

Enterprise Risk Management Policy and Procedures 2023

Frequently Asked Questions

It is recommended to access this document online, as it incorporates hyperlinks to link to responses with corresponding questions.

Additional accessibility functions include an interactive headings dashboard on the initial page, allowing you to navigate directly to related questions by clicking on specific boxes.

While browsing the document, use the bottom left link to return to the Headings on the first page, or click on the bottom right link to return to the List of Questions.

Questions index

Click on the relevant subject box to access a list of questions categorised under each respective heading.

Objectives and Uncertainty	Risk and Risk Management	Identifying Risk	Understanding Risks	Risk Analysis
Risk Evaluation	Responding to Risk	Measuring Risk	Essential Risk Information	Risk Recording and Reporting
	Communicating Risk	Monitoring and Review	Risk Management Training	
		Other		

Enterprise Risk Management Policy and Procedures 2023

List of questions

Click on the question to be brought to the answer

A. Objectives and Uncertainty

1. [What do we mean by objectives?](#)
2. [What do we mean by uncertainty?](#)

B. Risk and Risk Management

1. [What is risk?](#)
2. [What has uncertainty got to do with risk?](#)
3. [What is risk management?](#)
4. [Do we have a responsibility to manage risk?](#)
5. [What does “managing the effect of uncertainty” mean?](#)
6. [What is a risk event?](#)
7. [How do I describe a risk?](#)
8. [Is Health and Safety within the scope of the policy?](#)

C. Identifying Risk

1. [How do we identify risks?](#)
2. [What can help us identify risks?](#)

D. Understanding Risks

1. [What can help me to describe a risk?](#)
2. [Why is it important to understand the likelihood and impact of a risk?](#)
3. [What do we mean by risk velocity?](#)

E. Risk Analysis

1. [What is Inherent Risk?](#)
2. [What is Residual Risk?](#)
3. [What is the rationale for requiring inherent and residual risk levels?](#)
4. [What is a control and why are controls important?](#)
5. [What is an effective control and why is it important?](#)
6. [What types of controls are there?](#)
7. [Am I required to categorise controls into the four control types?](#)
8. [How do I rate a risk?](#)

Enterprise Risk Management Policy and Procedures 2023

F. Risk Evaluation

1. [What do I do after I've assessed the Inherent and Residual risk rating?](#)
2. [What is an acceptable level of risk?](#)
3. [What is target risk rating?](#)
4. [What do you mean by accept, reduce, transfer or avoid?](#)
5. [What is the HSE Risk Assessment Tool and where do I use it?](#)

G. Responding to Risk

1. [How do we manage risks?](#)
2. [What are examples of risk 'controls'?](#)
3. [What are some of the essential conditions of 'controls'?](#)
4. [Who is responsible for managing risk?](#)

H. Measuring Risk

1. [Why do we measure risk?](#)
2. [Does this mean I don't have to worry about the less serious risks?](#)
3. [What are we measuring?](#)
4. [How do we measure risk?](#)
5. [Is the measurement of risk subjective?](#)

I. Essential Risk Information

1. [What is the essential information I should have in relation to a risk?](#)
2. [What is a risk register?](#)

J. Risk Recording and Reporting

1. [Where do I record my risk?](#)
2. [How do I complete my risk register?](#)
3. [Who reviews the risk register and how often?](#)
4. [What does a good risk register look like?](#)
5. [How many risks should be on my risk register?](#)
6. [Who is responsible for the Risk Register and identification of risks?](#)
7. [I don't currently have a risk register, should I implement one?](#)
8. [What is the Corporate Risk Register?](#)
9. [Will there be a new electronic risk register system in place for the HSE?](#)

Enterprise Risk Management Policy and Procedures 2023

K. Communicating Risk

1. [Why is communication important in the risk management process?](#)
2. [What responsibilities do Line Managers have?](#)
3. [Are there more formal mechanisms for risk communication?](#)
4. [What is risk communication?](#)
5. [What is risk notification?](#)
6. [What is risk escalation and when do I escalate risk?](#)
7. [How and when do I escalate a risk?](#)
8. [What will my line manager do when they receive the escalated risk for consideration?](#)
9. [How will I be notified if my request from 'Proposed risk for consideration' was accepted?](#)
10. [How and when do I de-escalate a risk?](#)

L. Monitoring and Review

1. [How do I monitor risk in my area of responsibility?](#)

M. Risk Management Training

1. [Where can I get further training?](#)

N. Other

1. [What is the implementation date for the policy?](#)
2. [When do I commence using the new risk assessment form?](#)
3. [What is risk appetite and do I need to apply it?](#)
4. [My question is not listed, where can I find further guidance?](#)

Enterprise Risk Management Policy and Procedures 2023

Enterprise Risk Management Policy 2023

Frequently Asked Questions

A. Objectives and Uncertainty

1. What do we mean by objectives?

The **Key Messages** section of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Section 1.4 Key Definitions of the HSE Enterprise Risk Management Policy and Procedures 2023 defines risk as 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 also includes failing to maximise any opportunity that would help the HSE or service meet its objectives.'

Simply put, objectives provide clarity on the organisation's direction and focus the efforts of the organisation on its most important priorities. The HSE has clear objectives which are articulated in the **Corporate Plan**, with the **National Service Plan** setting out how these objectives will be progressed over each annual cycle.

2. What do we mean by uncertainty?

The **Key Messages** section of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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'

Simply put, even the best organisational decisions and plans are implemented in the future, whether that is tomorrow or next year. The future by its nature is uncertain.

Enterprise Risk Management Policy and Procedures 2023

B. Risk and Risk Management

1. What is risk?

Section 1.4 **Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines risk as 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 also includes failing to maximise any opportunity that would help the HSE or service meet its objectives.'

Simply put, a risk is therefore by definition a threat to us achieving an objective.

2. What has uncertainty got to do with risk?

The **Key Messages** section of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, because the future is uncertain so are the threats or risks we will face. This is further complicated by the fact that the number and type of possible risks is limitless. For this reason, we define the scope of risk to those threats which have the potential to prevent or derail our efforts to deliver on our objectives. This allows us to target our efforts on those threats or risks, which if not effectively managed, will have the highest impact.

3. What is risk management?

Section 2.1 **Scope, Context and Criteria** of the HSE Enterprise Risk Management Policy and Procedures 2023 states that '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.'

Simply put, each one of us unconsciously and naturally manage **risks** every day, in our homes, as we travel and at work. Risk management simply provides a structured approach to anticipating those threats, assists us in identifying the most effective way to manage them and provides the means by which we can measure how successful we have been in our efforts to reduce risk.

Enterprise Risk Management Policy and Procedures 2023

4. Do we have a responsibility to manage risk?

Section 1.5 **Roles and Responsibilities** of the HSE Enterprise Risk Management Policy and Procedures 2023 sets out the roles and responsibility in relation to risk management in the HSE, from the HSE Board to individual staff members.

Simply put, we have a duty to act in the best interests of those who rely on our services and the State who has entrusted us with significant resources and responsibilities to ensure we deliver our objectives as effectively as possible. Not to do so is a failure of governance.

5. What does “managing the effect of uncertainty” mean?

The **Key Messages** section of the HSE Enterprise Risk Management Policy and Procedures 2023 states ‘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.’

Simply put, consider what needs to go right to be able to consistently provide the safest, highest quality health and social care services and what **risk events** could arise that would prevent this?

6. What is a risk event?

Appendix 1: **Glossary of Terms** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines a ‘risk event’ as an ‘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.’

Simply put, a predicted risk becomes an event when it occurs. That is, it is a tangible event, you experience it or feel it. Before COVID-19, the risk or threat of a pandemic was an example of a predicted future event. However, with the arrival of COVID-19 in 2020 it very much became a reality, the predicted future event materialised. It became real.

7. How do I describe a risk?

Section **3.2 Procedure: Risk Description** of the HSE Enterprise Risk Management Policy and Procedures 2023 states that ‘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.’

The procedure document sets out the steps to follow in arriving at a good risk description.

Enterprise Risk Management Policy and Procedures 2023

Simply put, take your time and ask yourself ‘what is the risk event [possible future event/threat] that if it were to become a reality [materialise] could delay or prevent me from consistently providing the safest, highest quality health and social care services?’

In coming up with a good risk description there are three components. These are;

- the **risk event** that could threaten the achievement of my objective
- the **cause** of the risk event;
- the **impact** or consequence of that risk.

You may find it beneficial to follow the below template in describing your risks, setting them out as follows:

	Risk Event	Cause of the Risk	Impact or Consequence
Step 1	Capture and describe the risk event	Capture and describe the cause or source	Capture and describe the impact or consequence .
Formula	Risk Description = Risk event + cause [or source] + impact [or consequence]		
Step 2	Use the following sentence structure to set out your risk description: There is a risk of/to [Risk Event].....due to [Cause of risk].....resulting in [Impact]		

8. Is Health and Safety and Clinical risk assessments within the scope of the policy?

As set out in the policy, under **Section 3.1 Scope** there are specific risk assessment tools in place for Health and safety risk assessments (See <https://healthservice.hse.ie/staff/health-and-safety/risk-assessment>). The updated HSE Enterprise Risk Management Policy is enterprise wide and covers all organisational risks. It is therefore not intended to supersede or replace individual clinical or employee Health and Safety risk assessments. There are specific risk assessment tools in place for clinical risk assessment involving care and treatment relating to individual service users and for Health and Safety risk assessments. However the principles and tools contained in the ERM Policy and Procedures 2023 can be used to support a coordinated and strategic approach to clinical and Health and Safety risk assessment processes where relevant.

Simply put, any risk assessment relating to an individually-named staff member (a health and safety risk assessment) or an individually-named patient (a clinical risk assessment) is outside of the scope of this policy.

Enterprise Risk Management Policy and Procedures 2023

C. Identifying Risks

1. How do we identify risks?

Section **3.1 Procedure: Risk Identification** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on risk identification. It states ‘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.’

Simply put, 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.

2. What can help us identify risks?

Table 2 of the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on the sources and approaches for identifying risks. The sources of information, where possible, should be the most recent version available for review.

Simply put, start by asking questions such as: What could happen? How could it happen? Why might it happen? When could 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. Very often it may be someone’s experience and knowledge that can assist in identifying risks.

D. Understanding Risks

1. What can help me to describe a risk?

Section **3.2 Procedure: Risk Description** of the HSE Enterprise Risk Management Policy and Procedures 2023 states that ‘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.’ The procedure document sets out the steps to follow in arriving at a good risk description.

Simply put, when defining a risk, it is helpful to break it down into its essential components. These are the Risk Event, the Cause of the Risk and the Impact [consequence] of the Risk.

Enterprise Risk Management Policy and Procedures 2023

Risk Event: Risks should be described in terms of a 'risk event'. How will we know when it has occurred, how would we experience it? For example, the theoretical risk of a pandemic became a reality with the arrival of COVID-19, a theoretical cyber threat became a reality with the cyber-attack on the HSE's systems in 2021 and a theoretical threat of a fire disrupting a critical service became a reality in Wexford Hospital in March 2023.

Cause: Whereas the risk event defines the scope of our response, identifying the potential causes of the risk determines our response plan. The obvious cause isn't always the root cause, the one which starts the domino effect leading to the Risk Event.

Impact: Identifying the potential impact of the risk event can inform what actions need to be in place to ensure that if the event occurred, the negative impact is minimised or if it can't be minimised that we have the most effective response in place.

2. Why is it important to understand the likelihood and impact of a risk?

Section **3.3.1 Rating a Risk** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, understanding the likelihood of a risk occurring and its impact if it does, is essential to determining what our response to a risk will be. There are some risks for which it will be possible to reduce both its likelihood and impact. For others it may only be possible to mitigate the likelihood of it happening or the impact if it does.

For example, we may be able to reduce the likelihood of fires or floods shutting down critical infrastructure as well as the impact if these events do occur. Whereas we may not be able to reduce the likelihood of a pandemic occurring, but we can reduce its impact on the health service if it does.

3. What do we mean by risk velocity?

Section **3.4.1 Risk Velocity** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, risk velocity refers to how quickly we expect the risk to materialise and what is our response time likely to be if it does.

Enterprise Risk Management Policy and Procedures 2023

E. Risk Analysis

1. What is Inherent Risk?

Section **1.4 Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines inherent risk as ‘the level of risk before consideration of control and/or action measures.’

Simply put, inherent risk is the amount of risk before the consideration of any controls. This is the initial or preliminary risk rating determined as part of the first risk assessment.

2. What is Residual Risk?

Section **1.4 Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines residual risk as ‘the level of risk remaining after consideration of existing controls.’

Simply put, residual risk is the amount of risk remaining **after** consideration of controls. The residual risk rating changes frequently as completed actions may become controls and further reduce the risk rating. Actions which are not fully implemented have no impact on the residual risk rating.

3. What is the rationale for requiring inherent and residual risk levels?

The inherent risk demonstrates the level of risk that would occur should no measure be undertaken to reduce it. The residual risk is the level of risk remaining after consideration of existing controls, it demonstrates the effect that the controls are having on the risk. Establishing the inherent and residual risk levels enables clear communication of the importance of establishing controls and also the importance of maintaining the controls that are in place. The inherent, residual and target risk levels are aligned to the ISO international best practice risk management standard.

Simply put, inherent risk shows how high the risk is without any controls. Residual risk indicates the remaining risk after considering existing control measures, showing how well those measures work. Knowing both helps communicate why controls are vital and emphasises the need to maintain them. These concepts align with international risk management standards like ISO.

4. What is a control and why are controls important?

Section **1.4 Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines control as ‘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.’

Simply put, controls are measures we put in place to prevent or reduce the likelihood of the risk event occurring and its impact if it does occur.

Enterprise Risk Management Policy and Procedures 2023

5. What is an effective control and why is it important?

Section 3.3.8 **Effectiveness of Controls** from the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on control effectiveness. It states 'Controls can be broadly grouped into four types. Two types of controls, **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.'

Simply put, in the HSE, a control is a measure that is in place which is working effectively and operating to reduce either the likelihood or impact of a risk. A control must be verifiable [evidence of it working]. Controls are important because when they are designed and operating effectively they reduce the likelihood and/or consequence of a risk event occurring.

6. What types of controls are there?

Section **3.3.8 Effectiveness of Controls** from the HSE Enterprise Risk Management Policy and Procedures 2023 provides examples of each control type.

Proactive Controls:

Preventative 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.

Reactive Controls:

Detective controls aim to identify a breach after the event. Examples include internal audits, clinical audits, and 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 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

Enterprise Risk Management Policy and Procedures 2023

preventative controls.'

Simply put, there are two categories of controls, proactive and reactive. Proactive control provide direction in the form of policies and training for example. Preventative controls are strong controls as they prevent the risk event occurring in the first place, for example the use of passwords to protect against unauthorised access to ICT systems. Reactive controls happen after the risk event has occurred. They detect if the event occurred e.g. fire alarms in building and corrective controls are actions to correct the event if it occurs e.g. sprinkler system to put out a fire. The four control types are Preventative, Directive, Detective and Corrective.

7. Am I required to categorise controls into the four control types?

It is encouraged to consider the type of controls that are in place. This is a useful exercise that helps to determine the level of effectiveness that each of the control measures offer, with Preventative Controls - which are Proactive Controls - being the most effective type of control in reducing a risk.

Simply put, check the types of controls you have in place. The best type of controls to reduce risk is Preventative Controls and therefore it is smart to make sure that you include Preventative Control(s) if possible.

8. How do I rate a risk?

Section **3.3 Procedure: Risk Analysis (including Risk Rating)** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance on how to rate a risk. It states 'The process for rating risk is:

- 1) Using the Likelihood Table, in 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, in 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, in Appendix 2, align the score to a risk rating of High, Medium or Low.'

The HSE has adapted a standardised approach to the assignment of likelihood and impact scores for the rating of the risk. The Risk Assessment Tool, in 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.'

Simply put, risk is measured in terms of two dimensions, likelihood and impact i.e. the likelihood (probability) of the risk occurring and the impact (consequence) of the risk event should it occur.

1. Assess the likelihood of the risk event occurring having assessed the impact. Pick the best fit on the 1-5 scale from the Likelihood Table.
2. Assess the impact refer to the HSE Risk Assessment Tool and identify the worst,

Enterprise Risk Management Policy and Procedures 2023

realistic, primary impact category should the risk event occur. Pick the best fit on the 1-5 scale. It is not necessary to address each category.

Likelihood x Impact = Risk Score. Each risk score is associated with either High, Medium or Low rating depending on the score. Refer to the risk rating matrix in the HSE Risk Assessment Tool for more information.

F. