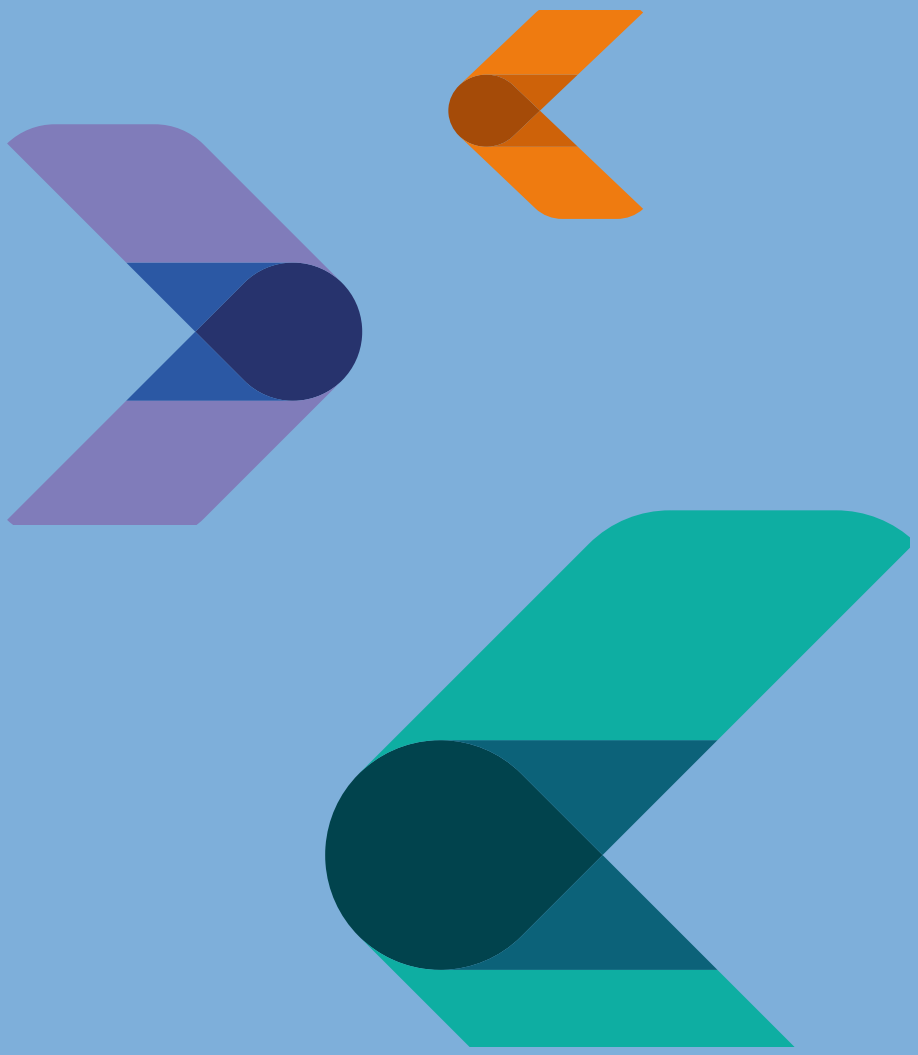
HSE Enterprise Risk Management Policy and Procedures 2023

Risk is the effect of uncertainty on objectives.

Health Service Executive (HSE) Enterprise Risk Management Policy and Procedures

International Standard Book Numbering (ISBN)	978-1-78602-205-9
Revision number	V0
EMT Review	21.03.2023
ARC Review	24.03.2023
Board approval date:	31.03.2023
Next revision date:	March 2026
Document developed by:	Enterprise Risk Management (ERM) Programme



Contents

Foreword

Bernard Gloster, Chief Executive Officer

As I take up my role as CEO of the HSE, I am conscious of the privilege it is to lead an organisation with so many dedicated healthcare professionals, managers and other critical workers across the country who provide the most critical of public services on a daily basis. This privilege comes with a deep sense of the responsibility I have to ensure we bring about the types of change needed and expected by those who depend on us for their care.

Over the course of a lifetime, everyone will have a need for our services. Whoever they are and for whatever reason they come to us, each one is an individual, a name, has a story and is part of a local community. Some will be facing life limiting conditions, or will be living with severe pain, or will be amongst the most vulnerable members of our society. Each person has the right to expect that we will meet their health or care needs and that we will do this in a timely manner. Therefore, for the term 'patient or service user centred care' to be real, it must be real for each person we serve.

There are pressing challenges facing the HSE, some of which at times seem insurmountable. It is my conviction that we can, and must, make a difference. I will be specifically focussed on ensuring we improve the ability of people to access our services as quickly as possible, that we implement our plans in a timely way and that we work to gain and retain the confidence of the population of this country.

How successful we are in making a difference in people's lives is dependent on many factors, one of which is our ability to anticipate and manage the unknowns, the things that can and will emerge tomorrow or next year or the unanticipated consequences of decisions we take. Risks are simply those unknown threats, that if and when they occur, can throw us off course. Managing risk is therefore fundamentally about improving our chances of success, by equipping us with the tools to anticipate what those threats could be, how we can prepare for them and how we can manage their impact if they do occur.

I am pleased therefore to present the HSE's Enterprise Risk Management (ERM) Policy and Procedures 2023 which have been adopted by the HSE Board.

The ERM Policy and Procedures has been contributed to by many of you across the health service and is based on international risk management standards. It provides a step by step guide to how we manage risk, in a way that is intended to be both useful and practical. The measure of its success will be how much it becomes a part of how we intuitively manage and ultimately how it assists us in staying on the ambitious path we have set for ourselves.

Acknowledgements

A word of thanks to the many people who contributed to the HSE Enterprise Risk Management Policy and Procedures, especially to all the **health service staff** who took the time to provide invaluable feedback during the consultation phases. A thanks also to the Executive Management Team and the Audit and Risk Committee members who provided advice and feedback on the process.

Introduction

Patrick Lynch, Chief Risk Officer

Since the HSE Board was re-established under the Health Service Executive Governance Act 2019, it has been charged with developing and implementing a more effective Corporate Governance Framework for the HSE. The Board has a specific responsibility to advise on the appropriateness, effectiveness and efficiency of HSE's procedures relating to risk management. Since 2019, the Board, the Audit and Risk Committee (ARC) of the Board and Executive Management Team (EMT) have been committed to strengthening our approach to managing risk. Embarking on this journey of improvement in 2019, we had little idea of the uncertainties just around the corner, not least of which was COVID.

There are however few examples that better demonstrate how uncertainty threatens our best laid plans and can potentially derail our efforts to deliver on those plans. The Government, on behalf of citizens, provides the HSE with a significant level of exchequer funding for the day to day running of the health service. It also invests in our longer term ambition that the experience of those receiving or waiting for care becomes demonstrably better. As the custodian of these resources, the HSE has an obligation to ensure they are managed effectively. Not to anticipate and plan for the uncertainties that threaten the delivery of our objectives would constitute a failure of corporate governance.

A risk by definition is a threat to an objective. Anticipating and managing those threats is the focus of risk management. For this reason, the CEO and ARC, supported by the EMT have made it a priority to develop and strengthen the HSE's risk management framework. One of the first decisions of the Board was to approve the recommendations of a 2019 Risk Review, a principal one being to establish an Enterprise Risk Management Programme. The ARC and EMT subsequently jointly commissioned an external examination of the HSE's corporate risk management process, the outcome of which has guided the Board and ARC's risk priorities, and has led to:

- More visible senior leadership for risk management,
- Greater clarity on the HSE's strategic risks and stronger Board oversight of risk through the Committees of the Board,
- Development of the HSE's first Risk Appetite Statement,
- Improved corporate risk reporting and the introduction of a Risk Information System,
- Securing of resources to build up the HSE's risk management expertise.

The publication of the HSE's Enterprise Risk Management Policy and Procedures 2023 marks another important milestone in our risk journey. Based on internationally recognised risk management standards and the practical experience of those managing risk across the health service, the Policy has been developed with considerable collaboration of colleagues from across the HSE and wider voluntary sector, a partnership which has enriched the content of the document.

It is our hope that the Policy will serve as a practical resource to you, whether you are a front-line worker in whatever capacity, including clinical staff, work in a critical support function, or serve in a management capacity. While the Policy sets out good practice in risk management, we have also sought to demystify what risk management means, to make it as accessible as possible, both to risk practitioners and others who will practically manage risk every day.

In all of our endeavours, managing risk well will improve our chances of achieving our objectives. The Policy signals our clear shared commitment to providing the highest quality health and social care services for the population of Ireland. As we continue our work, I hope that the Policy will support, in a practical way, all of you charged with implementing change, reaching our objectives and, most importantly, meeting the expectations of those who use our services.

Finally, I would like to acknowledge and thank Brendan Lenihan, the outgoing Chair of the ARC, for his commitment to our improvement journey, a commitment which was accompanied by a deep understanding both of our mission as a health service and of the important role the application of risk management can play in that mission.

Key Messages

Risk: Managing the Effect of Uncertainty on Our Objectives

As a health service, our objectives relate both to our day-to-day mission to provide, the highest quality health and social care services for the population of Ireland and to our longer term ambition that these services and the experience of those waiting for, or who are receiving care, become demonstrably better. Uncertainty about the future poses the single greatest barrier to us meeting both our day-to-day and longer term objectives. Uncertainty by its nature cannot be prevented and the only certainty is that situations will arise that threaten our ability to achieve those objectives.

Each one of us unconsciously and naturally manage **risks** every day, in our homes, as we travel and at work. **Risk management** simply provides us with a structured approach to anticipate the threats that could occur, assists us in identifying the most effective way to manage those threats and gives us the means by which we can measure how successful we have been in our efforts.

The **Enterprise Risk Management Policy and Procedures 2023** is therefore intended to be a practical resource for all healthcare workers, including clinicians and managers, with the aim of supporting you as you navigate the many uncertainties you face in your roles.

Uncertainty

Uncertainty: The future, whether that is tomorrow or next year, is uncertain. What has happened over the past year that we hadn't expected twelve months ago? Unexpected situations will always arise and they can prevent or hinder us from doing what we had planned to do. In our jobs this means preventing or hindering us in delivering on our core mission and objectives.

Predicting the future: Uncertainty means the future is difficult to predict. Attempting to predict it and prepare for it, can seem like wasted effort as many of today's predictions may never happen. However, if they do, they can have catastrophic consequences. When we recognise what could go wrong and the threat this poses, our focus is then on reducing the likelihood of these events occurring or should they occur, minimising their impact.

Identify

What are the real threats? We start by identifying the potential threats to our objectives, particularly those that are the most likely to occur, or the consequences of which would be most severe. The aim is not to predict every possible threat, but using the best information available to us to identify the ones we should be most concerned about.

What can help us identify them? We start by asking questions such as: What could happen? How could it happen? Why might it happen? There are also various sources of information that can assist us. These include data and trends (e.g. audit findings, incident data, complaints analysis, and performance trends), national and international surveillance systems and strategic risk surveys, the Government's National Risk Assessment, statistical modelling, other assessments of the internal and external factors influencing healthcare.

Describe

How do we know the threat has materialised? A predicted threat, when it occurs, will always be experienced in a tangible way, an Event. A threat of a pandemic was an example of a possible future event, however with the arrival of COVID-19 a theoretical future event, became a real one that was experienced. Similarly, the potential future threat of a cyber-attack became a tangible reality with the attack on the HSE's systems in 2021.

How do we describe the threat? When describing a future threat, there are three essential components:

(1) The **Event** itself: If the threat materialised, how would we recognise it? What would it look like? How would we experience it?

(2) The **potential cause(s)** of the Event. Start by identifying the potential causes recognising that often the obvious cause isn't the root cause which starts the domino effect that results in the Event. Understanding the cause(s) is fundamental to deciding how we can best eliminate or reduce the threat, and

(3) The **consequence or impact** of the Event if it occurred.

Evaluate

What are we attempting to control? We now need to put in place measures to prevent or reduce the likelihood of the threat occurring and its impact if it does occur. In some instances however, it may only be possible to control either the likelihood of it happening or the impact if it does. In the examples given above, there is very little we can do as a health service to reduce the likelihood of another pandemic. We can however reduce the impact if it does occur. Whereas in the event of a cyber-attack, we can reduce the likelihood of the attackers accessing our systems, as well as the impact if they do.

Respond

How do we respond? Having understood the potential Event and its cause(s), we can put in place measures aimed at either eliminating the threat, or at least reducing it. These measures called 'controls' fall into two categories, proactive and reactive. Proactive controls include **1)** directive controls, for example policies, procedures etc., and **2)** preventative controls that are designed to prevent the event occurring and are therefore typically stronger than other control types. Reactive controls include **3)** detective controls that are those that manage weaknesses or breaches after the event, for example audits and **4)** corrective controls and actions aim to fix the weaknesses or breaches detected. It is essential to understand that ***a control must be in place, be working effectively and have a direct influence on reducing the likelihood and/or impact of the threat.***

Analyse

What are we measuring? A simple scoring system is used to measure the level of threat. It looks at two things. What is the **1)** likelihood or probability of it materialising and **2)** what is its potential impact if it does? (Understanding the speed at which a threat could materialise is also an important consideration).

What does the scoring system tell us? Both the likelihood and impact are scored on a scale of 1 to 5 and multiplied, which means the lowest score is 1 (Low) and the highest is 25 (High). Obviously the higher the score is, the more we need to be concerned. Using this scoring system can help us to measure the threat level before we do anything about it (inherent), the level after we put effective controls in place (residual) and how far we want to reduce the level of threat (target). Where available, scoring should be informed by objective data/measures.

Review and Act

How do we record and monitor the effectiveness of our response?
Managers rely on a standard suite of reports to provide critical insights into how their area of responsibility is performing and which inform the decisions they have to make (e.g. Performance Reports, Financial Reports). In the same way, they also rely on a report (Register) that brings together in a summary form, all the essential information relating to the threats being managed. This includes a clear description of the threat, the measures that are in place to control the threat, the additional controls required to further reduce the threat and the measurement of the current level of threat. This Register should be regularly reviewed and used to inform management decisions, plans and actions.

Communication: Communication and consultation is essential to the process of identifying, assessing and responding to a threat. It ensures that the best information is available to the person managing it. It also provides an opportunity to mobilise others who can assist us in our efforts. Line Managers have a particular responsibility to understand the threats within their area of responsibility. Communication can be both informal and formal in this context, though should have a purpose and must have a clear objective and outcome. This includes **(i) Communication** where there is a sharing of information **(ii) Notification** that the threat has increased or to agree additional actions or **(iii) Escalation** where responsibility for managing the threat is accepted by the next level of management.

Apply

How do we use this approach? The approach set out in this Policy and Procedures is intended to become a core part of day-to-day management activity. In particular it should be used in:

Planning and Strategy development: Identified threats are a critical input to deciding our planning and strategy priorities. There may also be threats that could prevent or hinder their implementation. These need to be managed.

Decision making: Decisions we make can often lead to unintended consequences, or the benefits we expected do not materialise because of a threat which we hadn't anticipated. Considering the possible threats to, or consequences of, major decisions can assist us in (1) Prioritising (2) Making choices (3) Mitigating the threat.

Managing: Understanding the threats we face assists us in meeting our objectives. It creates a shared understanding of our core objectives and how teams can collectively work to reduce those threats. This will not happen spontaneously but requires us to integrate the approach described in this document into our day-to-day management of the health service.

Risk

Risk is defined as the *effect of uncertainty on our objectives*. Risk management is therefore about how we manage those uncertainties to give us the best chance of success in meeting our objectives. While this Policy and Procedures describes risk management in terminology that is recognised internationally and will be familiar to those who manage some part of the risk management process, the concepts of risk management are relatively straightforward and intuitive and will therefore be of use to everyone working across the health service.

Part 1: HSE Enterprise Risk Management Policy

1.0 Introduction

The HSE recognises the importance of adopting a proactive approach to the management of risk to support both the achievement of its objectives and compliance with governance requirements.

The HSE is committed to ensuring that risk management is seen as everybody's responsibility and is embedded both as part of the normal day-to-day business and informs the strategic and operational planning and performance cycle.

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. In particular, it guides the organisation to address risks comprehensively and coherently, instead of trying to manage them individually.[1]

This document sets out the policy and procedures by which the HSE manages risk. The approach is aligned with the ISO 31000:2018 Risk Management – Guidelines and replaces the HSE Integrated Risk Management Policy 2017.

1.1 Policy Statement

It is the policy of the HSE to manage risk on an enterprise-wide basis, that is, inclusive of all risks whether to do with management or service delivery processes. This involves proactively identifying risks that threaten the core objective of the HSE, which places patients and service users at the centre of our work, in delivering health and social care services to the population. It assists us in ensuring we fully comply with our legal and regulatory obligations and our responsibilities under the Code of Practice for the Governance of State Bodies.

1.2 Purpose

The purpose of this policy is to:

- Outline the commitment of the HSE to the proactive management of risk in line with our vision for a health service that puts patients and service users at the centre, makes the best use of public resources and fulfils our corporate governance responsibilities.
- Assist staff in understanding their role in, and the need to adopt a consistent approach to the assessment and management of risk.
- Set out the systems and processes that are required to ensure that risks are managed consistently across the HSE.

1 Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015) 'Enterprise Risk Management: Review, Critique, and Research Directions', *Long Range Planning*, 48, pp. 265-276

This policy supports this purpose by:

- Seeking to ensure that risk management is seen by all staff as part of the normal day-to-day activities in delivering healthcare services.
- Clearly defining the roles and responsibilities for risk management.
- Outlining a consistent process for risk management including risk identification, risk assessment and risk treatment.
- Outlining the process for the communication, notification and escalation of risk.
- Ensuring that, where actions to manage a particular risk are not within the control of the relevant Risk Owner, either because of lack of authority or resources, such actions can be escalated and then accepted by the next line of management for review and decision-making.
- Ensuring that all identified risks are recorded in a consistent manner, the minimum requirements for which are set out in this document.
- Identifying risk management tools required to support the implementation of the risk management policy.

1.3 Scope

This policy applies throughout the HSE and is applicable at a national level, and within Hospital Groups and Community Health Organisations (CHOs), the National Ambulance Service (NAS), other national services, and Regional Health Areas (RHAs), once established. It applies to both strategic and operational risks that the HSE is exposed to and manages on an integrated basis. Local risk policies and procedures must be aligned with and be consistent with the requirements of this policy.

This policy serves as a guide to managing risk in the context of interagency engagements, where the HSE is the lead stakeholder in the interagency governance arrangements. It will also support the communication of risks with external partners when delivering on common objectives.

It is essential that HSE funded agencies (Section 38 and Section 39 organisations) have a formal risk management policy and risk management process in place and which reflects best practice. While these organisations manage risk according to their internal policies, it is expected that this policy will assist them in the design and implementation of their own risk management framework.

PLEASE NOTE: that while this policy covers all organisational risks, there are specific risk assessment tools in place for:

- The clinical risk assessment involving care and treatment relating to individual service users.
- Health and safety risk assessments (See https://healthservice.hse.ie/staff/health-and-safety/risk-assessment)

1.4 Key Definitions

Risk is the effect of uncertainty on objectives[2]. 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.

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.

Actions are a future measure that will maintain and/or modify a risk. In the HSE, an action is a future measure to further reduce either the likelihood or impact of a risk.

Risk Treatment is a process to modify risk[2]. In the HSE, risk treatment includes the implementation of effective controls and future additional actions.

Inherent risk in the HSE is the level of risk before consideration of control and/or action measures.

Residual risk in the HSE is the level of risk remaining after consideration of existing controls.

Target risk in the HSE is the planned level of risk after consideration of both control and action measures.

Risk appetite is the amount and type of risk that an organisation is willing to pursue or retain[2]. In the HSE, it is the level of risk the HSE is willing to accept to achieve its strategic objectives.

