actions Log

Ref.	Observation	Source	Root Cause	Action item	Responsible	Target Date	Resolution Date	Status
001	Contact details in BCP not up to date	Kitchen Fire Exercise	Change of Staff in last year	Update Contact Details in BCP	Owner – BC Co-Ordinator	20.03.24	17.03.24	Complete
002	Fire Systems need testing	Kitchen Fire Exercise	Annual test schedule	Schedule Test of Fire Detection and alarm systems	Head of Facilities	20.03.24	15.03.23	Complete
003	Staff not adequately trained on use of fire suppression equipment	Kitchen Fire Exercise	Change of staff in last year	Schedule Fire Suppression Equipment Training for Kitchen	Hospital Manager	2004.22	TBC	Underway

Ref.	Observation	Source	Root Cause	Action item	Responsible	Target Date	Resolution Date	Status
004	Evacuation route not up to date	Kitchen Fire Exercise	Car park construction underway	Review Evacuation Plan with local Fire Service and other SMEs	Hospital Manager	20.04.24	TBC	Underway
005	RTO and RPOs not agreed with key staff	IT Internal Audit / Cyber Attack	Change of staff	Review RTOs and RPOs with key staff	Head of IT	30.06.24	TBC	Underway
006	Insufficient Vendor Contingency Planning	IT Internal Audit/Cyber Attack event	Procurement of IT contractors completed before BCP	Review vendor BCPs and update contracts	Head of IT	30.06.24	TBC	Underway
007	Crisis Comms Training	Cyber Attack Event	Crisis Comms roles and processes not explained to relevant staff	Crisis Comms training to be organized for all staff listed in the BCP	BC Leader	30.10.24	TBC	Underway
008	3 rd Party contacts not up to date	Cyber Attack Event	Changes in 3 rd parties not reflected in BCP	Contact details in BCP for 3 rd Parties to be updated	BC Co-ordinator	30.10.24	TBC	Underway

8.4 Plan Review and Update

Plan reviews are the systematic evaluation and assessment of the HSE's business continuity plans to ensure their accuracy, relevance, effectiveness, and alignment with changing circumstances.

Plan reviews ensure that the plans remain up to date, comprehensive, and capable of guiding the organisation through disruptions.

- Cyclical reviews – BCPs should be reviewed by the BC Leader on an annual basis. These reviews shall involve a comprehensive re-assessment of the risks, business impacts and strategies that the function/area has planned. Plans should be updated post this re-assessment as required.
- Out of cycle reviews – The BC Leader should consider a review and update of the BCP if any of the following arise:

- New risks that could potentially disrupt services
- A significant increase in the likelihood or magnitude of an identified risk
- Significant changes in the staff supporting BCM activities
- Significant changes in environmental factors – Regulatory changes, supplier changes, etc.
- Changes in key services being provided by the function/area
- Significant ICT implementation or changes

Confirmation to the BC Owner of amendments, updates, and changes to the BCPs.

Reviews of the BCM Policy will be performed every **3 years** in line with the HSE, Policy of development of Policies, Procedures, and Guidance. Learnings from the triggering of plans and exercises should be considered to ensure that continuous improvements are integrated in the updated versions.

Appendix 1 - Template Checklist

SECTION	TEMPLATE	REFERENCE								
PLAN	Stakeholder Analysis	Figure 1								
	Categories of risk by impact and reference to policy/framework	Figure 2								
	Service Mapping	Figure 3								
	Roles and Responsibilities	Figure 4								
DO	Common Causes & Impacts of disruption	Figure 5								
	Likelihood Scores	Figure 6								
	Risk Scores	Figure 7								
	Risk Rating	Figure 8								
	Priority Rankings Table	<p>Disruption impact and recovery objectives</p> <table border="1"> <thead> <tr> <th>Priority 1</th> <th>Priority 2</th> <th>Priority 3</th> </tr> </thead> <tbody> <tr> <td>0 – 24 Hours</td> <td>> 24 hours</td> <td>>7 days</td> </tr> <tr> <td>Services, operations, or activities that cannot tolerate any disruption beyond the maximum of 1 day. If activities are not resumed immediately it may result in significant negative impacts on patient or service users, our</td> <td>Services, operations or activities which can tolerate a very short period of disruption and must be resumed within 24 hours to a maximum week before a failure to return to BAU starts to materially compromise health and</td> <td>Services, operations, or activities that can be delayed for more than a week given our Priority 1 and 2 objectives. They can tolerate a >7 days disruption before a failure to return to BAU starts to materially compromise health and</td> </tr> </tbody> </table>	Priority 1	Priority 2	Priority 3	0 – 24 Hours	> 24 hours	>7 days	Services, operations, or activities that cannot tolerate any disruption beyond the maximum of 1 day. If activities are not resumed immediately it may result in significant negative impacts on patient or service users, our	Services, operations or activities which can tolerate a very short period of disruption and must be resumed within 24 hours to a maximum week before a failure to return to BAU starts to materially compromise health and
Priority 1	Priority 2	Priority 3								
0 – 24 Hours	> 24 hours	>7 days								
Services, operations, or activities that cannot tolerate any disruption beyond the maximum of 1 day. If activities are not resumed immediately it may result in significant negative impacts on patient or service users, our	Services, operations or activities which can tolerate a very short period of disruption and must be resumed within 24 hours to a maximum week before a failure to return to BAU starts to materially compromise health and	Services, operations, or activities that can be delayed for more than a week given our Priority 1 and 2 objectives. They can tolerate a >7 days disruption before a failure to return to BAU starts to materially compromise health and								

		<p>staff and/or other HSE services.</p> <p>Priority 1 items may need a high-level BC Strategy and a detailed BC Plan. This will be agreed between the BC Owner and BC Leader.</p>	<p>social care services.</p> <p>Priority 2 items may need a high-level BC Strategy and a Plan on an exception basis. This will be agreed between the BC Owner and BC Leader.</p>	<p>social care services.</p> <p>Priority 3 items may need a high-level BC Strategy but unlikely to need a BC Plan. This will be agreed between the BC Owner and BC Leader.</p>
		Figure 9		
	Business Impact Assessment	Figure 10		
	Key Principles for Continuity Strategies	Figure 12		
	Recovery Strategy	Figure 13		
	Strategies for reducing the impact of events	Figure 15		
	Event Log	Figure 16		
	Training Plan	Figure 17		
	Test Plan Template	Figure 18		
CHECK	Self-assessment for BCM			
	Compliance Rating			
	KPIs			
ACT	AAR Report	Figure 22		
	Post Exercise Report	Figure 23		
	Corrective Actions Log	Figure 24		

Appendix 2 – Business Continuity Plan Template

1. Document history

Provide version history details of the document

Date of issue	Version Number	Nature of Change	Author	Reviewer

2. Distribution and retention details

Provide all person / roles to whom changes to the document need to be communicated to. Additionally provide details of the various locations where the document will be stored for referencing.

Name	Title / Role

Storage and communication

Location	Format (Physical / Electronic)

3. Approval details

Provide all details of approval obtained for the document

Name	Position	Signature	Date

4. Scope statement

Provide details of the scope statement of the BCP based on the guidance of [Section 1.5 - Scoping the BCM](#).

5. Understanding of the context, services, teams, reporting structure / organisational chart, facilities, collaborations / partnerships, supply chain / vendors, stakeholders, and objectives of the function.

Provide details of the context and environment of the function's BCP.

6. Objective of the plan

Provide details of the objective of the business continuity plan.

7. Roles and responsibilities

Provide details of roles and responsibilities relevant for a service disruption event based on the guidance of [Section 2.2 Roles and Responsibilities](#).

8. Risk Assessment

Detail the identification and assessment of the function's continuity risks based on the guidance of [Sections 3 Risk Assessment](#).

9. Business Impact Analysis

Detail an assessment of the impact of the service disruption events on the function based on the guidance of [Section 4 – Business Impact Assessment](#).

10. Triggering the Plan activation

Provide details of how to invoke the plan based on the guidance of [Section 5.5 Triggering a BCP](#).

11. BCM Call tree and contact details

Provide the details of persons to be contacted as part BCM process and their contacts.

Internal Key Contacts

Name	Position / Role / Team	Email Address / Physical Address / Business Phone Number	Home Address / Phone Number	Mobile Phone Number	Alternate Contact

External Stakeholders and vendor contact list

Organisation / Service Provided	Name / Role	Email Address / Physical Address / Business Phone Number	Home Address / Phone Number	Mobile Phone Number	Alternate Contact

12. Business Continuity Strategies and Plans

Map the specific plans the function has identified for the management of the identified service disruption events based on the guidance of [Section 5 Strategies and Plans](#).

- Action Cards:

Document the specific action cards for each role and event in the Appendix section of the plan. Guidance is provided in [section 5.3 Action Cards](#).

- Communication Plans:

Guidance on communication is provided in [section 5.4 Communication](#).

Document communication plans for event coordination using the template below:

FUNCTION				
Time since event	Communication Activity	Target Audience	Media	Sample Text
15 mins	Decision on invocation	BC Owner/BC Steer Co.	Phone / SMS / EM IM Channel	<event> occurred at <location and time> caused by <cause> expected to result in <>
30 mins	Invocation of plan	Patients, Staff, Relevant Suppliers, Relevant PRAs	SMS / Mail/ IM Channels / Website / Phone	

13. Test planning, execution, and reporting

Provide details of the test plans to be implemented indicating frequency, third party involvement and reporting format.

Guidance on Testing is provided in [Section 6.3 Testing](#).

14. Training and awareness creation

Provide details of planned training and updates delivery and the medium through which they will be delivered. Also indicate the target groups for each session.

Guidance on Training is provided in [Section 6.1 Training](#).

15. Evaluation

Provide details of how self-assessment will be performed and where the information will be stored.

Guidance on self-assessment is provided in [Section 7 Management Reviews](#).

Appendices to BCP Template

Table 11: Business Continuity Action Card Template

Action Card	<Name of function/area>	ACTION CARD NUMBER
	Designated person / Disruption Response Role e.g., Director of Nursing	1.1
EVENT:		

You Report To:		You Brief:	
Your Responsibilities			
IMMEDIATE ACTIONS ON ACTIVATION or STANDBY FOR ACTIVATION			
When Activated Do These Things “Break Glass” Instructions when incident has occurred		When On Stand-By Do These Things “Pre-Incident” Instructions i.e., before incident has impacted your service	

Consider these points				
<i>Continued overleaf if necessary</i>				
Version Control	Date Approved	dd/mm/yyyy	Valid Until	dd/mm/yyyy

Appendix 3 - Glossary of terms

Term	Definition
Action	<p>Actions are a future measure that will maintain and/or modify a risk.</p> <p>An action is a future measure to further reduce either the likelihood or impact of a risk.</p>
Business Continuity Management (BCM)	A holistic management process that identified potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, reputation, brand, and value-creating activities.
Business Continuity Management System (BCMS)	A BCM that is fully integrated into the management structure of an organization and that forms part of an overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption
Business Impact Analysis (BIA)	A process of analysing activities and the effect that a business disruption might have upon them.
Controls	Controls are measures that maintain and/or modify risk. In the HSE, a control is a measure that is in place, is working effectively and operating to reduce either the likelihood or impact of a risk. Controls include but are not limited to, any process, policy, device, practice, or other conditions and/or actions that are in place and maintain and/or modify risk.
Enterprise Risk Management (ERM)	Enterprise Risk Management (ERM) in healthcare promotes a comprehensive framework for making risk-based decisions that guide the protection and development of high-quality services and their contribution to improving healthcare outcomes. It enables better management of uncertainty and associated risks and opportunities. It guides the organisation to address risks comprehensively and coherently, instead of trying to manage them individually.
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.
Inherent Risk	Inherent risk in the HSE is the level of risk before consideration of control and/or action measures.
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 organization aims to resume its critical functions and services 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 operations. This also includes failing to maximise any opportunity that would help the HSE, or service meet its objectives.
Risk Analysis	Risk analysis is a process of determining how the identified risk can affect us and to estimate the level of risk attaching to it.
Risk Assessment	The overall process of risk identification, risk analysis, and risk evaluation.
Risk Rating	Risk is measured in terms of two dimensions, impact, and likelihood i.e., the impact (consequence) of the risk should it occur and the likelihood (probability) of the risk occurring. Likelihood x Impact = Risk Score. This is plotted on a 5 x 5 risk rating matrix and assigned a rate of High, Medium, or low.
Stakeholder	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: <ul style="list-style-type: none"> ▪ The Department for Health ▪ The Health Information and Quality Authority (HIQA) ▪ The National Cyber Security Centre (NCSC) ▪ The Board and its sub-committees ▪ Other Hospitals, Hospitals Groups and Community Health Organisations ▪ HSE funded services ▪ Patient Advocacy Groups ▪ Third Party Suppliers and Contractors The Public
Threat	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.

Appendix 4 - Acronyms

Acronym	Definition
ARC	Audit and Risk Committee
BAU	Business As Usual
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
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 5 - References

- ISO 22301:2019 – Societal Security – Business Continuity Management Systems
- ISO 22313 – Societal Security – Business Continuity Management Systems - Guidance
- ISO 22399:2007 – Societal Security - Guideline for Incident Preparedness and Operational 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: 24 February 2025