Risk tolerance is an organisation's readiness to bear the residual risk in order to achieve its objectives[2]. The HSE defines risk tolerance as the level of deviation from risk appetite that we are prepared to tolerate.

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

This policy aims to provide a unified language of risk and it is recognised it can take time for definitions to be adopted into everyday practice. Where appropriate, the definitions used are from the ISO 31073:2022(E) 'Risk Management – Vocabulary' document referenced throughout this policy. However, there are some departures from this guide to be consistent with the internal context of the HSE.

The terms Inherent, Residual and Target are introduced in this update of the policy and are for use, in line with the guidance below, subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

Other risk terminology commonly used throughout the HSE are now defined below.

Initial risk is the level of risk after existing controls are considered **when the risk was originally assessed**.

Current risk is the level of risk after both the existing controls and actions are considered **at the point in time the risk is being assessed.**

2 ISO 31073:2022(E) Risk Management – Vocabulary

1.5 Roles and Responsibilities

1.5.1 HSE Board

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

1.5.2 HSE Audit and Risk Committee and other Board Committees

The HSE's Audit and Risk Committee (ARC) has responsibility for providing oversight and advice concerning the operation of the HSE's risk management policy and related activities within the function of risk management. Other Board Committees provide oversight of specific principal risks of the HSE as delegated by the ARC Chair.

1.5.3 HSE Executive Management Team

The Executive Management Team (EMT), led by the Chief Executive Officer (CEO), is responsible for executive decision-making in the HSE. This includes implementing and ensuring compliance with the HSE's risk management policy. *(In the context of the HSE's organisational changes, the term EMT also refers to any successor team to the EMT. References to the EMT in this Policy and Procedures should be understood as such).*

1.5.4 Managers

All managers are responsible for:

- Implementation of and ensuring compliance with the HSE's Enterprise Risk Management Policy in their area of responsibility.
- Ensuring that appropriate and effective risk management processes are in place within their delegated areas.
- Risk assessing all strategies, business plans/service developments including changes to service delivery.
- Developing specific objectives within their service or operational plans which reflect their own risk profile and the management of risk.
- Ensuring that a process of risk identification is in place for both clinical and non-clinical risks throughout their areas of responsibility and that risk assessments are conducted in accordance with this policy.
- Maintaining a risk register and formally reporting on risk to the next level of management.
- Ensuring that all staff identify risks within their working environment and are aware of their personal responsibilities in accordance with the Enterprise Risk Management Policy and Procedures.

1.5.5 Staff

All staff are required to:

- Be familiar with the HSE's Enterprise Risk Management Policy and Procedures.
- Understand that risk management is integral to their working practice within the HSE
- Have a working knowledge of related risk management procedures.
- Identify and report any potential risks to their Line Manager.
- Complete risk management training appropriate to their role.

Whereas every staff member is responsible for identifying and managing risk within the context of their work, there are certain common roles and responsibilities within every level of the health service for communication, notification, and escalation of identified risks, controls, and actions.

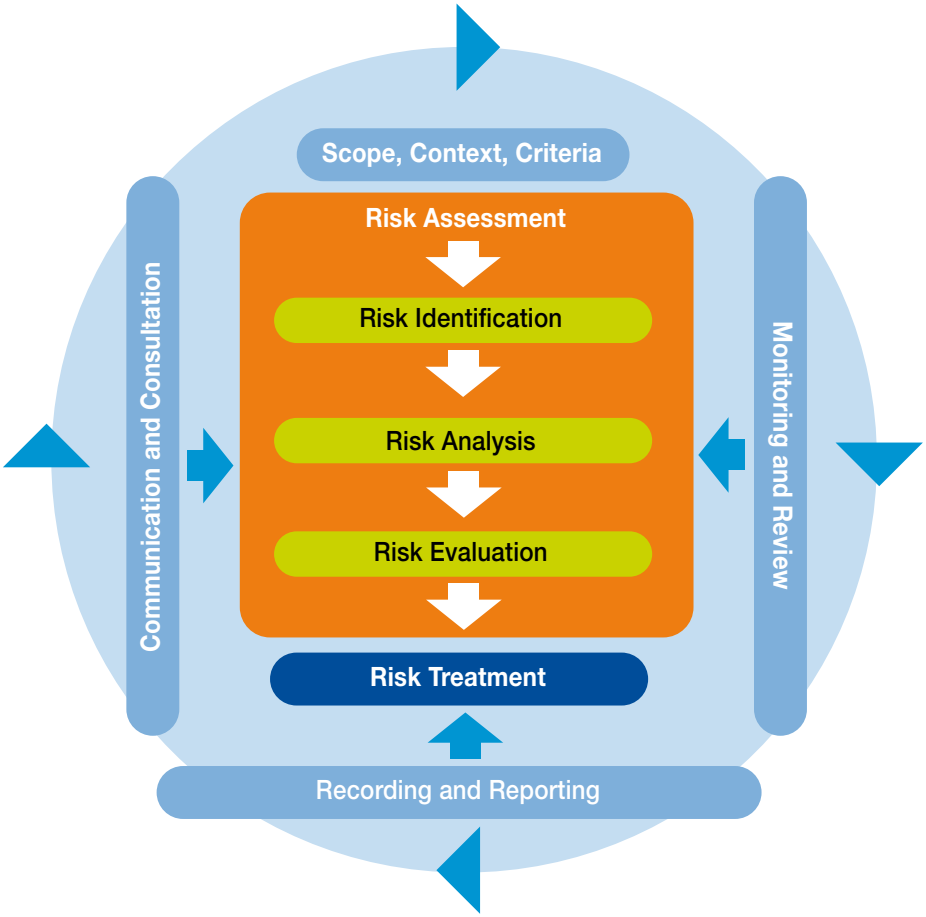
1.5.6 Risk Roles Common to Each Level of the Health Service

Role	Definition
Risk Owner	Each risk should be assigned to a Risk Owner who is responsible for ensuring that the risk is managed appropriately and in line with this policy. This includes ensuring; ▸ Controls and actions are in place to manage the risk. ▸ Actions identified to manage the risk have been assigned to an Action Owner and a completion date agreed. ▸ Notification, escalation or de-escalation of the risk or actions where appropriate. The Risk Owner is normally the Manager of the function/service in which the risk is identified. Where multiple personnel have direct responsibility for, or oversight of, activities to manage an identified risk, they should collaborate with the accountable Risk Owner in their risk management efforts.
Risk Lead	The role of the Risk Lead is to support the Risk Owner by facilitating and advising on the technical aspects of the risk management process. They **may** also be responsible for the administration of the risk register and the provision of reports to the Risk Owner and their Management Team.
Risk Coordinator	The role of the Risk Coordinator is to assist the Risk Owner and Risk Lead with the initial assessment, ongoing review, monitoring and reporting of an individual risk.
Subject Matter Expert (SME)	The role of the Subject Matter Expert (SME) is to assist the Risk Owner and Risk Lead with the initial assessment of the risk by providing expertise on the subject matter of the risk being assessed and following this, to assist the Risk Owner with the risks' ongoing review and monitoring. There are many SMEs in the HSE and these include for example, people working in the following areas or roles i.e. Clinical, Health & Safety, Occupational Health, Data Protection, HR, Finance, IT, Digital and Cyber experts, Quality and Patient Safety Staff etc.
Action Owner	The Action Owner is accountable to the Risk Owner and is responsible for ensuring delivery of an action assigned to them and reporting on progress relating to the achievement of that action. Actions may then become controls once completed and operating effectively.
Control Owner	The Control Owner is the person responsible for performing the control. It is the responsibility of the Risk Owner to identify the Control Owner and set a future date to review the control as relevant to the risk to ensure that the control remains effective.

1.6 Risk Management Process

The HSE's approach to risk management is aligned with the ISO 31000:2018 and can be broken down into a number of steps as outlined in Figure 1. For an overview of the risk management process refer to Section 2 of this document.

Figure 1: HSE Risk Management Process



Source: adapted from ISO 31000:2018

1.7 Monitoring Implementation of and Compliance with Policy

Each Manager is responsible for the implementation of, and monitoring of compliance with, this policy within their area of responsibility.

The Enterprise Risk Management (ERM) Team in the Office of the HSE's Chief Risk Officer (CRO) will provide implementation support.

In order to provide assurance on the implementation of the policy the ERM Team may undertake audits and report on compliance. An audit can involve self-assessments, the review of completed risk registers and risk assessment forms as well as the documentation that evidences the assignment and monitoring of risks, controls and action plans that are relevant to the area or service.

Risk Management audits may also be carried out by the HSE's Internal Audit function. Reports and recommendations arising from internal audits will be reported to the relevant Senior Accountable Officer, the HSE's EMT, and ARC.

1.8 Dissemination

This policy will be distributed by the Chief Risk Officer to members of the EMT, National Directors, Chief Officers, Chief Executives of Hospital Groups and to national services and functions for cascading throughout the HSE and will be available on the HSE website. Its publication will be supported by a broadcast email to all staff.

1.9 Implementation

To support services in the application of the policy, process and guidance, useful tools have been developed and are referenced in this document. Supporting guidance and tools are also available on https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/

Training resources are available on HSeLanD such as:

HSE Excel Risk Register eLearning

As additional tools are developed they will also be made available either on HSeLanD or on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie

The CRO commits to continuing to work with relevant National teams and services to design and develop further guidance, tools and training required to operate in line with the requirements of the policy, process and guidance.

Targeted training will also be available to support the implementation of this Policy and Procedures.

Part 2: HSE Enterprise Risk Management Process

2.0 Risk Management Process

The HSE's approach to risk management is aligned with ISO 31000:2018. The key components of the risk management process are:

- 2.1: Scope, Context and Criteria
- 2.2: Risk Assessment
- 2.3: Risk Treatment
- 2.4: Recording and Reporting
- 2.5: Communication and Consultation
- 2.6: Monitoring and Review
- 2.7: HSE Corporate Risk Register Reporting
- 2.8: External Risk Engagement

This document aims to provide a framework to manage risk in line with the above steps of the risk management process, shown in Figure 1.

2.1 Scope, Context and Criteria

The effective management of risk is central to the ongoing success and resilience of the HSE in the delivery of health and social care services. The HSE recognises that risk management is good management practice and in accordance with effective corporate governance as it progresses the achievement of both strategic and operational objectives, and improves decision-making.

2.1.1 Scope of Risk and our Objectives

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. In addition to these plans the HSE also develops major strategies relating to a broad range of developments.

Planning and risk are part of a continuous cycle whereby strategy is informed by and responds to risk, while the risks to the implementation of strategy are identified and managed. Risk identification and management are therefore central to future planning and strategy development and should be integral to the development of strategy, that is the risks that the strategy is responding to and the risks to the delivery of the strategy. Evidence of this having been done should be part of the approval process for new strategies. Anticipating and proactively managing these risks assists the organisation by improving the opportunities for success.

2.1.2 Scope of Risk Based Decision-making

Management Teams at each level of the health service have to make significant **decisions**. These may relate to areas such as planning choices, strategy development, investment decisions and resource allocation. Assessing risks at the decision-making stage, at the commencement of and during the implementation of these decisions should be a formal part of the decision-making and implementation process. The identified risks and mitigating measures should be documented in all proposal papers tabled for decision.

2.1.3 Establishing the Context

The expanding and changing healthcare environment, rapid changes in healthcare technology and health literacy, threats to public trust and confidence in the health service, staff and patient experience, cyber security, and the ever-changing regulatory, legal, and political environment have introduced a new level of complexity to managing risk in healthcare.

Establishing the context requires us to identify the **external and internal factors** that the HSE and its services must consider when they manage risk. Examples of some external and internal factors that can impact objectives are set out in Figure 2 below.

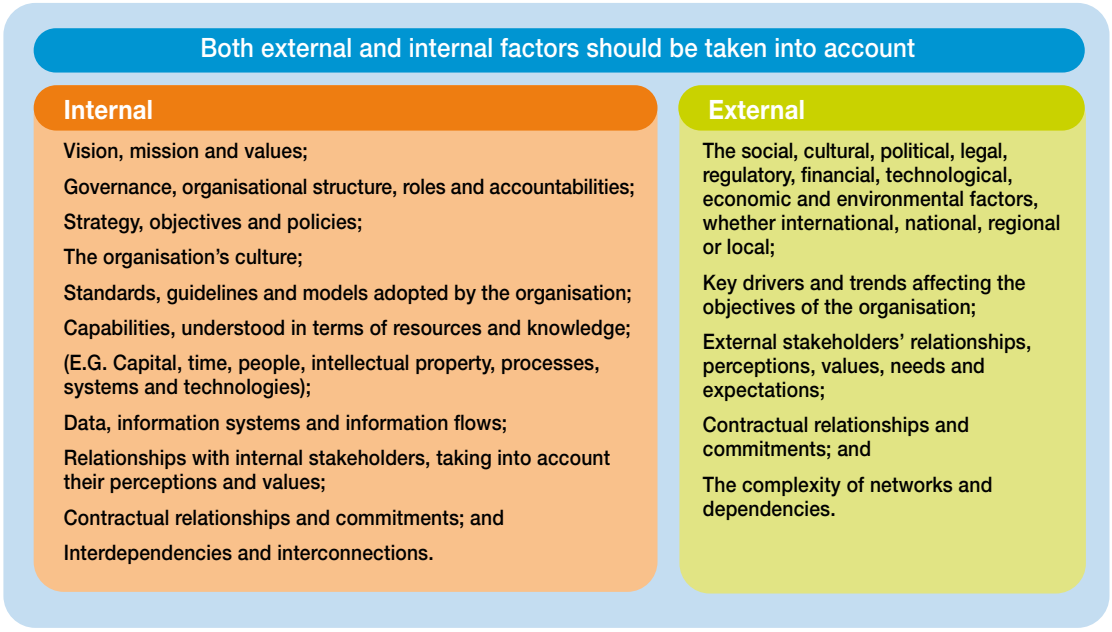
2.1.3.1 Understanding the Internal Context

The HSE's internal context includes its strategic objectives, governance arrangements, legal and regulatory obligations, organisational objectives, resourcing, contractual arrangements and key partners in the delivery of health and social care services, for example, with HSE funded agencies (Section 38/39 agencies). It also includes the HSE's workforce, capacity and capability, internal policies and procedures including the Incident Management Framework, Corporate Safety Statement, Human Resource policies, Clinical and Care policies, compliance obligations, financial regulations, etc. Internal context can also relate to a specific service and the factors that must be considered when managing risk, for example, the risks associated with delayed access to care.

2.1.3.2 Understanding the External Context

The HSE's external context includes its external stakeholders, for example, the Department of Health, and other government departments, Regulators, patient/service users. It also involves public policy and the legal and regulatory framework that applies to healthcare delivery in addition to political, economic, technical, and demographic influences.

Figure 2: Examples of External and Internal Factors that can Impact on Objectives



Source: adapted from ISO 31000:2018

2.1.4 Establishing the Criteria (including Risk Appetite)

In the HSE, establishing the criteria requires us to identify risks as either strategic or operational. This can provide a structured view of how such risks should be managed. Then, the risks that have been identified should be categorised and assessed according to the primary area of risk impact.

Lastly, the amount and type of risk that we may or may not take, should be determined relative to our objectives, and our appetite for risk.

2.1.4.1 Strategic and Operational Risks

Strategic risks concern threats to delivering on the medium to long-term strategic objectives of the HSE. These may be external or internal to the organisation. Strategic risks are most commonly identified at a national, corporate, or Senior Management level.

Operational risks concern the day-to-day threats that the organisation is confronted with as it strives to deliver its objectives. Operational risks are most commonly identified at a service delivery level.

2.1.4.2 Categorisation by Risk Impact

This policy requires that identified risks be categorised and assessed in relation to the primary area upon which they impact. For this purpose the HSE had previously identified a number of **risk impact categories** that have now been expanded, see Table 1 below.

Table 1: Categories by Risk Impact

Categories by Risk Impact
Harm to a Person (service user, patient, staff & public)
Service User Experience
Business/Service Disruption/Security (unauthorised and/or inappropriate access to systems/assets including data)
Loss of Trust/Confidence or Morale (Public/Staff), including reputational risk
Organisational Objectives or Outcomes
Compliance (legislative, policy, regulatory including data)
Financial (including performance to budget, claims, etc.)
Environmental/Infrastructure/Equipment
Strategic Programme/Project (objectives/timeframes) – *HSE Executive Use Only*

Only **one impact area should be chosen as the primary category**, even though a risk may impact many of the categories (secondary impacts). As an example, a risk that relates to *Harm to a Person* may also result in poor *Service User Experience* and the *Loss of Trust/Confidence or Morale*, but if the physical harm was prevented the latter two impacts would not have occurred. This will become important when it comes to analysing the risk.

The categories by risk impact have further detail provided within the HSE's Risk Impact Table included in Appendix 2.

2.1.5 Risk Appetite

The Board is responsible for setting the **risk appetite** for the HSE and this is articulated through the Risk Appetite Statement which defines the risk appetite and risk tolerance for specific areas of risk. The HSE's risk appetite framework is evolving to make it an increasingly useful tool for guiding the level of risk the HSE is willing to accept.

Though risk appetite and risk tolerance may be new concepts to many, these will progressively become a feature of the HSE's enterprise risk management approach as the organisation's risk maturity evolves.

2.1.5.1 What is Risk Appetite and a Risk Appetite Statement?

Risk appetite is the level of risk the HSE is willing to accept to achieve its strategic objectives.

The HSE's Risk Appetite Statement describes the type of risk the Board of the HSE is prepared to accept in the pursuit of its strategic objectives. It provides guidance and broadly informs the level of risk it is willing to tolerate across key risk areas.

The HSE defines risk tolerance as the level of deviation from risk appetite we are prepared to tolerate. Depending on the nature of the risks, tolerance levels will typically be temporary by nature and should have an associated reduction plan.

The HSE's overarching risk management strategy is to be cautious with a preference for safe options where the expected level of benefit is limited. While the HSE understands that it cannot manage all risks, the HSE is willing to accept well managed risk-taking in certain circumstances; for example, where it is satisfied that there is a likelihood of better patient outcomes or where there is scope to increase the effectiveness of services or care pathways through innovation and integration.

2.1.5.2 How to use Risk Appetite?

Risks outside of appetite are required to be addressed to bring them back within tolerance and to the desired target level of risk appetite.

It is acknowledged that due to its complexity and the nature of the services it provides, the health service often operates with a high level of risk. Indeed there are times when it is appropriate for the organisation to embrace risk as it pursues its goals. However, the risk management process requires that when risks are identified, measures required to reduce the risk to an acceptable level, or within appetite, are undertaken. These measures, controls and actions, are further explained later in the document and should be detailed as part of the risk treatment process.

There can be circumstances, where a risk, when rated, is outside of the HSE's risk appetite or tolerance, where defined, or when a risk continues to have a high residual risk rating, above the target risk rating. This may be acceptable for a defined period of time once agreed by the relevant accountable person or within the existing governance structures (e.g. Management Team). However, the rationale for the decision and the decision itself should be clearly documented and retained for audit purposes. There also needs to be an associated treatment plan with definitive timelines identified and stated timeframes within which the decision will be reviewed.

2.2 Risk Assessment

Risk assessment is a process consisting of the following three steps:

- Risk Identification
- Risk Analysis (including Risk Rating)
- Risk Evaluation

Detail of these three steps are set out below and examples of some of the tools that can assist in the risk assessment process are detailed in Section 3, such as the Risk Universe, Political, Economic, Societal, Technological, Legal and Environmental (PESTLE) analysis, Bow-tie analysis, Horizon scanning and the '5 Whys' method.

2.2.1 Risk Identification

Risk identification is an ongoing activity of all managers and their teams. Risks may be identified from a variety of sources both internal and external, as set out above. Having understood the risk, it will then need to be described in a succinct but structured way that describes the **event** itself, **cause**(s) of the risk and the **impact** or consequences if it does materialise.

The **risk description** is an important summary that will be used to effectively communicate the risk to the organisation. As such it should be clear and be described in a consistent manner. The risk description is a structured statement of risk usually containing three elements: risk event, cause and impact. A method used to do this is as follows;

'There is a risk of (event)… due to (cause)….resulting in (impact)'

Although risks and issues can sometimes be confused, simply stated, a risk is something that **may** happen, whereas an issue concerns something that **has** happened.

2.2.2 Risk Analysis (including Risk Rating)

Risk analysis is a process of determining how the identified risk 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 process for rating risk is:

1) Using the **Likelihood Table**, see Appendix 2, identify and assign the **likelihood** score of the risk occurring on a scale of 1 to 5; and
2) Using the **Risk Impact Table**, see Appendix 2, 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.

The assessment of likelihood and impact is in some cases subjective but should be assessed by relevant managers and subject matter experts to reduce the level of subjectivity. Preferably, where it is available, independent data to support your assessment should be used. This can include performance data, incident data, internal and external audit reports, inspections, surveys and a range of other available internal and external information.

The HSE has developed a **Risk Assessment Tool** for this purpose, see Appendix 2.

The **Risk Assessment Tool** is comprised of the Likelihood Table, HSE Impact Table, HSE Risk Scoring Matrix and the HSE Risk Rating Matrix.

Application of this tool will result in a risk being rated as high risk (red), medium risk (amber), or low risk (green). This rating will assist both in the evaluation of risk and the prioritisation of the management of risks.

The following are the levels of risk ratings for the analysis of risk, illustrated in Figure 3. These are;

Inherent risk in the HSE is the level of risk before consideration of control and/or action measures.

Residual risk in the HSE is the level of risk remaining after consideration of existing controls.

Target risk in the HSE is the planned level of risk after consideration of both control and action measures.

Other terms in use

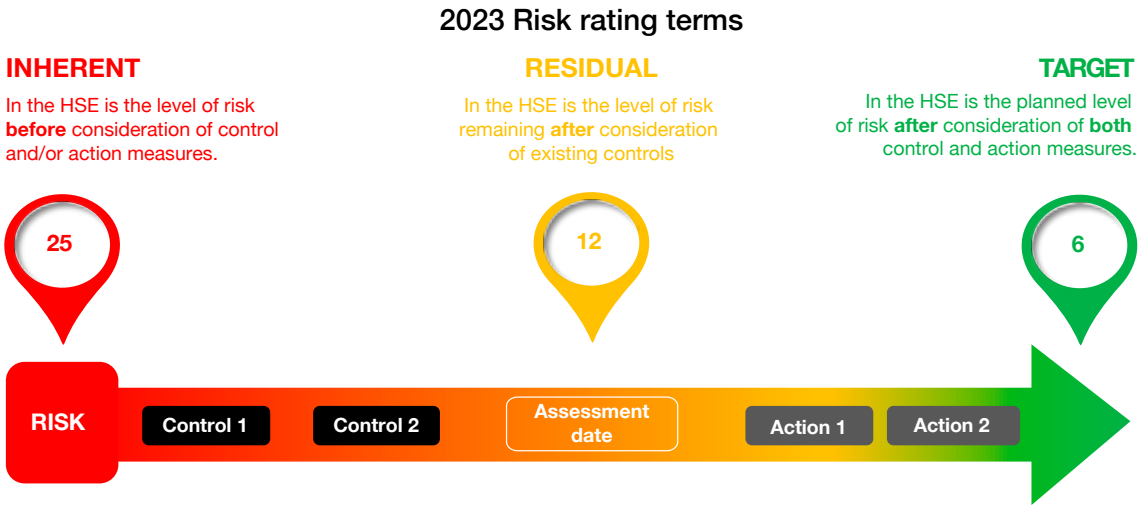
Initial risk is the level of risk after existing controls are considered **when the risk was originally assessed**.

Current risk is the level of risk after both the existing controls and actions are considered **at the point in time the risk is being assessed**.

It is recognised that both initial and current risk, as defined above, are in use at the time of this update when assessing and reporting on risks using the Generic Risk Assessment Form 2018 (Word document) and HSE Excel Risk Register v4 Mar 2018 (Excel document) available on the HSE internet.

Further to the implementation plans referenced above, the terms Inherent, Residual and Target are introduced in this update of the policy and are for use, in line with the guidance below, subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

Figure 3: Risk rating terms



2.2.3 Risk Evaluation

The purpose of risk evaluation is to make decisions based on the risk analysis stage of the risk process, about which risks need treatment and the treatment priorities. The process considers whether or not a risk is within the desired level of risk. Where it is determined that the level of risk posed is not acceptable, the risk must be treated.

Risk evaluation leads to the determination of the most suitable method to manage the risk, such as;

- **Avoid/Terminate** it completely e.g. do not proceed with the planned activity.
- **Accept** the level of risk based on existing information e.g. pursue the opportunity.
- **Transfer the risk** e.g. to an identified individual or unit, that has been communicated to and notified, where many of the actions identified as required to mitigate are better managed and are within their span of control.
- **Reduce** the risk with further controls and/or actions.

There can also be circumstances, where a risk, when rated, is outside of the HSE's risk appetite, or tolerance, where defined, or when a risk continues to have a high residual risk rating, above the target risk rating. This may be acceptable for a defined period of time once agreed by the relevant accountable person or within the existing governance structures (e.g. Management Team). However, the rationale for the decision and the decision itself should be clearly documented and retained for audit purposes. There also needs to be an associated treatment plan with definitive timelines identified and stated timeframes within which the decision will be reviewed. These decisions may also be reviewed at a more senior level of management.

2.3 Risk Treatment

Risk treatment is a process to modify risk. In the HSE, risk treatment includes both **control and action measures** to be implemented to reduce either the likelihood or impact of a risk.

Controls can be broadly grouped into two categories, that of proactive and reactive. There are four types of controls, both **Preventative** and **Directive** are proactive and the further two types, **Detective** and **Corrective** are reactive. A variety of the above controls can be adopted, again in line with the risk treatment process decided upon.

As set out above, one way to reduce risk is to avoid it. However, this may not always be possible or practical, so other options will have to be considered. Several options are available to reduce risk, either by decreasing the likelihood of occurrence, the impact, or both. The correct level of risk identification and analysis is important as it influences the level of controls required, the justification of the costs of controls, and the control approach. Risk treatment should include efficient and effective control measures to reduce the risk. The effectiveness of control is the degree to which the risk will either be reduced or eliminated by the proposed measures.

Ongoing reviews of the risk may highlight the need to further reduce the risk and so more controls/ actions may be required. These should be listed as discrete measures that can be assigned by the Risk Owner to a named individual (Control Owner or Action Owner) and relate to a measurable deliverable.

The Risk Owner should agree with the **Control Owner** on a set date to review the control to ensure it continues to operate effectively.

The Risk Owner should decide with the **Action Owner** on a reasonable timeframe for the completion of an action. In keeping within the lines of accountability, the Risk Owner can assign actions relating to their risk register to themselves, to someone who reports to them (i.e. a member of their team) or to the person they report to (i.e. their Line Manager).

While all possible measures should be taken to reduce or eliminate risk, it may not be feasible to put in place the range of actions required. This may be due to resources or other constraints. What is important is that as the Risk Owner, you have taken any actions required that are within your direct control and appropriately communicated the actions that lie outside of your control to your Line Manager. In circumstances where you can provide evidence that this has occurred, you have fulfilled your responsibility to your Line Manager (i.e. you cannot be held accountable for aspects of the risk which lie outside your control).

These decisions may also be reviewed at a more senior level of management.

2.4 Recording and Reporting of Risk

The outcome of the risk assessment and treatment stage of risk management should be documented on a Risk Assessment Form and recorded on the relevant risk register using the standardised excel risk register tool both available at: Risk Management Support Tools – HSE.ie. Copies of the Risk Assessment Form and any related documentation should be kept on file for future reference and audit purposes and per the requirements of records retention.

2.4.1 What is a Risk Register?

The risk register is an important document for those who are responsible for managing risk. Managers rely on a standard suite of reports to provide critical insights into how their area of responsibility is performing and which inform the decisions they have to make (e.g. Performance Reports, Financial Reports). In the same way, they also rely on a risk register that brings together, in a summary form, all the essential information relating to all of the risks being managed.

The register involves, for individual risks, a clear description of the risk, the control measures that are in place to reduce the risk, the additional actions required to further reduce the risk and the measurement of the level of threat. It also records performance in managing the risk over time through the decreasing or increasing of the ratings.

In many situations, having a risk register in place is viewed as the primary objective of the risk management process. This is, however, not the case but should be used to inform management decisions, plans and actions.

In order to be most effective, the risk register should be reviewed at a minimum on a quarterly basis.

The HSE has commenced the process of recording certain risk registers on an online risk information system. In areas where deployment has not yet occurred and where there is no risk information system currently available to you, services should continue to use the risk tools made available on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie

2.4.2 Changing the Status of Risks on the Register

Whilst under active management, a risk has the status of being **Open**. Upon completion of actions and where there is evidence that the risk has reduced and/or been effectively brought to the desired level of risk, consideration can be given to changing its status to either **Monitor** or **Closed**. Risks with a status of **Monitor** undergo periodic review to ensure that they remain at the desired level of risk, as far as is reasonably practicable. Risks that have all the required actions completed, are within the desired level or appetite, and require no further actions are assigned the **Closed** status and are archived onto a Closed Register for audit purposes. Closed risks should be reviewed periodically to ensure controls continue to operate effectively. Where control measures no longer maintain or modify the risk, the risk rating should be reassessed.

2.5 Communication and Consultation

Communicating and consultation is an essential part of the risk management process. It can enrich the risk identification and assessment process and assist in identifying options for managing a given risk. Communicating about risk within and across teams can help to ensure that the risks to the organisation are better understood, systemic risks can be identified and that effective plans are developed to manage the risk. Communicating about risk is also a core management responsibility. In this context there are three levels of communication, each of which increases the formality associated with the communication. These are;

- Risk communication
- Risk notification, or
- Risk escalation

Risk communication is the sharing or exchanging of information and gaining a common understanding of the risk. Line Managers have a responsibility to understand the risks across the part of the organisation they have responsibility for. This type of communication should therefore form a routine part of the management process between a Line Manager and their direct reports and therefore a review of the relevant risk register should be regularly undertaken.

Risk notification in the HSE, is recognising the risk is increasing or is not being managed effectively, and so requires notification to the next level of management. A risk notification is not a formal escalation of risk. A written record of the notification and any subsequent actions agreed should be retained on file. Where a Line Manager has received a risk notification they should decide whether the subject of the notification needs to be, in turn, notified to their Line Manager.

Risk escalation is required in certain circumstances that could include when a risk can no longer be managed at the level in which it is expected to materialise i.e. it is agreed that a higher level manager would be a more appropriate owner or the risk is more systemic and a more comprehensive set of actions to manage the risk are required. A written record of the escalation and any subsequent actions agreed should be retained on file.

A fundamental principle is that risk is managed at the level at which it is expected to materialise.

2.6 Monitoring and Review of Risk

Risks recorded on the risk register must be subject to **ongoing monitoring** by the Risk Owner and relevant Management Team to ensure that actions identified as required are completed.

The risk register should be tabled regularly for review at Management Team meetings, and at a minimum on a quarterly basis.

With the completion of actions, the level of risk (the rating) may be reassessed to consider whether its likelihood or impact has reduced. Where the implementation of actions does not appear to be reducing the risk, or where the nature of the risk has changed, the appropriateness of actions should be reviewed and revised treatment plans developed.

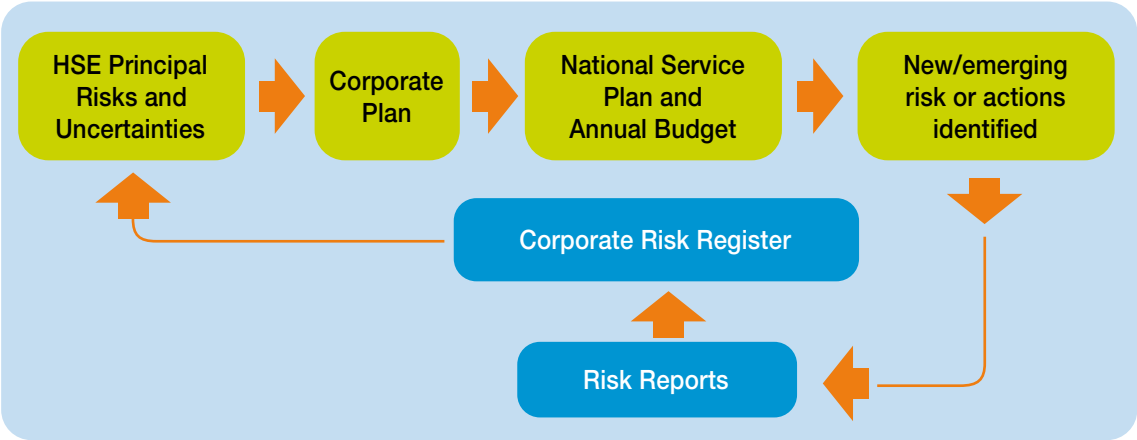
2.7 HSE Corporate Risk Register Reporting

The Chief Risk Officer is responsible for facilitating the monitoring and reporting of risk to the HSE's EMT, ARC and other Board Committees to the Board. This involves, amongst other responsibilities, promoting awareness in the area of enterprise risk management, engagement with the corporate planning cycle, supporting the assessment of potential or emerging risks, internal risk reporting, including the 'HSE's Corporate Risk Register', and external risk reporting with relevant external stakeholders.

2.7.1 Corporate Planning Cycle

As risk management is concerned with the achievement of objectives, the understanding of corporate risks is central to the corporate planning cycle. A high level overview of this process is included in Figure 4 below.

Figure 4: Corporate Planning and Risk Management cycle



Following a robust risk assessment process, the HSE Board approves the **principal risks and uncertainties** impacting the organisation. The assessment is also used in developing the Corporate Plan, National Service Plan (NSP), and annual Budget. Each of these principal risks has an associated action plan which is intended to mitigate the risk by either reducing the likelihood of it occurring or its impact if it does materialise. These **principal risks** are recorded in the HSE's Corporate Risk Register (CRR).

2.7.2 HSE's Corporate Risk Register

The HSE's principal risks are recorded on the HSE's CRR. They are approved by the EMT and reviewed by the Audit and Risk Committee and other Board Committees who have responsibility for oversight of the HSE's principal risks. In accordance with the Code of Practice for the Governance of State Bodies, the Board review and approve the HSE's Corporate Risk Register for its annual sign off on the HSE's principal risks and uncertainties to form the basis of reporting in the HSE's Annual Report.

All HSE corporate risks, recorded on the HSE's CRR, and associated action plans are reviewed by the EMT as part of either a monthly or quarterly review process depending on the nature of the risk. Each of the risks on the CRR is assigned to a member of the EMT as the owner of that risk. The Chair of the ARC allocates each of the risks to one of the committees of the Board to provide oversight for the management of risks and review these risks and associated action plans with the relevant members of the EMT.

The format and structure of the CRR may vary, but in principle includes both a summary of the most significant risks the HSE faces, including any changes in risk profile, and a status update on risk treatment plans.

2.8 External Risk Engagement

Some risks, particularly the HSE's strategic risks, emerge from factors external to the organisation. As such, the actions required to mitigate these risks, lie outside of the control of the HSE. It is important therefore to establish mechanisms for communicating these risks with the relevant body, with a view to arriving at a shared understanding of the risk and of what is required to mitigate it. These can involve joint risk assessments, the sharing of relevant risk reports, or joint engagements to inform the planning or provision of similar services.

One example is that of the Government regularly publishing a National Risk Assessment to identify and discuss significant risks facing the country. The National Risk Assessment is intended to inform the detailed risk identification and management and preparedness that happens across Government departments and agencies. Since it was first published in 2014, the National Risk Assessment process has called attention to various risks that subsequently became major issues for Irish society, including Brexit, risks around the housing supply, and indeed, pandemics.

Part 3: HSE Enterprise Risk Management Procedures

3.0 Procedure: Scope, Context and Criteria

Establishing the scope, context and criteria sets the framework for undertaking the risk assessment, makes clear the reasons for carrying out the risk assessment and provides the background against which you can identify and assess risks.

Understanding the external and internal environment is the first step in the risk management process. It considers risks and opportunities in the context of our vision, key objectives, the healthcare environment and our stakeholders.

- **Set the scope**. Determining the scope identifies what you are assessing, for example, is it a new infrastructure project, new ICT system implementation, or an operational risk event such as Harm to a Person?
- **Define the objectives**. Identify the reason for the risk assessment (a change in law or regulation, a request from the Department of Health, HIQA or other regulators, on foot of an internal or external audit report, implementing best practice or an operational change or review)
- **Identify the relevant stakeholders**. Identify the areas that are, or might be, impacted and seek their input. The aim is to have a complete inclusive process from the beginning.
- **Gather background information**. Having the correct information is key. Ask the right people and identify the available information.

Consider:

- Corporate and National Service Plans.
- Division/Hospital Group/CHO/Area Plans.
- Previous events, investigations, or reports.
- Internal or External Audit Reports.
- Subject Matter Expert Reports (Occupational Health & Safety, General Data Protection Regulation (GDPR), etc.).
- Controls Assurance Review Process (CARP).
- Protected Disclosures reports.
- Risk assessments undertaken as part of any strategy development i.e. the Government's National Risk assessment.

3.1 Procedure: Risk Identification

Identify the risks and/or opportunities that might have an impact on the objectives of the organisation.

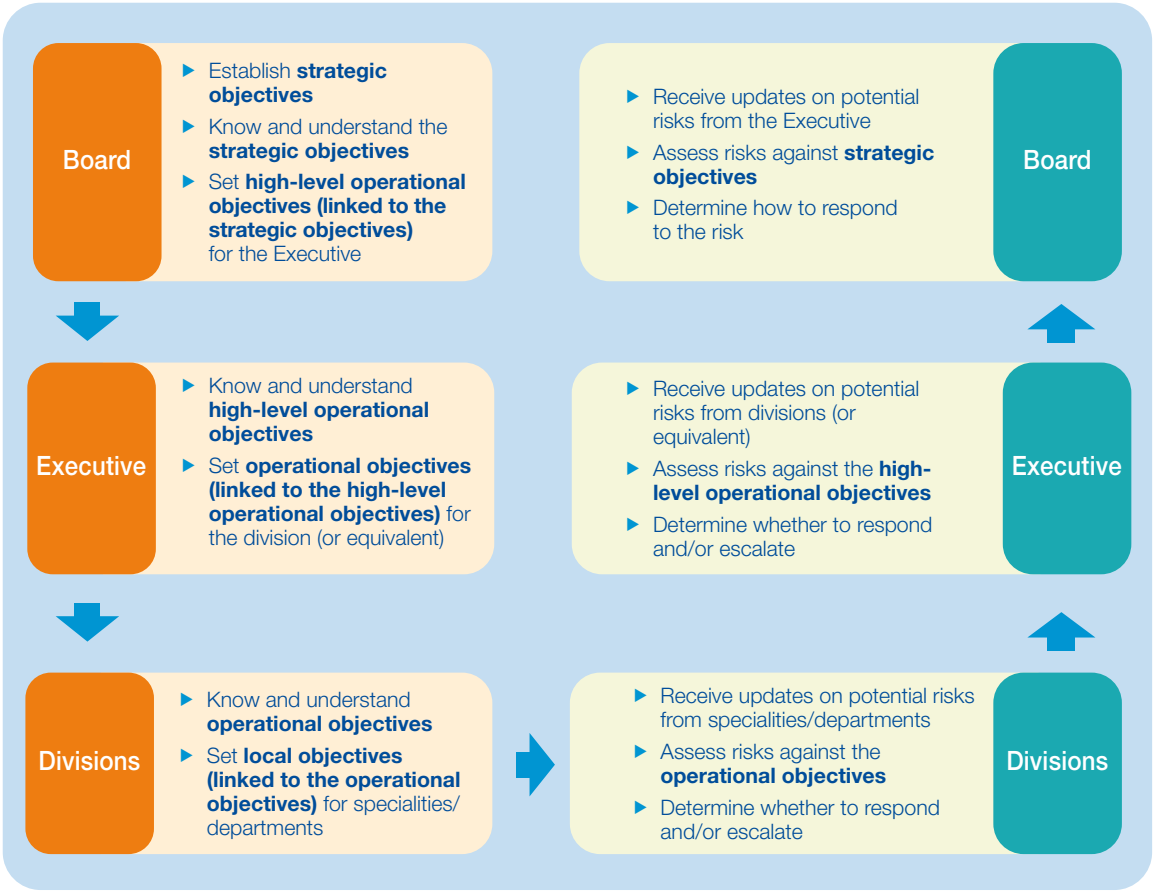
There can be several approaches to identifying the risk, areas of impact, events, their causes, and potential impact. You should also aim to identify the results associated with not pursuing an opportunity, that is, the risk of doing nothing and missing an opportunity. The HSE uses a combination of top-down and bottom-up risk assessments for this.

A **bottom-up risk assessment** process concerns risk assessments that are undertaken by individual members of staff and local departmental management.

A **top-down risk assessment** process concerns risk assessments that are undertaken by a board of directors, EMT, or senior leaders as a top-down exercise.

The process of setting **objectives**, aligning them at strategic/operational and local levels, and then assessing the risks to those objectives, is iterative. This includes how the assessment of risks informs the decision-making process and how the identification, communication, notification and escalation of potential risks should be carried out and is illustrated in Figure 5.

Figure 5: Iterative process of assessing risks to objectives[3]



In identifying the risk, it is useful to consider the following four key elements such as **Anticipate**, **Vigilance**, **Respond**, and **Learn and Improve**.

3 360_GGI_Assurance_Framework_guidance.pdf (360assurance.co.uk)

Anticipate: Anticipation involves thinking ahead and envisioning the things that are most likely to contribute to a risk event.

- **What could happen?** What could result in harm and how can you prevent it occurring?

What might go wrong, or what might prevent the achievement of the relevant goals? What events or occurrences could threaten the intended outcomes?

Vigilance: Vigilance refers to the heightened sense of risk awareness that you need to adopt and encourage within the workplace.

- **How could it happen?** Are you and your staff alert to the potential of harm occurring within your workplace? Is the risk likely to occur anywhere or in any environment/place? Or is it a risk that is dependent on the location, physical area, time or activity?
- **Why might it happen?** What causes would need to be present for the risk event to happen or occur again? Understanding why a risk might occur or be repeated is important if the risk is to be managed.
- **What might the impact be?** If the risk were to materialise, what impact would this have? Will the impact be felt locally, or will it impact the whole organisation? Areas of impact to consider include:
  - Harm to a person (Service User, Patient, Staff & Public)
  - Service User Experience
  - Business/Service disruption/Security (unauthorised and/or inappropriate access to systems/assets including data)
  - Loss of trust/confidence or morale (Public/Staff)
  - Organisational objectives or outcomes
  - Compliance (Legislative, Policy, Regulatory including data)
  - Financial (including performance to budget, claims etc.)
  - Environmental/Infrastructure/Equipment
  - Strategic Programme/Project (long term objectives/timeframes)
- **Who does or can influence this activity?** How much is within the HSE's control? Ensure Line Managers are informed if not actively involved. See section 'Communication and Consultation' for more details.

Respond: Risk management is about anticipating what might go wrong and putting in place systems and processes to prevent this or mitigate the impact. Information from data relating to events that occur is one critical source of risk information.

Learn and improve: Within your Division/Hospital Group/CHO/area, there will be a wealth of existing information and intelligence, gathered formally and informally. By combining information from different sources you can often get a sense of possible risk events. We aim to learn and improve to prevent recurrence of risk events.

Useful tool: Table 2 below can be used in establishing relevant sources and approaches to the identification of risks. The sources of information, where possible, should be the most recent version available for review. This document includes further guidance on some of the approaches to identifying risk.

Table 2: Sources and Approaches for Identifying Risks

Potential Sources of Information	
Risk Registers	Complaints/Surveys/Investigation Reports
Internal and External Audit Reports	Incident/Near Miss Tracking and Trending
Press	Incident Review Reports
Reviews	Non-conformance reports/performance reports
Policies, Procedures, Protocols and Guidelines	
Examples of Approaches to Identifying Risks	
PESTLE analysis	Benchmarking
Bow-tie Analysis	Meetings/committees
Risk assessment workshops	Data Protection Impact Assessment
Brainstorming	Horizon Scanning
Questionnaires/Surveys	

3.2 Procedure: Risk Description

An accurate and specific **risk description** will assist you in identifying what needs to be in place to manage the risk whereas a vague or poorly defined risk will leave you grappling at the next step in the process. The risk description is a structured statement of risk usually containing three elements: risk event, cause and impact.

So when developing the risk description, take your time and ask yourself *'What is the risk (possible future event/threat) that if it were to materialise could delay or prevent me from achieving my objective?'*

The three components of a good risk description are:

- the **risk event** that could threaten an objective being achieved;
- the **cause of the risk**;
- the **impact** or consequence of that risk.

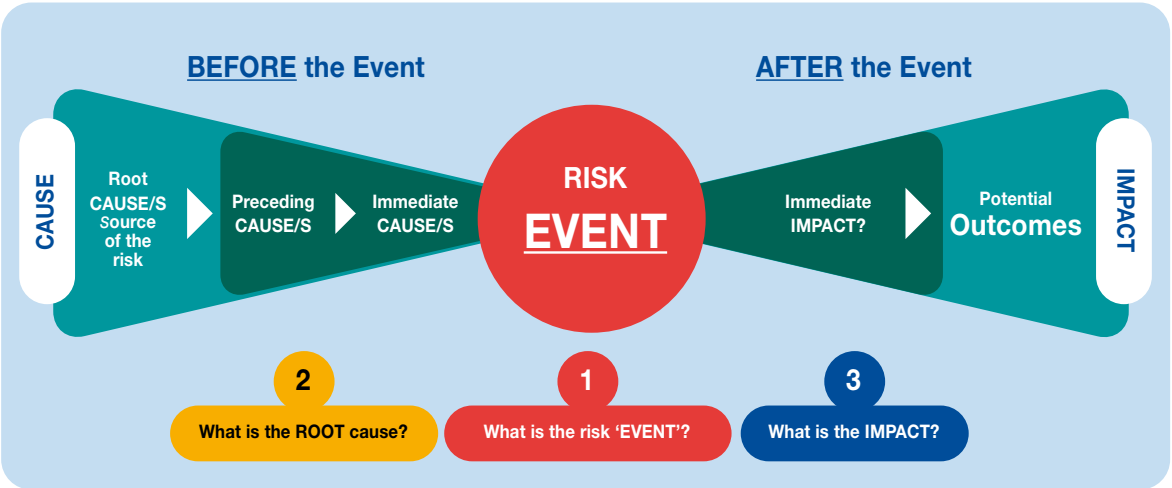
It is the predicted risk that becomes '**an event**' when it occurs. That is, it is a tangible event, you experience it or feel it. Before COVID-19, the predicted 'risk event' (or threat) was of 'a pandemic'. With the arrival of COVID-19 in 2020 it very much became a reality, the predicted future risk event of a pandemic materialised. Similarly, the potential future threat of a cyber-attack became a tangible reality with the attack on the HSE's systems in 2021. The table below may be used to break down the component parts and structure a risk description.

Table 3: Template for components of a risk description

Components of a risk description			
	Risk Event	**Cause of the Risk**	**Impact or Consequence**
What it means	The occurrence whereby we know we have moved from a theoretical risk to one that has materialised (e.g. Risk of a pandemic to arrival of COVID-19; risk of cyber-attack to occurrence of cyber-attack)	Understanding the likely cause(s) of risk is essential to deciding on whether removing the cause of risk will remove the risk or whether controls need to be applied to reduce or mitigate the risk.	Understanding the potential impact(s) or consequences of a risk materialising is essential when considering how we respond to the risk event.
Expressed as…	There is a risk of/to/that (event)….	… due to (cause),	… resulting in (impact/ consequence)
Template components of a risk description **Risk Description = Risk Event + Cause (Source) + Impact (Consequence).**			
Capture	Capture and describe the **risk event** *This should be a tangible event, you experience it or feel it e.g. pandemic/cyber-attack*		
	Capture and describe the **cause(s) (source)** *Consider using the '5 Whys' method, outlined in Section 3.14, to determine the root cause, rather than a presenting cause, to provide a focus to treatment plans*		
	Capture and describe the **impact(s) (consequence)** *What impact will this have on your objectives?*		
Collate	Collate into your **risk description** using the formula below: *There is a risk of/to/that (risk event)……due to (cause of risk)……resulting in (impact)*		
Result	***There is the risk*** *of a cyber-attack* ***due to*** *poor access controls* ***resulting in*** *potential breach of data*		

The elements of a risk are illustrated in Figure 6 below.

Figure 6: Components of a Risk



Another example is provided below;

> Some may say that healthcare-acquired infection is a risk. Whereas that goes part of the way to describing the risk, it is somewhat vague and does not target the core of exactly what the risk is.
>
> If however the risk is described as 'There is a risk of acquiring an infection associated with receiving healthcare due to poor infection prevention and control practices resulting in harm to patients, service users or staff' then we can start to see what needs to be targeted (i.e. poor infection prevention and control practices).
>
> The question then becomes what should be in place to improve infection prevention and control practices to avoid healthcare-acquired infection and what is in place?

3.3 Procedure: Risk Analysis (including Risk Rating)

Now that we have identified and described the risk, we analyse it in order to develop a detailed understanding of the risk.

This analysis is important for separating low risks from high ones. Once the risk has been identified and the context, causes, and impacts/consequences have been described, we look at the strengths and weaknesses of existing systems and processes designed to help control the risk.

3.3.1 Rating a Risk

Risk is measured in terms of two dimensions, likelihood and impact i.e., the likelihood (probability/frequency) of the risk occurring and the impact (consequence) of the risk should it occur. In rating the risk it is important to understand both the impact of a risk event and the likelihood of the risk event occurring. This will inform the approach you take to controlling the risk. It may be possible to reduce one or both the likelihood and impact of a risk event.

The process for rating risk is:

1) Using the **Likelihood Table**, see Appendix 2, identify and assign the **likelihood** score of the risk occurring on a scale of 1 to 5; and
2) Using the **Risk Impact Table**, see Appendix 2, 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**, see Appendix 2, align the score to a risk rating of High, Medium or Low.

The HSE has adopted a standardised approach to the assignment of likelihood and impact scores for the rating of the risk. The **Risk Assessment Tool**, see Appendix 2, includes the Risk Impact Table, Likelihood Table, Risk Scoring Matrix, and Risk Rating Matrix. This tool should be applied uniformly to all processes where a risk assessment is required to be rated.

The assessment of likelihood and impact is in some cases subjective but should be assessed by relevant managers and subject matter experts to reduce the level of subjectivity. Preferably, where it is available, independent data to support your assessment should be used. This can include performance data, incident data, internal and external audit reports, inspections, surveys, and a range of other available internal and external information.

As previously stated it is not intended that this tool replace the risk assessment process used in specific Health & Safety, clinical or care risk assessments, for example, falls, pressure ulcer, etc., as the outcome of the application of those specific assessments supports clinical decision-making about the individual Service User and/or care planning process.

3.3.1.1 Likelihood of a Risk

Likelihood is the chance of something happening and is determined by the probability of occurrence or potential frequency. The HSE's Likelihood Table is provided in Appendix 2 and is shown in Table 4 below.

To start with, ask yourself how likely is the risk to occur? How frequently has this occurred previously in our service? Then, using the Likelihood Table in Appendix 2, assign a score of 1 to 5.

A **1** would indicate that the risk has less than a 5% probability of occurring or would occur once in 5 years.

Conversely, a **5** would indicate that the risk has a greater than 90% probability of occurrence or at least a monthly occurrence.

Table 4: Likelihood Table

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

The likelihood level of 1 to 5, is based on the expertise, knowledge, and experience of the person/group scoring the likelihood. It is those competencies that will inform the decision as to the aspect that is most appropriate to use e.g. the probability of the risk occurring or the frequency of occurrence.

Either of the dimensions (probability or frequency) can be used when determining the likelihood score as it will be dependent on which is most appropriate. For example, when determining the likelihood of a pandemic, the probability could be a **5**, that is **>90%** (Almost Certain) however the frequency would be **1 in 5 years** (Rare).

3.3.1.1.1 Alternative Likelihood of a Risk (Event/Case Occurrence)

As set out above, there are a number of factors that will inform the decision as to the likelihood of a risk, with Table 4 above providing the guidance in relation to scoring based on the probability or frequency.

An alternative option to consider when determining the likelihood of a risk is the level of event or case occurrence. Table 5 below includes the details of scoring from 1-5 against each level of this occurrence and as above, this score is based on the expertise, knowledge, and experience of the person/group scoring the likelihood.

Table 5: Event/Case Occurrence

Score	Likelihood	Event/Case Occurrence* **Event** (per Acute Hospital Admissions/Completed Episode of Care) **Case** (Incident)
5	**Almost Certain**	1 or more in 10
4	**Likely**	1 in 100
3	**Possible**	1 in 1,000
2	**Unlikely**	1 in 10,000
1	**Rare**	1 in 100,000 or more

* *Per Annum.*

3.3.1.2 Impact of a Risk

The HSE has identified several risk impact categories to be managed which are detailed in the **HSE Risk Impact Table**, Appendix 2. A list and description of these areas are provided in Table 6 below.

There are **two stages to assigning an impact score**, the first is to decide on the primary impact category, and the second is to assign a score of 1 to 5 from the impact table, see the HSE's Risk Assessment Tool (See Appendix 2).

3.3.1.2.1 Stage 1: Identify Primary Category of Impact

To start with, **only one impact category should be chosen as the primary category**, even though a risk may impact a number of the categories listed. For example a risk that relates to *Harm to a Person* may also result in poor *Service User Experience* and the *Loss of trust/confidence or morale*, but if the physical harm was prevented the latter two impacts would not have occurred. Therefore, the primary impact will be Harm to a Person. Other areas in which the risk impacts are known as secondary impacts. The selection of a primary category will become important when it comes to assessing the risk.

Table 6: Impact Category and Description

Impact Categories	Description
Harm to a person (Service User, Patient, Staff & Public)	Physical or psychological injury related to a person, i.e. service user, staff member, or member of the public.
Service User Experience	Negative service user experience that may have a negative impact on the outcome, limit their engagement with a service, or lead to a complaint.
Business/Service disruption/Security (unauthorised and/or inappropriate access to systems/assets including data)	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.
Loss of trust/confidence or morale (Public/Staff)	Adverse publicity in the media, loss of public/staff confidence in a service or the organisation, e.g. poor service performance.
Organisational objectives or outcomes	Slippage in the achievement of organisational objective/ outcome i.e. not delivering on a key objective.
Compliance Requirements (Legislative, Policy, Regulatory including data)	Failure to comply with HIQA/Mental Health Commission (MHC) standards, Codes of Practice or Conduct set by the Department of Health, DPER, and/or professional regulators, relevant legislation, e.g. Safety, Health and Welfare at Work Act, Financial Regulations, GDPR, Policies, Procedures, Protocols and Guidelines (PPPGs) etc.
Financial, including performance to budget, claims, etc.	Variance to budget (relevant to area being risk assessed), fraud, fines and claims.
Environmental/Infrastructure/ Equipment	Releases of substances that would have a detrimental environmental impact, e.g. chemical spills, poor waste management practices, and radiation leaks. Damage to infrastructure or key equipment.
Strategic Programme/Project (Objectives/timeframes) – HSE Executive Use Only	Strategic Programme/Project scope or quality slippage. Project delays.

3.3.1.2.2 Stage 2: Assign an Impact Score

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 in Appendix 2, 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. The Impact Table is shown in Appendix 2.

3.3.1.3 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

Using the **HSE Risk Scoring Matrix** (Appendix 2) shown in Figure 7 below we can plot the likelihood and impact levels and determine whether the risk score is 1-5 (green), 6-12 (amber) or 15-25 (red).

Figure 7: HSE Risk Scoring Matrix

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

IMPACT

3.3.1.4 How to get a Risk Rating?

Now with the risk score to hand, as can be seen from the **HSE Risk Rating Matrix** (Appendix 2) 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.

Figure 8: HSE Risk Rating Matrix

LIKELIHOOD	Negligible	Minor	Moderate	Major	Extreme
Almost Certain	Low	Medium	High	High	High
Likely	Low	Medium	Medium	High	High
Possible	Low	Medium	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Low	Low	Low

IMPACT

We now look at the levels of risk, which involves the follow:

- Rate the risk at an **inherent level**
- Assess controls
- Rate the risk at a **residual level**
- Detail the treatment option (controls and actions)
- Set a **target risk level**

It is recognised that both initial and current risk, as defined above, are in use at the time of this update when assessing and reporting on risks using the Generic Risk Assessment Form 2018 (Word document) and HSE Excel Risk Register v4 Mar 2018 (Excel document) available on the HSE internet.

The terms Inherent, Residual and Target are introduced in this update of the policy and are for use, in line with the guidance, subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

When determining the level of risk rating, we start with the **inherent risk level**, which is the rating to reflect what activity or event would pose if no controls or other mitigating factors were in place.

3.3.2 Inherent Risk Level

Inherent risk in the HSE is the level of risk before consideration of control and/or action measures.

To do this;

- **Assess and assign the likelihood score** from the most appropriate dimension used for likelihood of a risk, that is, probability **or** frequency (See Appendix 2).

  Assign a likelihood score of 1-5.

Likelihood Score	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost Certain

- **Identify the primary impact category** should the event occur (See Appendix 2).
- **Assess and assign the impact score** (See Appendix 2) of 1-5.

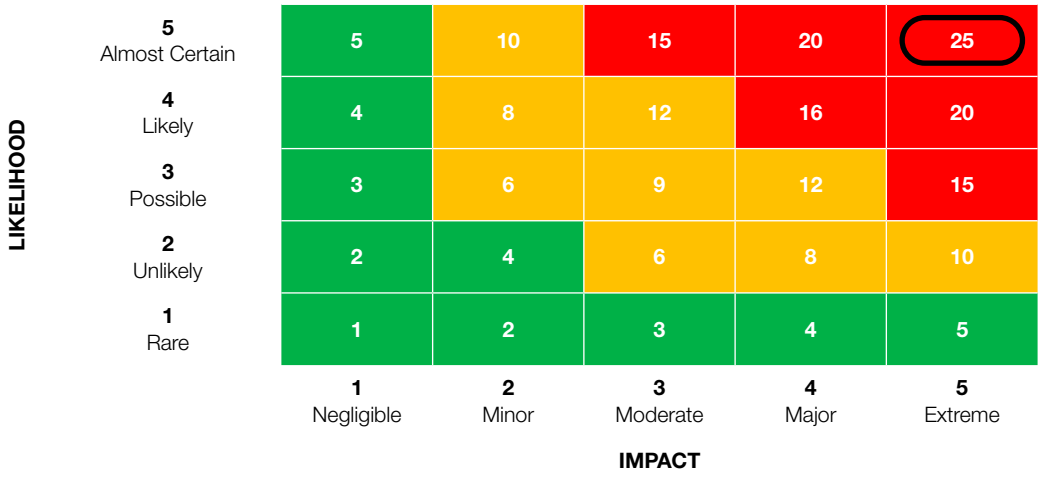
Impact Score	1	2	3	4	5
	Negligible	Minor	Moderate	Major	Extreme

- **Multiply the likelihood score by the impact score** to give the inherent risk score.

  Risk Score = Likelihood score x Impact score

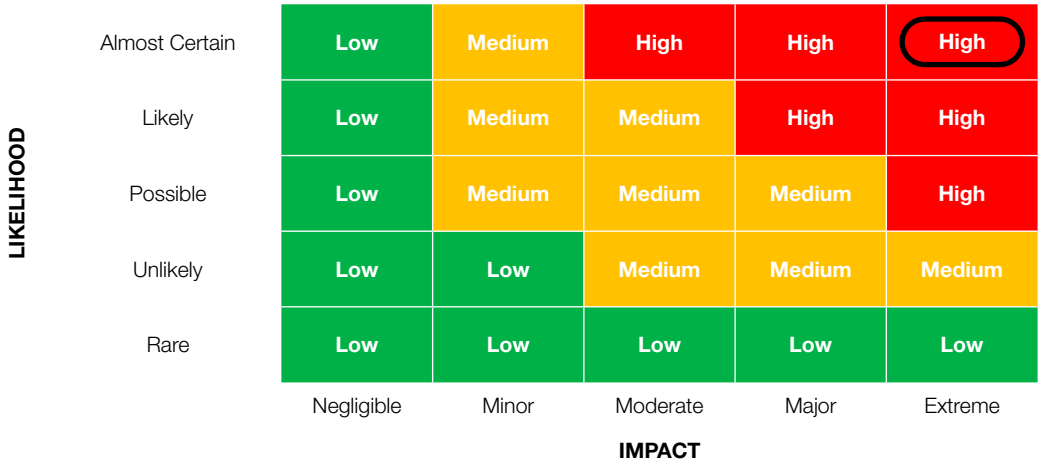
For example, if a risk has been assigned a likelihood score of **5** (Almost Certain) and an impact score of **5** (Extreme) the inherent risk score will be **25**. See below the result plotted on the HSE's Risk Scoring Matrix in Figure 9.

Figure 9: Inherent Risk Rating plotted on the HSE Risk Scoring Matrix



- **Plot** the risk score onto the HSE Risk Rating Matrix, which shows an inherent risk rating of 'High'. See below the result plotted on the HSE's Risk Rating Matrix in Figure 10.

Figure 10: HSE Risk Rating Matrix



As stated above, the use of inherent risk level has been introduced in this update and will be required subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

3.3.3 How to Identify Controls and Actions that should be in place?

You may have analysed the risk and determined the rating, prior to any measures (controls or actions) being undertaken, the next question is:

"If we were to prevent this risk from occurring, what would we need to have in place to reduce its likelihood of occurring or to minimise its impact if it was to occur?"

Though the risk description may outline a substantial risk there can be measures (controls and actions) in place that may serve to significantly reduce the likelihood or impact of the risk recurring.

Such measures may include:

- Policy, Procedure, Protocol, Guidelines and committee oversight, etc.
- Education and training relating to the skills and knowledge required by staff to manage the risk.
- Equipment and resources.
- Physical environment.
- Processes and systems such as tools and checklists, communication (for example formal handovers, use of ISBAR3 (Recommendation/Readback/Risk), documentation, etc.
- Monitoring measures, for example, audit.

In risk terms, a control is a measure that maintains and/or modifies a risk, that is, an existing activity that is currently in place to reduce either the likelihood or impact of the risk.

A definition of a control is provided below.

Controls are a measure that maintains and/or modifies risk. Controls include but are not limited to, any process, policy, device, practice, or other conditions and/or actions 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.

An action is a measure that is yet to be completed, though is planned in order to further reduce the likelihood or impact of a risk.

A definition of an action is provided below.

Actions are a future measure that will maintain and/or modify a risk. In the HSE an action is a future measure to further reduce either the likelihood or impact of a risk.

Simply put, if the measure is in place, completed, and reduces the likelihood or impact of the risk, it is a **control**. It is important that controls are specific, verifiable, and operating effectively.

If for any reason, the activity is not yet in place, is planned to be in place, or would cumulatively as part of a broader work programme impact on the likelihood or impact of the risk, it would be deemed an **action**.

A template to help identify the controls that should be in place and action plans to be put in place, is available at: Risk Management Support Tools – HSE.ie. To complete the template, start listing all the controls required to manage the risk against each identified risk. When you have completed your list, go through it, and opposite each item tick one of the three columns as follows:

- **YES** – the item is in place. This item is a control.
- **NO** – the item is not in place. This item is an action and will form part of the action plan.

  YES but… – the item is partly but not fully in place. This item is part of the action plan until fully in place and verifiable.

3.3.4 Effectiveness of Controls

Controls can be broadly grouped into four types. Two types of control, **Preventative** and **Directive** are put in place before the risk materialises and would be considered proactive controls. The further two types are **Detective** and **Corrective** (which are closely linked) and focus on what happens after the risk occurs or which identify weaknesses in our current controls, these are reactive controls.

In general, proactive controls would be seen as more effective than reactive controls.

Examples of each type are provided below.

3.3.4.1 Proactive Controls

Preventative controls are controls designed to stop, discourage, pre-empt or limit the possibility of an undesirable event before it occurs. These controls act to address the root cause of a risk and thus prevent the risk event from occurring in the first place. These can be, for example, automated processes, formal written approval processes, dual authorisation for certain high risk activities, the use of personal protective equipment, physical security, segregation of duties and computer passwords.

Preventative controls would be regarded as the strongest form of controls.

Directive controls give direction. These can be, for example, statutory obligations, regulatory standards including professional standards, or other organisational requirements or instructions, many of which are converted into policies, procedures, circulars, standard operating procedures and training.

Directive controls can however, be weak controls, as while they state the practice to be followed, of themselves, they do not prevent poor practice from occurring.

3.3.4.2 Reactive Controls

Detective controls are designed to search for and identify errors or undesirable events after they have occurred so that corrective actions can be taken. For example, detective controls aim to identify a breach after the event. Examples include internal audits, clinical audits, regulatory reports, incident reviews, monitoring information from reporting systems including incident reporting, performance reports, financial reporting, financial reviews, and complaints data.

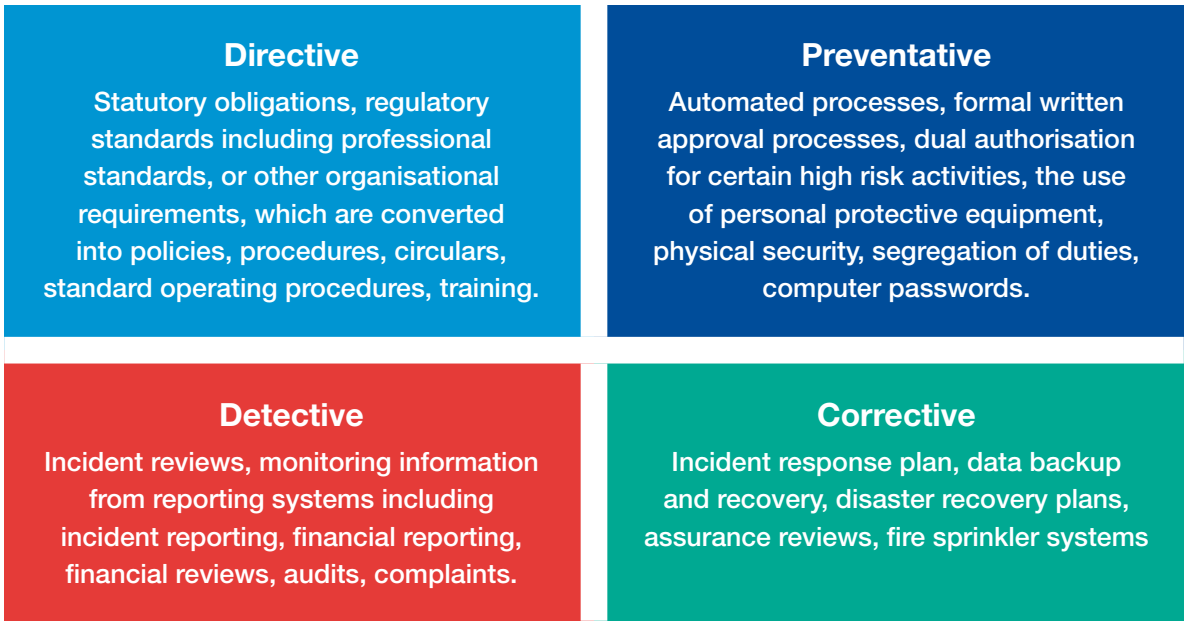
Detective controls can identify important corrective actions that need to be taken.

Corrective controls are designed to correct errors or undesirable events which have occurred and will prevent further occurrences. For example, corrective controls are put in place after a breach, system failure or weakness, or other gap is identified.

Once these new controls are put in place, they can become a **directive** or **preventative** control.

Figure 11 illustrates examples of controls that can be adopted as directive, preventative, detective or corrective.

Figure 11: Types of Controls



3.3.5 Residual Risk Level

So, next is the residual risk level. In rating the residual risk you must only consider the controls that are in place, i.e. the existing controls.

Residual risk in the HSE is the level of risk remaining after consideration of existing controls.

Considering **the existing controls that are in place**, we;

- **Assess and assign the likelihood score** from the most appropriate dimension used for likelihood of a risk, that is, probability **or** frequency (See Appendix 2).

  Assign a likelihood score of 1-5.

Likelihood Score	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost Certain

- **Assess and assign the impact score** (See Appendix 2). Having identified the most realistic primary impact category above. Assign an impact score of 1-5.

Impact Score	1	2	3	4	5
	Negligible	Minor	Moderate	Major	Extreme

- **Multiply the likelihood score by the impact score** to give the residual risk score.

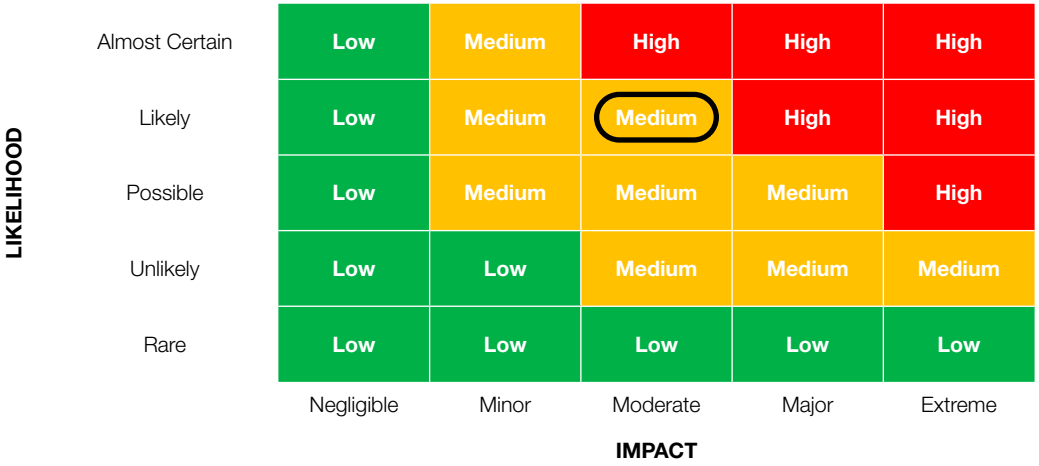
  Risk Score = Likelihood score x Impact score

Using the HSE's Risk Scoring Matrix (See Appendix 2), we can plot the likelihood and impact result and determine whether the risk score is green, amber, or red. Figure 12 below shows the result if a risk has been assigned a likelihood score of **4** (Likely) and an impact score of **3** (Moderate).

Figure 12: Residual Risk Rating plotted on the HSE Risk Scoring Matrix

- **Plot** the risk score onto the HSE Risk Rating Matrix, which shows a residual risk rating of **Medium**. See below the result plotted on the HSE's Risk Rating Matrix in Figure 13.

Figure 13: HSE Risk Rating Matrix



If the residual risk still remains at a high or medium level, further controls or actions should be considered and a plan developed of these activities to further reduce the likelihood or impact of the risk.

The Risk Owner should set the target risk level having given consideration to the resources and timeframes to achieve these.

As stated above, the use of residual risk level has been introduced in this update and will be required subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

3.3.6 Target Risk Level

Target risk in the HSE is the planned level of risk after consideration of both control and action measures. If the desired target is lower than the residual risk rating, additional actions will be required to reduce the likelihood or impact of the risk to within the desired target level or appetite. If this is the case, and the residual risk rating is above the target risk rating there should be an agreed, realistic timeframe set out to achieve the target rating.

When establishing a realistic timeframe for delivery of the desired level of risk rating, an **interim target** risk rating can be set. The interim ratings can be agreed over several periods of the lifecycle or existence of the risk i.e. the first assessment of a risk could result in a target rating to be set at **12** for that year end, with a further reduction considered, for the same risk, of **10** in the following year.

As before, **taking into account the controls that are in place and now further actions that will be required** we;

- **Assess and assign the likelihood score** from the most appropriate dimension used for likelihood of a risk, that is, probability **or** frequency (See Appendix 2).

  Assign a likelihood score of 1-5.

Likelihood Score	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost Certain

- **Assess and assign the impact score** (See Appendix 2). Having selected the primary impact category above. Assign an impact score of 1-5.

Impact Score	1	2	3	4	5
	Negligible	Minor	Moderate	Major	Extreme

- **Multiply the likelihood score by the impact score** to give the target risk rate

  Risk Score = Likelihood score x Impact score

- **Plot** the risk score onto the HSE Risk Rating Matrix, which will show the target risk rating to be achieved.

Provided below is a case study example that outlines the use of Inherent, Residual and Target risk ratings.

As stated above, the use of target risk level has been introduced in this update and will be required subsequent to the availability of online/in-person training and updated Word and Excel forms or with the deployment and access to an online risk information system to your service/area.

Case study example of Risk Management in everyday practice

Inherent, residual and target levels can be explained through the use of a risk, outlined below, which is *"if there was a similar pandemic to COVID there is a risk of a significant additional pressure on the health sector resulting in an inability to provide services"*

To start, the inherent risk level in the HSE is the level of risk before consideration of control and/or action measures. For example, the inherent risk score could be assessed as a likelihood score of **4** or **Likely** with an impact score of **4** or **Major**.

This would give an inherent risk score of **16**, which is an inherent risk rating of **High**.

The residual risk level in the HSE is the level of risk remaining after consideration of existing controls. Controls may reduce the likelihood or impact of the risk.

In this case, the HSE may have no ability to reduce the likelihood of a pandemic occurring and therefore its focus will be on reducing the impact of the risk.

Controls that could be considered to modify the impact of additional pressures would include:

- increasing ICU capacity;
- redeployment of healthcare staff;
- advance sourcing and procuring of sufficient Personal Protective Equipment;
- increasing public communications;
- infection prevention and control measures;
- screening and streaming of infected/exposed/non-infected/exposed patients;
- physical distancing;
- compulsory mask wearing; and
- restricted visitor access to healthcare facilities.

The residual risk score could then be assessed, as remaining at **4** or **Likely**. From the control measures taken above this would result in a reduction in the impact from the score of 4 above to an impact score of **3** or **Moderate**.

This would give a residual risk score of **12**, which is a residual risk rating of **Medium**.

The target risk level in the HSE is the planned level of risk after consideration of both control and action measures.

The target risk score, based on the consideration of what would be an acceptable level of risk, can potentially be set at a lower level than the residual risk score. If so, then further actions will need to be undertaken to reduce the residual rating to the lower target risk rating.

In this example, the actions to be undertaken to further reduce the risk of additional pressure could include:

- introduction of a vaccination system
- expanding the test and trace system.

The target risk score could then be assessed, retaining the likelihood score of **4** or Likely. With the above actions, there would be a change in the impact score to **2** or **Minor**.

This would give a target risk score of **8**, which is a target risk rating of **Medium**.

3.4 Procedure: 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.

A risk assessed as being high is likely that you as Risk Owner will need to ensure that actions required to reduce the risk are identified and implemented. Risk evaluation allows you to look at the totality of risks assessed and to prioritise these in terms of which risks require the most urgent action or treatment.

Upon assessing the risks you may decide to place greater management focus on risks rated as high and less focus on risks which have a lower rating. Such decision-making should not be guided solely by the rating of the risk but rather the rating of a risk should inform decision-making.

> At national or Senior Management level, risks to the strategic objectives of the organisation are considered against the Risk Appetite Statement to determine what requirements are needed to address those risks and to bring them within appetite. At a regional, service, or individual unit level, the risks to the objectives or goals would be assessed against the desired target risk rating.

Therefore, when evaluating a risk;

- If the residual risk rating is not acceptable or tolerable or if the desired target risk rating is different from the residual risk then the risk should be treated as set out in the procedure for Risk Treatment.
- A risk could be acceptable in the following circumstances:
  - No treatment is available.
  - Treatment costs are prohibitive (particularly relevant with low rated risks)
  - The level of risk is low and does not warrant using resources to treat.
  - The opportunities involved significantly outweigh the threats.

A further mechanism to evaluate a risk is to determine its risk velocity.

3.4.1 Risk Velocity

Understanding risk velocity can also be a helpful way to consider risk. Risk velocity refers to how fast a risk may affect an organisation. Certain risks will have an immediate risk velocity such as an IT system outage following a significant security failure. Others may have a slower velocity.

Table 7 below outlines the Risk Velocity Assessment Criteria which is an option that may be used to focus management efforts and develop targeted response plans for highly rated risks that also would be assessed as having a ‘High’ velocity measure.

Risk velocity maybe used to rank risks, in particular where you have risks with the same rating. A high velocity risk would rank above a low velocity risk.

As part of the ongoing monitoring and assessment of risks, it can be beneficial to periodically monitor risk velocity. This is in acknowledgement of the fast-changing landscape for some risks, with a knock-on effect on the timeframes between a risk materialising and its impact and time sensitivity for a response.

Table 7: Risk Velocity Assessment Criteria

Velocity Measure	High	Medium	Low
Time to Impact	Risk impact will be felt **in less than one month** after the occurrence.	Risk impact will be felt **within 1 to 3 months** after the occurrence.	Risk impact will be **felt more than 3 months after the** occurrence.
Reaction Time	There will be **very little or no time for reaction and response** planning before consequences of the risk materialise.	There will be **limited time for reaction and response** planning before consequences of the risk materialise.	There **will be time for reaction and response** planning before the consequences of the risk materialise.

3.4.2 Evaluation Response

The purpose of risk evaluation is to allow you to look at the totality of assessed risks, prioritising them and identifying which risks require additional action(s). Table 8 can be used as a guide when considering the prioritisation of action plans.

Table 8: Risk Evaluation Criteria

Risk Evaluation		
Risk Rating	**Acceptable/ Not acceptable**	**Action**
High (Red)	Not acceptable	Where it is not possible to terminate or transfer the risk, a treatment plan should be developed and the actions required assigned to action owners and their completion should be monitored by the relevant Management Team.
Medium (Amber)	Acceptable/ Not acceptable	Such risks require consideration by the Management Team. It may be that a decision is to take risk treatment options [Reduce, Avoid or Transfer] or to accept the risk but keep it under review [monitor] with an option to open it for further management in the future.
Low (Green)	Acceptable	Such risks require no further action or can be managed by an appropriate person or department. Quarterly monitoring, review, and/or testing of controls will be in place to ensure that controls remain effective to manage the risk.

3.5 Procedure: Risk Treatment

Risk treatment is the process to modify risk. The type of risk treatment chosen will often depend on the nature of the risk and the desired target rating for that risk. One way to determine this is to ask the question '*What is the aim of our treatment of this particular risk?*'.

This could be to avoid/terminate, accept, transfer or reduce the risk as set out below:

- **Avoid/Terminate** it completely e.g. do not proceed with the planned activity.
- **Accept** the level of risk based on existing information e.g. pursue the opportunity.
- **Transfer the risk** e.g. to an identified individual or unit, that has been communicated to and notified, where many of the actions identified as required to mitigate are better managed and are within their span of control. (See Communication and Consultation for notification of risk).
- **Reduce** the risk with further actions.

When we treat a risk, it is to ensure that there are **treatment plans** in place, which detail both action and effective control plans, to minimise the likelihood and impact of the identified risk.

3.5.1 Development of a Treatment Plan

The development of a treatment plan aims to reduce the likelihood or impact of the risk and achieve the desired target risk rating. When developing the treatment plan, it is important to work out what kind of treatment is desirable for the risk.

Once the treatment has been identified, a treatment plan should be prepared and documented. Treatment plans should identify responsibilities for Action Owners and detail actions, timeframes for implementation, budget requirements or resource implications, and proposed dates of review. Treatment plans should also set out responsibilities for Control Owners, where appropriate.

3.5.1.1 Assigning Actions to Action Owners

As risk management is a line management responsibility the manager responsible for the risk has three options for assigning owners to actions relating to risks on their register. These options are as follows:

- To themselves as the Line Manager
- To someone who reports to them (i.e. a member of their team)
- To the person, the manager reports to (i.e. their Line Manager)

To complete the action the Action Owner may need to involve or consult with others. However, in order to monitor the action one person must have lead responsibility.

3.5.1.2 Agree Due Dates with Action Owners

Assignment of due dates for actions should be in discussion and agreement with the Action Owner. This allows for consideration of what is a reasonable timeframe given that the manager and Action Owner need to consider the totality of work assigned to the Action Owner and depending on the criticality of the completion of the action, workload prioritisation may be required.

3.5.1.3 Implement Agreed Risk Treatment

Once any options requiring authorisation for resourcing, funding, or other actions have been approved, the risk treatment should be implemented. The Risk Owner assigned with the primary responsibility for the risk is ultimately accountable for the treatment of the risk.

It is acknowledged, while all possible measures should be taken to reduce or eliminate risk, it may not be possible to complete all actions identified as required. This may be due to resources or other constraints. What is important however is that as the Risk Owner, you have acted to minimise risk concerning any actions required that are within your direct control and that you have communicated appropriately the actions that lie outside of your control. In circumstances where you can provide evidence that this has occurred, you have fulfilled your responsibility to your manager (i.e. you cannot be held accountable for aspects of the risk which lie outside your control).

There can be circumstances, where a risk, when rated, could be determined to remain outside of the desired target level of risk, which is the risk retains a higher residual risk rating, above the target risk rating. This may be acceptable if in compliance with the HSE's core corporate governance and decision-making processes. However, should that occur, there needs to be a clear response plan in place, in case the potential risk is realised. That is, a plan that sets out the course of action to respond effectively should the risk materialise.

3.6 Procedure: Recording and Reporting

Managers rely on a standard suite of reports to provide critical insights into how their area of responsibility is performing and which inform the decisions they have to make (e.g. Performance Reports, Financial Reports). In the same way, they also rely on a risk register that brings together in a summary form, all the essential information relating to all of the risks being managed. This includes, a clear description of the risk, the measures that are in place to control the risk, the additional actions required to further reduce the risk and the measurement of the level of threat.

The establishment of your service's risk context and clarifying your objectives sets the scene for identifying key risks to be managed. Keeping these in mind, consider what you know about where your key areas of risk may be. Risks identified which do not require a formal management plan, for example, where the management of risk requires the supervision of staff, or assurance in relation to the systems already in place, do not need to be included on the relevant risk register.

3.6.1 Documenting your Risk Assessment

Risk assessments should be documented on the Risk Assessment Form available at: Risk Management Support Tools – HSE.ie. At this point you will have completed the risk assessment and have all the information required to enter it onto the risk register.

Risks assessed and managed at an individual ward/unit or single residential unit or committee are to be maintained for reference by staff using that place of work. The manager should then determine which of these assessed risks need to be recorded on the risk register at Service or Corporate level.

3.6.2 What is the Process for Entering the Risk Assessment onto the Risk Register?

A question that is often asked is '*Is it necessary to enter all assessed risks onto the register?*'

Risks included in the risk register should be at a relatively high level and aggregated where possible (for example, hospital-acquired infections versus separate risks for different types of infections). This means that the focus is on a limited number of key risks which if managed appropriately would have the most benefit.

As the risk register is primarily a log of risk management activity then it is good practice to enter assessed risks onto the register in agreement with the staff and responsible manager. Updating the risk register is an iterative process and the register should be subject to a scheduled review process to ensure effective monitoring.

3.6.3 Inclusion of New Risks on the Register

The Management Team should agree on the criteria for the inclusion of new risks on the register. Such criteria may include risk events that require the Management Team to plan for example, where actions may need to be allocated to a number of members of the Management Team, significant risks which require the direct oversight of the Management Team, or risks notified from another level in the organisation.

When you enter an assessment onto the register you will be required to allocate a status to it that is **open** or **monitor**.

It is recognised that proposals for the addition of new risks onto the risk register can be made at any time but the decision to include these as risks on the risk register will be made and recorded at the Management Team meeting. New risks to be considered should be submitted to the Risk Owner (Manager) on the 'Proposed risks for inclusion' form available on Risk Management Support Tools – HSE.ie.

At the Management Team meeting, the team can decide to:

1) **Accept** the risk onto the risk register
2) **Not accept** the risk onto the risk register
3) **Request further information**

If **accepted** that the risk should be included on the register, the Senior Manager will nominate an SME to work with the Risk Lead to conduct the analysis and evaluation of the risk and present this at the next meeting for sign off and inclusion on the register.

If **accepted or not accepted**, following the meeting the decisions are formally communicated to the Management Team members who submitted the risk for consideration.

Requests for further information are notified to the Management Team member who submitted the risk for consideration requesting the required information is available for the next available Management Team meeting.

3.6.4 Reviewing the Risk Register

In relation to the risk register, the Management Team will:

- Review the risk register including any new risks submitted for consideration.
- Agree and sign off any additional measures required to mitigate a risk and updates to the existing risks on the risk register.
- Accept/reject recommendation for re-rating/de-escalation/changes to the risk status of existing risks.
- Consider whether any risks require notification to the manager to which a service reports.
- Agree upon amended timeframes for actions due and incomplete.
- Identify actions relating to any existing controls whose status has changed and assign to a member of the Management Team.
- Decide if any additional actions/controls, above those already identified on the register, are required.
- Decide whether any significant changes to, or increase in, the risks should be notified to the next level of management.

The decisions reached on the principal risks and relevant treatment plans will be collectively agreed, documented and communicated to the Management Team member who are responsible for the management of the risk.

It is recommended that the risk register should be reviewed monthly at the relevant Management Team meeting but at a minimum quarterly.

3.6.5 Updating Existing Risks on the Register

To update risks on the register, the Risk Coordinator/Risk Lead should facilitate, in association with Risk Owners, the following steps;

- Assigned Action Owners must provide an update on progress to the Risk Owner on any action assigned to them where the due date is falling due and also to provide updates on the progress and status of any action assigned to them.
- Where the due date for an action has been reached and the action remains outstanding, the update should reflect the reason for this and a new due date should be proposed.
- Where confirmation of an action is implemented/complete and evidence available it reduces the likelihood or impact of the risk, it is added as a control in the risk register. In such an instance the action required should be closed and the new control should be reflected in the existing control section of the register.
- When action updates have been reflected on the register, the Risk Coordinators in consultation with the Risk Lead/SME, Risk Owner and with input from Action Owners, if required, will reassess each of the risks.
- The risk register will be updated based on the outcome of the revised risk assessment.
- The revised register should be sent to the Risk Owner (Manager) in advance of the Management Team meeting to review each of the risks for which they are assigned. This must include a review of the risk description to ensure it remains valid and a review of the existing controls to ensure they continue to operate effectively since the risk was last reviewed.
- The Risk Owner (Manager) reviews the updated risk register including the key changes since the last report e.g. new risks added, risks closed, actions completed/outstanding and changes to risk ratings, prior to submission to the Management Team for approval.
- Controls that were considered strong controls may no longer be applicable or some new controls may be now in place which require inclusion in the register.
- Any areas requiring amendment should be notified immediately to the Risk Coordinator/ Risk Lead so that these may be reflected in the register.
- The Risk Owner in consultation with Risk SMEs should review the risk rating in the context of the above and be in a position to recommend re-rating the risk at the Management Team meeting if relevant.
- The Risk Lead will provide a report to the Management Team which outlines:
  - actions due and complete;
  - actions due and incomplete;
  - actions due for the next period;
  - existing controls whose status has changed; and
  - recommendations for re-rating/changing the risk status of existing risks/de-escalation.

3.6.6 What is the Status of a Risk on the Risk Register?

An **open** risk is one where you have identified several additional controls which require implementation whilst a **monitored** risk is one where you acknowledge it as a risk but have decided that further action is not indicated at that time.

Therefore those risks assigned a status of **Open** will be the ones that will be actively managed at your Management Team meetings. Risks with a status of **Monitor** will be reviewed on a minimum of a quarterly basis, or more frequently should circumstances indicate that the controls in place are not working as intended. Where control measures no longer maintain or modify the risk, the risk rating should be reassessed.

A **closed** risk has all required actions completed and requires no further action. They are archived onto a closed register for audit purposes. Closed risks should be reviewed periodically to ensure controls continue to operate effectively.

3.7 Procedure: Communication and Consultation

Effective communication and consultation enhance risk management. All parties need to understand each other's perspectives and, where appropriate, be actively involved in decision-making.

There should be clear routes and processes for the **communication**, **notification** and **escalation** of risk from one level of the organisation to another. However, it is also important to realise that such activity does not absolve the responsibility of the Manager, to which the risk relates, of taking any actions required to mitigate a risk that is within their span of control. The risk, therefore, remains on their risk register.

3.7.1 Risk Communication

Management Teams across the HSE regularly discuss risks at the level of the organisation for which they are responsible for. These discussions and decisions are part of the normal management/ performance process. However, oftentimes those discussions are not framed using the language of risk or part of the formal risk management process and therefore opportunities to embed risk management into day-to-day management practice can be missed.

One simple discipline that can be adopted is to add a standing agenda item to team or committee meetings to reflect on whether any of the discussions at the meeting constituted a risk, and/or actions to address those risks were identified or add "risk management/register" as a specific agenda item. Integrating risk management awareness into normal management practice will assist in making the risk management process and risk register a more useful and meaningful management tool.

There should be ongoing communication of risks with a Risk Owner's relevant Line Manager to ensure awareness and understanding of risks, and to obtain feedback and other relevant information to support decision-making. Due consideration should be given to the effectiveness of the controls in place to mitigate the risk and whether the nature of the risk is changing. This process can include a general communication, risk notification or may, in certain circumstances, result in a risk escalation.

3.7.2 Risk Notification

Risk notification is an exchange of information to support the decision-making process. A risk notification is not a formal escalation of risk.

When a risk is notified to a more Senior Manager that Senior Manager can:

- review the risk and decide **not to accept** it but seek assurances in relation to the adequacy of its management within the referring service area. This can include the provision of resources/ authority to assist in its mitigation.
- Decide **to accept** that the risk **should be included on their risk register**. Reasons for inclusion are generally due to one of the following reasons:
  - that the significance of the risk is such that it requires oversight on their register
  - though the risk that was notified was identified by one area of the service, it has resonance across the service as a whole. So rather than managing it on each individual register, for effectiveness and efficiency, many of the actions identified are better managed collectively, for example, if an over-arching policy or process is required, an individual could be assigned to lead out on its development.

- If multiple services could be impacted by this risk, this may involve informing and/or consultation with other services on how to best mitigate this risk.

On accepting the notified risk, the Senior Manager arranges for it to be assessed in the context of their area of responsibility and includes it on their risk register. Any additional actions that are identified as being required are assigned according to the business rules, that is:

- to themselves,
- members of their Management Team or
- to their Line Manager.

Table 9 below can assist in determining the process for notification of risks.

Table 9: Notification of Risks

Risk Rating	Risk Owner	Line Manager/Senior Manager
High	Notify Line Manager/Senior Manager.	Reviews the risk assessment and decides if the risk should be included on their risk register.
Medium	Continue to manage at a local level. Continue to inform Line Manager through communication process and notify if rating increases.	Reviews the risk assessment and seeks assurances in relation to the adequacy of its management.
Low	Continue to manage at a local level. Continue to inform Line Manager through communication process.	Review all low risks on a quarterly basis.

Possible outcomes of a risk notification are as follows:

- It provides assurances that the measures undertaken and presented by the Risk Owner are effective.
- No further action by the Risk Owner is required.
- Further controls or more actions are required to mitigate the risk.
- The risk will continue to be managed at the level it is currently managed at.
- Further resources/authority to assist in its mitigation are required.
- The risk has been reduced to a level that its status can change from **Open** to **Monitor** or **Closed** and recorded as such.

Note: While most risks are identified and managed locally, sometimes when they materialise they may become the subject of significant regulatory or public concern. In addition to ensuring that appropriate measures are in place to manage the risk, there may be a need to inform more senior levels of management that the risk has materialised. In the first instance, your Line Manager should be notified as soon as possible and they will be responsible for further notification where required. Having good records available that demonstrate the measures taken to manage the risk will be important when providing briefings on the risk as it materialises.

3.7.3 Risk Escalation

There may be occasions when the Line Manager may decide that the current Risk Owner cannot address the necessary actions as they are outside of the Risk Owner's control. For example, the risk may be more systemic or the most appropriate Action Owner is at a higher management level or there remains a concern about the existing level of risk, which requires additional stakeholders to contribute to ensure an appropriate set of actions are put in place to address the risk.

In these circumstances, the Line Manager may decide following a review of the risk with the Risk Owner that the risk should be escalated to them, for management.

As the responsibility for the management of risk generally lies at the level it may manifest, **escalation must be subject to a formal decision by the Line Manager** which should be documented and communicated. Likewise, the decision of the Line Manager to de-escalate a risk should be documented and communicated. A de-escalation can occur if the Line Manager decides that the risk is within their direct report's control to manage.

The decision to accept or not accept a risk or action, or the escalation of a risk to another level of management and therefore recorded on their risk register must be formally agreed between the relevant Line Manager and current Risk Owner who is requesting an escalation of the risk. This decision should be recorded and formally communicated between the Line Manager and the Risk Owner. A decision to escalate should not be an end in itself but must be accompanied by an agreed set of actions/ responsibilities. Where a risk is subject to a formal decision agreed between the current Risk Owner and by the next level of management it should include the agreement of transfer of ownership for specific controls/actions also. Where a decision is taken not to accept an escalated risk other actions may be required. This could include providing additional supports or resources to manage the risk.

The outcome of such considerations must be communicated back to the service that notified the risk.

As previously set out any risks proposed for notification, escalation or inclusion on another risk register are subject to a formal request for consideration. For this purpose, there is a 'Proposed risk for inclusion' form available on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie.

Understanding risks in your area of responsibility is an important management function. Managers should therefore ensure an understanding of the potential risks for their service or function, whether through the review of risk registers and/or meetings with the teams who report to you.

Risks that are deemed more dynamic in nature may be monitored more frequently to provide additional supports and/or to notify or escalate to next level of management. All risks will continue to be reviewed as part of the normal monitoring cycle.

3.8 Procedure: Monitoring and Review

This step involves the monitoring of changes to the source and context of risks, the tolerance for certain risks, and the adequacy of controls. It is also to ensure processes are in place to review and report on risks regularly.

To ensure structured reviews and regular reporting, a process should be in place to allow key risks within your area to be monitored. Given the diverse and dynamic nature of the healthcare environment, it is important to be alert to emerging risks as well as monitoring known risks.

3.8.1 Reviewing the entirety of the Register

Though risk is monitored (on an ongoing basis as outlined above at relevant Management Team meetings), the Management Team should consider the entirety of the register periodically, ideally at a dedicated risk management meeting. Such a review process can assist in keeping the register relevant and allow for the identification of new risks and the archiving of risks that have been managed. It is recommended that the risk register should be reviewed in its entirety at **a minimum** on a biannual basis.

3.8.2 Re-Rating Risk

With the completion of some or all of the actions, the level of risk (the rating) may be reassessed to consider whether its likelihood or impact score has reduced.

Re-rating the risk should be done by the Risk Owner supported by the Risk Lead in consultation with the person who acted as the Risk SME at the time the risk was initially assessed. This is because it is the Risk SME that has the expertise in relation to the risk and will be able to 'evaluate' the extent to which the completion of additional controls serves to reduce or mitigate the risk. Where the implementation of actions does not appear to be serving to reduce the risk, the appropriateness of the actions identified should be reviewed and revised actions planned. Re-rating the risk assists in evidencing that the risk is being actively managed.

3.8.3 Changing the Risk Status

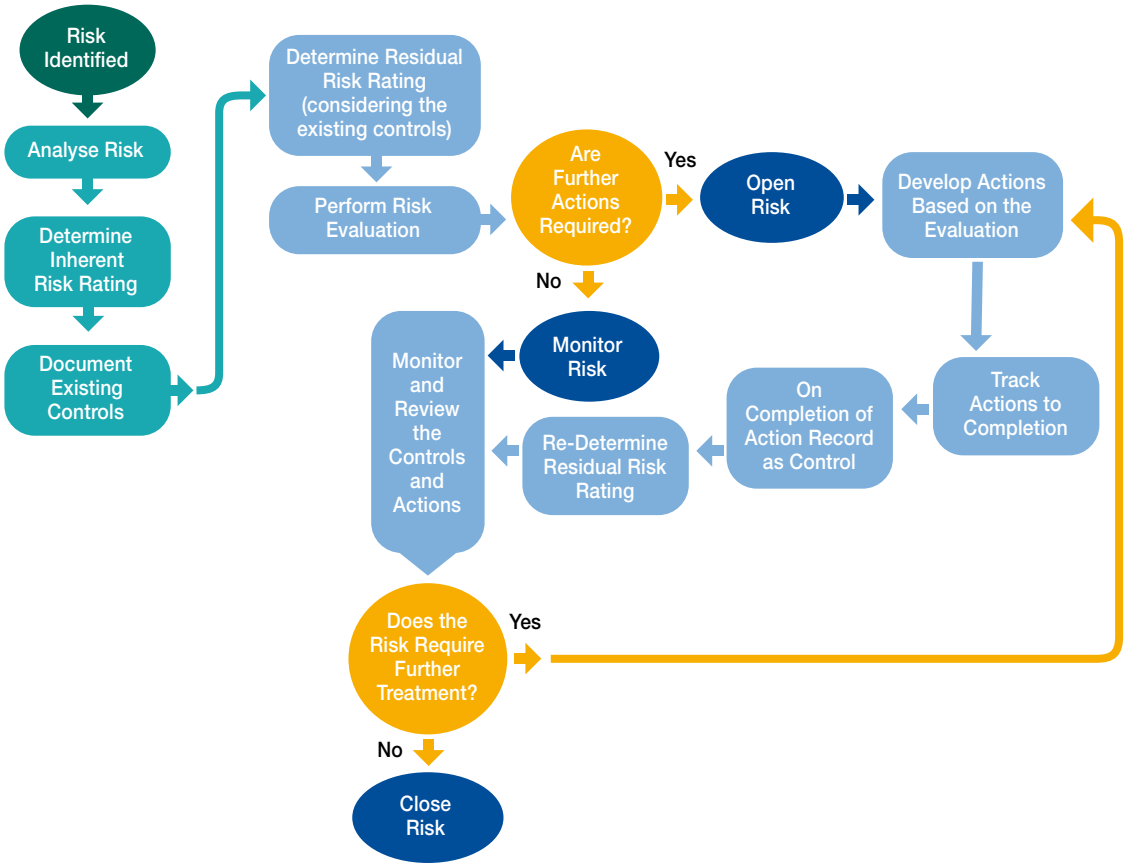
Whilst under active management, a risk has the status of being **Open**. With the completion of actions and the mitigation of the risk, consideration can be given to changing its status to either **Monitor** or **Closed**. Closed risks should be reviewed periodically to ensure controls continue to operate effectively. Where control measures no longer maintain or modify the risk, the risk rating should be reassessed.

3.8.4 De-escalating Risk

In instances where a risk was notified to and accepted onto the register of a more senior manager for oversight, it may be that following the implementation of actions the rating of the risk has reduced to an acceptable level, or, remaining actions lie within the control of the manager at the level below. In such circumstances, a decision may be taken to **Close** the risk on the register and to de-escalate it onto the register of the manager on the level below. Such risks when added to the register below are given a risk status of **Open** on that register and are reviewed at the next Management Team meeting of that manager.

Figure 14 illustrates the process for management of risk from identification to closing of a risk.

Figure 14: Risk Process and Status of Risk



3.8.5 Ongoing Risk Reviews

Once risks have been identified, recorded, analysed, and agreed treatments implemented, managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. An appropriate monitoring and reporting regime should be established to keep track of how effective the treatment is in controlling the risk.

Wherever possible, risk management should become an agenda item on management meetings or committees rather than a separate process. The aim of regular reviews is to identify when new risks arise and monitor existing risks to ensure that controls are still effective and appropriate and actions are completed as required. How frequently a review process and reporting cycle occurs will depend on the residual risk rating versus what the target risk rating has been set to achieve. However, it is suggested that this should not be less than quarterly.

In addition, risk assessments should be reviewed if there is a change in the service/organisation, for example, when new resources or procedures are introduced that would impact the risk. Changes made to the risk assessment should be brought to the attention of relevant staff and other persons.

This continual process of review is to aid in the ongoing process of assurance that risks are being identified and managed. Such assurances are seen as part of the organisation's lines of defence.

3.8.6 Risk Management as a Line of Defence

Risk Management plays an important role in the lines of defence within an organisation. By defining the sources of assurance in broad categories, the lines of defence model helps an organisation to understand how each line contributes to the overall level of assurance provided. Figure 15 provides an illustration of such a model. This is in line with the HSE's Controls Assurance Framework (hse-accountability-framework.pdf) and examples of each line of the lines of defence are detailed below.

First line: the way risks are managed and controlled day-to-day. Assurance comes directly from those responsible for delivering specific objectives or processes. Its value comes from those who know the business, culture and day-to-day challenges.

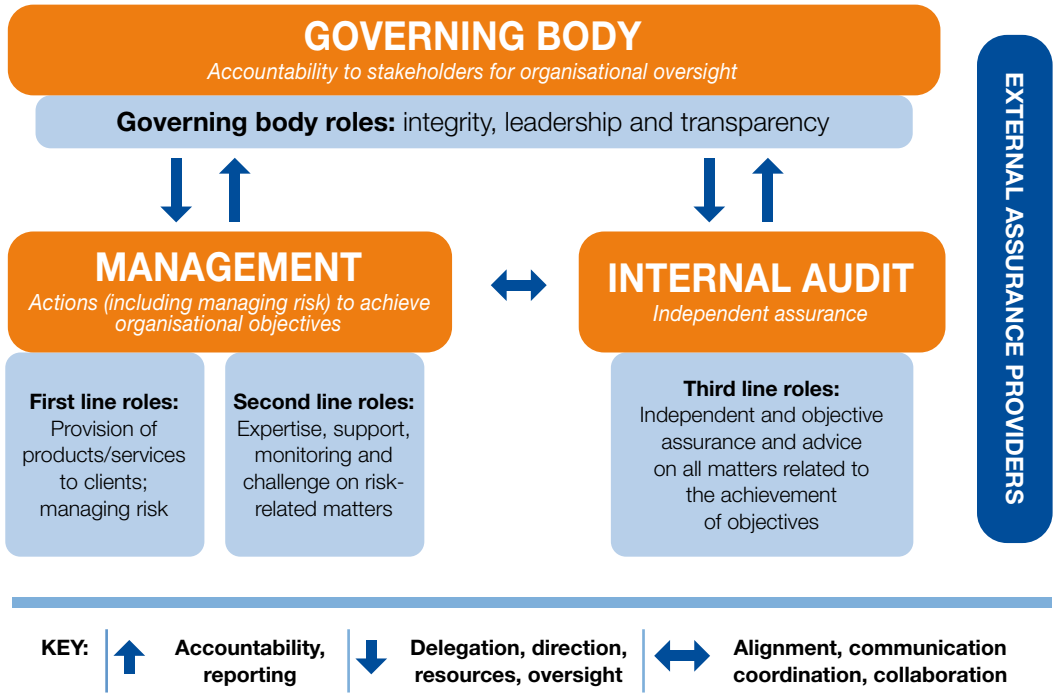
Second line: the way the organisation oversees the control framework so that it operates effectively. The assurance provided is separate from those responsible for delivery, but not independent of the management chain, such as risk and compliance functions.

Third line: objective and independent assurance, e.g. internal audit, providing reasonable (not absolute) assurance of the overall effectiveness of governance, risk management and controls. The level and depth of assurance provided will depend on the size and focus of the internal audit function and management's appetite for internal audit assurance.

External Assurance Providers: assurance from external independent assurance providers such as Regulators.

While every staff member is responsible for identifying and managing risk within the context of their work, risk management is a line management responsibility and a core management process. It must therefore be a focus of Management Teams at all levels in the HSE.

Figure 15: 3 Lines of defence model



Taken from Institute of Internal Auditors (IIAs)

3.9 Procedure: Tools for Understanding Risk

This procedure section sets out in detail several useful tools and techniques available to assist during the risk management process. Table 10 below provides a summary of the tools and techniques that are discussed in more detail in the subsequent sections.

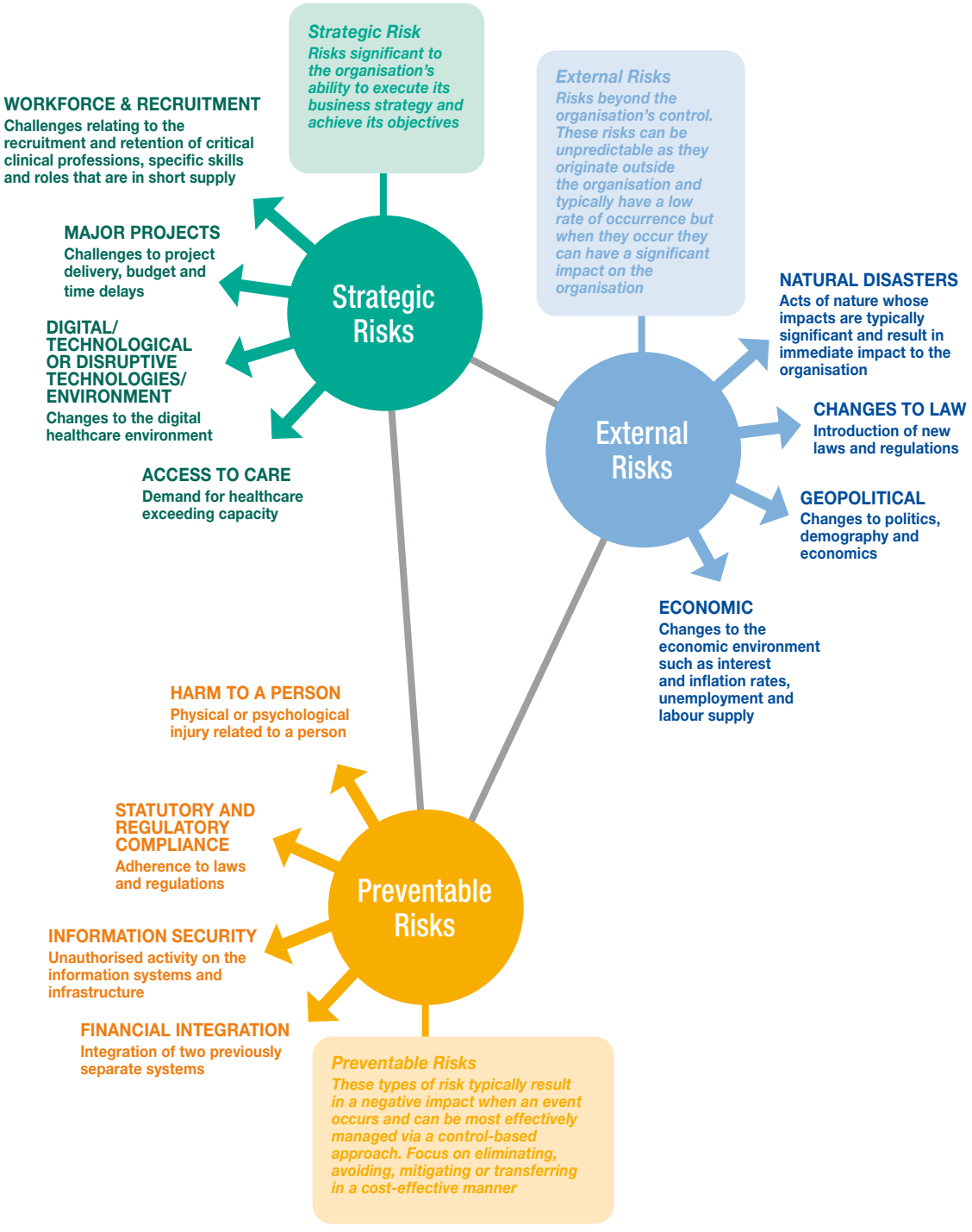
Table 10: Useful Tools and Techniques Overview

Part of process	Tool	Brief description
Identifying risk	Risk Universe	A risk universe is a list of possible risks that could be faced by an organisation. It is useful when trying to identify risks in your area of responsibility.
	PESTLE Analysis	A tool used to examine an organisation's external environment and as such can assist the risk identification process.
	Horizon Scanning	A tool to examine future threats and opportunities before they occur across the short, medium or longer term. Particularly useful when it comes to emerging risks.
Understanding the risk	Bow-tie analysis	A tool used to better understand the identified risk event, causes, impacts/consequences and proactive and reactive controls.
	The '5 Whys' Technique	The '5 Whys' is an iterative question-asking technique to identify the root cause underlying a particular risk causal factor.

3.10 Procedure: Tools for Understanding Risk – Risk Universe

A Risk Universe is a list of **possible** risks that could be faced by an organisation. It provides a useful starting point when seeking to identify the potential risks specific to an organisation and the external and internal factors contributing to risk. Giving consideration to the Risk Universe also allows for the assessment of emerging risks. Emerging risks are new or unforeseen risks that have not yet been fully contemplated. This is a risk that should be on our radar but is not, and its potential for harm or loss is not known. While not an exhaustive list, an example of a Risk Universe is provided in Figure 16 below.

Figure 16: Risk Universe within a Healthcare Setting



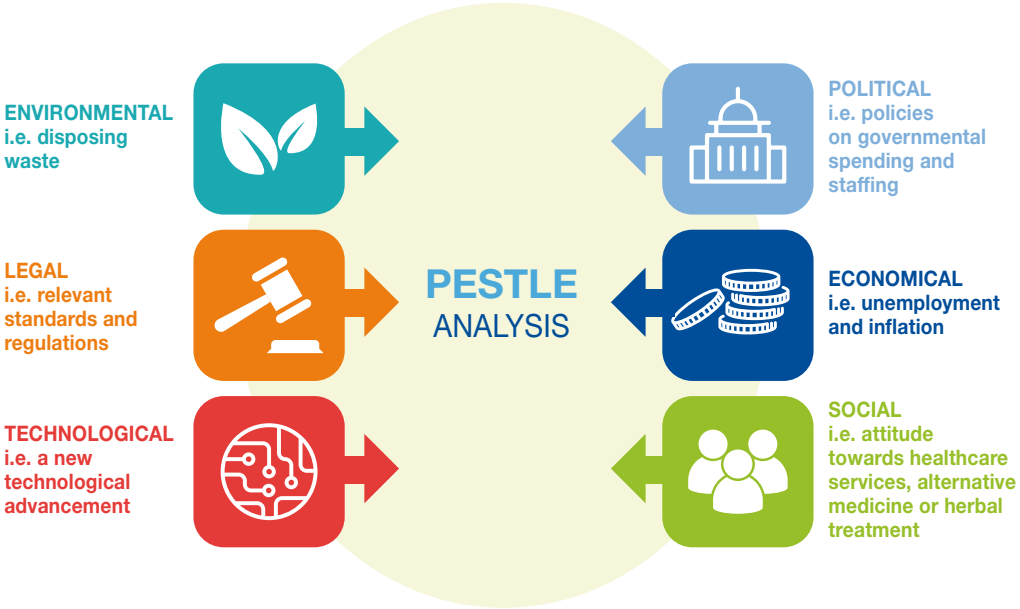
Source: Adapted from Robert Kaplan and Annett Mikes, "Managing Risk: A New Framework" Harvard Business Review

3.11 Procedure: Tools for Understanding Risk – PESTLE Analysis

A PESTLE analysis is a tool used to examine an organisation's external environment and as such can assist the risk assessment process. PESTLE stands for Political, Economic, Societal, Technological, Legal and Environmental factors.

To understand the environment in which you, as a staff member operate, a PESTLE analysis can be used to determine the various elements involved in the achievement of your objectives. A high level PESTLE analysis is illustrated in Figure 17 below. A template to assist with the completion of a PESTLE analysis is provided below and a more detailed worked example is available on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie

Figure 17: PESTLE analysis



PESTLE Analysis Template

PESTLE ANALYSIS	
Business Objective	
Date	
Political	
Economic	
Societal	
Technological	
Legal	
Environmental	

3.12 Procedure: Tools for Understanding Risk – Bow-tie Analysis

A Bow-tie analysis is a method of analysing, mapping and understanding risks. It assists in clarifying the components of a risk, which is the risk event, the cause(s) of the risk event and the potential impacts and consequences of the risk event if it were to materialise. The Bow-tie represents the fact that a range of factors (causes) can converge to create the risk event and then once the Event has occurred that its consequences can be very far reaching.

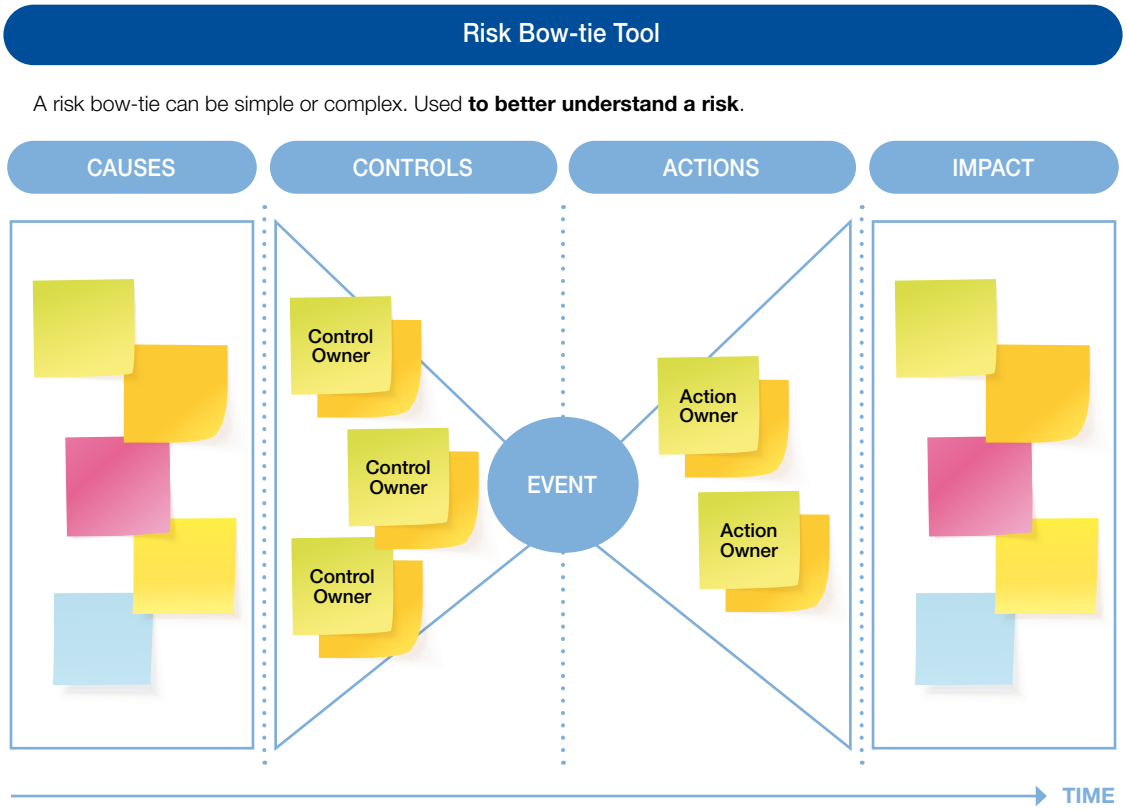
By understanding the cause(s) of a risk event, particularly the root cause(s) we can identify the best strategy to prevent or reduce the risk. There will always be some consequence of a risk event if it were to occur. Managing risk requires us consider how we respond to these consequences. The response could include managing the immediate disruption arising from the risk event and/or understanding what caused the risk event to occur and taking corrective action to reduce the likelihood or impact of it happening again.

The Bow-tie analysis is also used to visually display and communicate information about risks in situations where an event has a range of possible causes and potential impacts. A Bow-tie is used when assessing controls to check that each pathway from cause to event and event to impact has effective controls and that factors that could cause controls to fail are recognised. A Bow-tie analysis is illustrated in Figure 18 below. Both a template to assist with the completion of a Bow-tie analysis and a more detailed worked example is available on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie

An understanding of the causes of potential events and the drivers of risk can be used to design strategies to prevent adverse consequences or enhance positive ones. Often there is a hierarchy of causes with several layers before the root cause is reached. Generally causes are analysed until actions can be determined and justified. Refer to section 3.14 for the '5 Whys' causal analysis technique to help understand the root cause.

Bow-tie analysis can be used to explore in detail the causes and consequences of events that are recorded in a simple form in a risk register. It is particularly used for analysing events with more serious consequences. It can be used as the basis of a means to record information about a risk that does not fit the simple linear representation of a risk register and it can be used proactively to consider potential events and also retrospectively to model events that have already occurred.

Figure 18: Illustrative example of a Bow-tie analysis



Simply illustrated;

- The event of interest, or risk, is represented by the central knot of the Bow-tie.
- Potential causes of risk (or hazards/threats in a safety context) are listed on the left-hand side of the knot and joined to the knot by lines representing the different mechanisms by which sources of risk can lead to the event.
- Controls and actions for each cause are shown.
- On the right-hand side of the knot are the potential impacts.

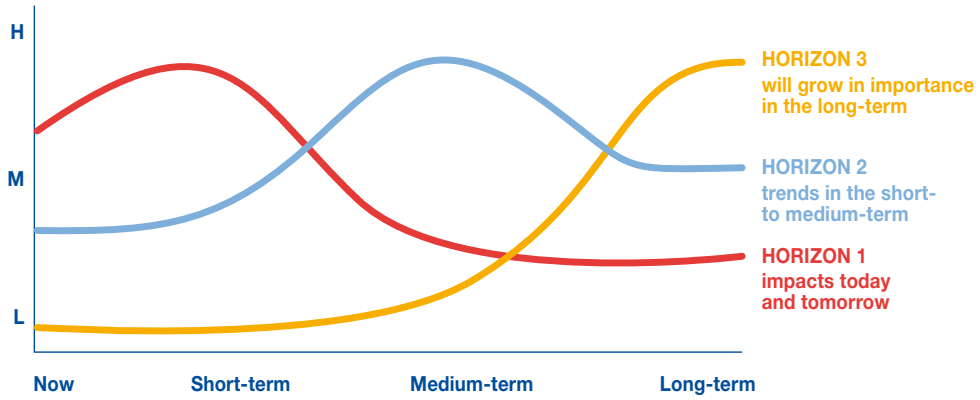
3.13 Procedure: Tools for Understanding Risk – Horizon Scanning

Horizon scanning is a good technique to look at areas of complexity, challenge assumptions and review multiple ways that events could unfold, in order to increase the resilience and reliability of organisational responses to risk. It is not about trying to predict the future but rather reviewing options so that evidence-based decisions can be made.

Horizon scanning can be defined as the exploration of what the future might look like to understand uncertainties better and to analyse whether the organisation is adequately prepared for potential opportunities and threats[4].

A high level Horizons Model is illustrated in Figure 19 below and highlights the difference in planning and action requirements for potential risks in the short, medium, and long term. A template to assist with the completion of a Horizons Model is provided below and a more detailed worked example is available on the Risk Management Support Tools website page at: Risk Management Support Tools – HSE.ie

Figure 19: Three Horizons Model



HORIZON 1: Where are you currently taking action
HORIZON 2: Visible trends for strategic consideration
HORIZON 3: Little trend information today but planning needed

One way for organisations to keep on top of their risk profile is to scan the horizon, to look at what may or may not be likely and how that would have an impact on their day-to-day running, their financials, and their reputation, and ensure that they are prepared for as many risks as possible that may be on the horizon.

Carrying out a horizon scanning, it effectively adds another dimension of assessment by capturing when the event will happen on the horizon that is chosen typically in respect to set periods, i.e. short, medium and long term. You can use both the various sources and approaches of information that have been mentioned in the policy in Table 2, or other forms of assessment included in the guidance. A template for use is provided below.

4 Horizon Scanning: A Practitioner's Guide

Horizon Scanning Template

Business Objective			
Date			
< 5 Years			
Insert category of potentially affected area, e.g. financial, regulatory	**High Impact** **If assessed as 'High Impact' provide detail available to date and potential impact**	**Medium Impact** **If assessed as 'Medium Impact' provide detail available to date and potential impact**	**Low Impact** **If assessed as 'Low Impact' provide detail available to date and potential impact**
5 to 10 Years			
> 10 Years			

3.14 Procedure: Tools for Understanding Risk – The '5 Whys'

What is the '5 Whys' method and how can it help you?

The '5 Whys' method is set out in the HSE's 2020 Incident Management Framework document, '*Tools to assist in the conduct of a systems analysis*'. It explains how the '5 Whys' method is a simple tool which focuses on repeatedly asking the question 'Why?' and, as a tool, can help to determine the cause-effect relationships in a risk event and can be used whenever the real cause of a risk event is not clear or is to be determined.

As explained in the document;

The idea is simple: ask "why" 5 times, until you get to the root cause of your issue.

Start with a statement of the situation and ask why it occurred. Then turn the answer to the first question into a second 'Why' question. The next answer becomes the third 'Why' question and so on. By refusing to be satisfied with each answer the odds of finding the underlying cause of the event increase. Though this technique is called '5 Whys', five is a rule of thumb. You may ask more or less whys before finding the cause of a problem.

The goal of the '5 Whys' problem-solving method is to reach the root cause of an issue faster and to drill down to countermeasures.

For an illustrated example, a '5 Whys' table is provided in the Incident Management Framework document, available at this link: https://www.hse.ie/eng/about/who/nqpsd/qps-incident-management/incident-management/hse-2020-incident-management-framework-guidance.pdf

Appendix 1: Glossary of Terms

Term	Definition
Action	Actions are a future measure that will maintain and/or modify a risk. In the HSE, an action is a future measure to further reduce either the likelihood or impact of a risk.
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.
Corrective Controls	Corrective controls are designed to correct errors or undesirable events which have occurred and will prevent further occurrences.
Current Risk	Current risk is the level of risk after both the existing controls and actions are considered at the point in time the risk is being assessed.
Detective Controls	Detective controls are designed to search for and identify errors or undesirable events after they have occurred so that corrective actions can be taken.
Directive Controls	Directive controls give direction. These can be, for example, statutory obligations, regulatory standards including professional standards, or other organisational requirements or instructions, many of which are converted into policies, procedures, circulars, standard operating procedures and training.
Emerging Risk	Emerging risks are new or unforeseen risks that have not yet been fully contemplated. This is a risk that should be on our radar but is not, and its potential for harm or loss is not fully known.
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. In particular, it guides the organisation to address risks comprehensively and coherently, instead of trying to manage them individually.
Establishing the Context	Establishing the context requires us to identify the external and internal factors that the HSE and its services must consider when they manage risk.
Hazard	A potential source of harm or adverse health effect on a person or persons.
Impact	The outcome or consequence of an event affecting objectives. It can be expressed either qualitatively or quantitatively, being a loss, disadvantage, or gain. There may be a range of possible outcomes associated with an event.
Inherent Risk	Inherent risk in the HSE is the level of risk before consideration of control and/or action measures.
Initial Risk	Initial risk is the level of risk after existing controls are considered when the risk was originally assessed.

Term	Definition
Issue	A relevant event that has happened was not planned and requires management action.
Likelihood	The chance of something happening (also described as the probability or frequency of an event occurring).
Monitor	To check, supervise, observe critically or record the progress of an activity, action or system, regularly to identify change.
Operational Risk	Operational risks concern the day-to-day threats that the organisation is confronted with as it strives to deliver its objectives. Operational risks are most commonly identified at a service delivery level.
Preventative Controls	Preventative controls are controls designed to stop, discourage, pre-empt or limit the possibility of an undesirable event before it occurs.
Residual Risk	Residual risk in the HSE is the level of risk remaining after consideration of existing controls
Risk	Risk is the effect of uncertainty on 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 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 the HSE and to estimate the level of risk attaching to it.
Risk Appetite	Risk appetite is the amount and type of risk that an organisation is willing to pursue or retain. In the HSE, it is the level of risk the HSE is willing to accept to achieve its strategic objectives.
Risk Appetite Statement	A Risk Appetite Statement is a broad overarching statement of the level of risk an organisation is willing to pursue or retain.
Risk Assessment	The overall process of risk identification, risk analysis, and risk evaluation.
Risk Avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk. Risk avoidance may increase the significance of other risks or may lead to the loss of opportunities for gain.
Risk Categories	The categories used by the organisation to group similar opportunities or risks for the purposes of reporting and assigning responsibility.
Risk Communication	Risk communication is the sharing or exchanging of information and gaining a common understanding of the risk.
Risk Criteria	Risk criteria relate to the identification of risk as either strategic or operational and to further categorise a risk based on the area upon which it impacts.
Risk Description	A structured statement of risk usually containing three elements: risk event, cause and impact.
Risk Escalation	Risk escalation is required in certain circumstances that could include when a risk can no longer be managed at the level in which it is expected to materialise i.e. it is agreed that a higher level manager would be a more appropriate action owner or the risk is more systemic and a more comprehensive set of actions to manage the risk are required.

Term	Definition
Risk Evaluation	The purpose of risk evaluation is to make decisions based on the risk analysis stage of the risk process, about which risks need treatment, the treatment type, and treatment priorities.
Risk Event	Occurrence of a particular set of circumstances that was earlier deemed only a possibility. Depending on the nature of the risk event, it may be referred to as an incident or disaster. In principle any risk that materialises is a risk event. E.g. Cyber Incident or Natural Disaster.
Risk Identification	Risk identification is the process of finding, recognising, and describing risks. Risk identification is an ongoing activity of all managers and their teams.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Process	The systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring, and reviewing risk.
Risk Notification	Risk notification is an exchange of information to support the decision-making process. A risk notification is not a formal escalation of risk. In the HSE, risk notification is recognising the risk is increasing or is not being managed effectively, and so requires notification to the next level of management.
Risk Profile	In the HSE, a Services' risk profile is set out in its risk register. A risk profile is a written description of a set of risks. A risk profile can include the risks that the entire organisation must manage or only those that a particular function or part of the organisation must address.
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 occur- ring. 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.
Risk Register	A risk register is a database of assessed risks that face any organisation at any one time. Always changing to reflect the dynamic nature of risks and the organisation's management of them, its purpose is to help managers prioritise available resources to minimise risk and target improvements to best effect.
Risk Tolerance	Risk tolerance is an organisation's readiness to bear the residual risk in order to achieve its objectives. The HSE defines risk tolerance as the level of deviation from risk appetite we are prepared to tolerate.
Risk Treatment	Risk treatment is a process to modify risk. In the HSE, risk treatment includes the implementation of effective operating controls and future additional actions.
Risk Universe	A Risk universe is a list of possible risks that could be faced by an organisation
Risk Velocity	Risk velocity refers to how fast a risk may affect an organisation.
Target Risk	Target risk in the HSE is the planned level of risk after consideration of both control and action measures.

Appendix 2: Risk Assessment Tool

HSE Impact Table

Impact Rating	1	2	3	4	5
Categories	**Negligible**	**Minor**	**Moderate**	**Major**	**Extreme**
Harm to a person (Service User, Patient, Staff & Public)	No harm. No need for treatment. No impairment of ability to manage normal daily routines. No impaired psychosocial functioning. No time off work	Adverse event/incident leading to **minor harm** needing minimal additional intervention. (e.g. first aid, extra observation or minor treatment) Requiring first aid/extended hospital stay for treatment of ≤ 72 hours. Recovery of ability to manage daily routines within 72 hours. Impaired psychosocial functioning (> 72 hours ≤ 1 month) ≤ 72 hours absence from work.	Adverse event/incident leading to **moderate harm** (significant, but not permanent harm) requiring a moderate increase in treatment. (e.g. an unplanned return to surgery, an unplanned re-admission, cancelling of treatment leading to prolonged symptoms/disease, or transfer to another treatment area (such as short stay in intensive care with good recovery) Extended hospital stay for treatment of (> 72 hours to ≤ 8 days) Recovery of ability to manage daily routine within a month and without significant complication or significant permanent disability. Impaired psychosocial functioning (> 1 month ≤ 6 months) > 72 hours absence from work to ≤ 6 months. Agency reportable e.g. Gardaí (violent and aggressive acts), Tusla, HIQA, MHC and HSA.	Adverse event/incident leading to **severe harm** such as permanent lessening of bodily, sensory, motor, physiologic or intellectual functions resulting in long-term incapacity or disability (e.g. loss of limb, blindness, brain damage/HIE, shortening of life expectancy) Extended length of stay in hospital (> 8 days) Significant complication/significant permanent disability impacting ability to manage normal daily routine in the same manner as before. Impaired psychosocial functioning (> 6 months) Absence > 6 months Agency reportable e.g. Gardaí (violent and aggressive acts), Tusla, HIQA, MHC and HSA.	Adverse event/incident leading to death or permanent total disability. (e.g. unanticipated death that did not arise from, or was a consequence of (or wholly attributable to) the illness of the patient or an underlying condition of the patient occurring while receiving care) Permanent psychosocial functioning incapacity. Agency reportable e.g. Gardaí (violent and aggressive acts), Tusla, HIQA, MHC and HSA.
Service User Experience	Unsatisfactory experience not directly related to the provision of care services or supports (e.g. inadequate provision of information)	Unsatisfactory service user experience readily resolvable. (e.g. less than optimal treatment/ inadequate information; not being talked to and treated as an equal; or not being treated with honesty, dignity and respect)	Unsatisfactory level of service user experience resulting in short term resolvable consequences (< 1 week) (e.g. related to less than optimal treatment)	Mismanagement of service user experience resulting in long term consequences. (e.g. related to poor or incorrect treatment)	Totally unsatisfactory service user outcome or extremely poor care provision resulting in long term consequences.
Business/Service disruption/Security (unauthorised and/or inappropriate access to systems/assets including data)	No material disruption to dependent work. Interruption in a service which does not materially impact on the delivery of service user care or the ability to continue to provide service.	Short-term temporary suspension of work. Minor public impact. (e.g. delays in waiting time) Local management assistance required. Short term disruption to service with minor impact on service user care. Backlog cleared in a week. Backlog requires extended work, overtime or additional resources to clear. Unplanned loss of IT facilities ≤ 4 hours.	Medium-term temporary suspension of work. Additional resources/budget required Regional management assistance required (HG CEO or CHO CO). Manageable impact. Some disruption in service with unacceptable impact on service user care. Temporary loss of ability to provide service. Unplanned loss of IT facilities between > 4 ≤ 8 hours.	Prolonged suspension of work. Additional resources, budget. National/management assistance required. (National Director) Performance criteria compromised. Sustained loss of service which has serious impact on delivery of service user care or service resulting in major contingency plans being involved. Unplanned loss of IT facilities between > 1 day ≤ 1 week.	Indeterminate prolonged suspension of work. Significant additional resources, budget/ management assistance required. CEO, Department of Health and Minister of Health intervention required. Non-performance. Other providers appointed. Permanent loss of core service or facility. Disruption to facility leading to significant 'knock on' effect. Unplanned loss of IT facilities > 1 week.
Loss of trust/ confidence or morale (Public/Staff), including reputational risk	Rumours, no media coverage. No public concerns voiced. Little effect on staff morale. No review/investigation necessary.	Local/national media coverage – Short term. Some public concern. Minor effect on staff morale/public attitudes. Internal review necessary.	Numerous local/national media outlets – adverse publicity. Significant effect on staff morale and public perception of the organisation. Public calls (at local level) for specific remedial actions. Comprehensive review/investigation necessary.	National media/adverse publicity, <3 days. News stories & features in national papers. Local media – long term adverse publicity. Public and staff confidence in the organisation undermined. HSE use of resources questioned. Minister may make comment. Possible questions in the Dáil. Public calls (at national level) for specific remedial actions to be taken possible HSE review/ investigation	National/International media/adverse publicity, > than 3 days. Editorial follows days of news stories and features in national papers. Public and staff confidence in the organisation undermined. CEO's performance questioned. Calls for individual HSE officials to be sanctioned. Taoiseach/Minister forced to comment or intervene. Questions in the Dáil. Public calls (at national level) for specific remedial actions to be taken. Court action. Public (independent) Inquiry.

Impact Rating	1	2	3	4	5
Categories	**Negligible**	**Minor**	**Moderate**	**Major**	**Extreme**
Organisational objectives or outcomes	Little impact e.g. Minor delays	Inconvenient delays.	Material delays. Performance behind target (e.g. KPIs)	Significant delays. Performance significantly under target.	Non-achievement of objective/outcome. Total performance failure.
Compliance (Legislative, Regulatory, Policy)	Non-compliance with internal policies. Procedural breach. Evidence of good faith by degree of care/diligence. Unintentional or accidental breaches of security, which may constitute an exposure that needs to be addressed. Non-notifiable breach of data, no adverse outcome.	Material Non-compliance with internal policies. Single failure to meet internal PPPGs. Breach, objection/complaint lodged. Minor harm with investigation. Evidence of good faith arguable. Deliberate and unauthorised breaches of security to gain access to information systems with a notifiable breach of data, readily resolvable.	Repeated failure to meet internal PPPGs. Serious breach. Lack of good faith evident. Performance review initiated. Material harm caused. Misconduct established. Deliberate and unauthorised breaches of security to gain access to information systems with a notifiable breach of data requiring notification to the data subject.	Failure to meet compliance obligations. (e.g. Legislative, Regulatory, Public Policy etc.) Deliberate breach or gross negligence. Formal investigation by external body. Disciplinary action. Ministerial involvement. Serious misconduct. Deliberate and unauthorised breaches of security to gain access to information systems with a notifiable breach of data, requiring notification to multiple data subjects.	Gross failure to meet compliance obligations (e.g. Legislative, Regulatory, Public Policy etc.) Criminal negligence or act. Litigation or prosecution with significant penalty. Dismissal. Ministerial censure. Evidence of criminal misconduct. Deliberate and unauthorised breaches of security to gain access to information systems with a notifiable breach of data, requiring notification to mass data subjects.
Financial (including performance to budget, claims, etc.)	≤ €10,000 loss.	> €10,000 to ≤ €100,000 loss	> €100,000 to ≤ €1,000,000 loss.	> €1,000,000 to ≤ €10,000,000 loss.	> €10,000,000 loss.
	0.33% of budget deficit	0.33 – 0.5% of budget deficit	0.5 – 1.0% budget deficit	1.0 – 2.0% of budget deficit	> 2.0% of budget deficit
Environmental/ Infrastructure/ Equipment	Nuisance Release. No disruption to access or exposure.	On site release contained with minimal intervention. Minimal disruption to access or exposure.	On site release contained with moderation intervention. Short to medium-term restriction of access or exposure.	High level but recoverable, unacceptable damage or contamination of a significant resource or area of the environment. Significant intervention required for permanent cessation of harmful activity' Long-term suspended access, presence or use of resource.	Toxic release affecting off-site with detrimental effect requiring outside assistance. Extensive, very long-term or permanent, significant, unacceptable damage to or contamination of a significant resource or area of the environment. Very long-term or permanent denial of access or exposure.
	Inconsequential damage to buildings/environment/historic resources that requires little or no remedial action.	Recoverable damage to 'non-priority' buildings/environment/historic resources.	Recoverable damage to 'priority' buildings, or loss of 'non-priority' buildings/environment/historic resources.	Permanent damage to priority buildings/ environment/historic resources	Loss of 'priority' buildings/environment/historic resources.
Strategic Programme/Project (objectives/ timeframes) – HSE Executive Use Only	≤ 1% variation to programme/ project deliverables	> 1% to 5% variation to programme/ project deliverables	> 5% to 10% variation programme/project deliverables	> 10% to 20% variation to programme/project deliverables	> 20% variation to programme/project deliverables
	≤ 5% delay (e.g. for a project with a projected timeframe of 3 years an anticipated 2 month over run equals a 5% delay)	> 5% to 10% delay	> 10% to 25% delay	> 25% to 100% delay	> 100% delay

Appendix 2: Risk Assessment Tool

HSE Likelihood Table

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

HSE Risk Scoring Matrix

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

IMPACT

HSE Risk Rating Matrix

LIKELIHOOD	Negligible	Minor	Moderate	Major	Extreme
Almost Certain	Low	Medium	High	High	High
Likely	Low	Medium	Medium	High	High
Possible	Low	Medium	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Low	Low	Low

IMPACT

Appendix 3: Acronyms

Acronym	
ARC	Audit and Risk Committee
CARP	Controls Assurance Review Process
CEO	Chief Executive Officer
CHOs	Community Health Organisations
CRO	Chief Risk Officer
CRR	HSE's Corporate Risk Register
DPER	Department of Public Expenditure and Reform
EMT	Executive Management Team
ERM	Enterprise Risk Management
HIQA	Health Information and Quality Authority
HG	Hospital Group
HSA	Health and Safety Authority
HSE	Health Service Executive
ICT	Information and Communication Technology
IT	Information Technology
MHC	Mental Health Commission
NAS	National Ambulance Service
NRA	National Risk Assessment
NSP	National Service Plan
OHS	Occupational Health and Safety
PPPGs	Policies, Procedures, Protocols and Guidelines
RHAs	Regional Health Areas
SAO	Senior Accountable Officer
SME	Subject Matter Expert

Notes

Contact Details

Office of the Chief Strategy Office

Chief Risk Officer

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

Phone: 01 635 2230

Email: govandrisk@hse.ie

Publication Date: April 2023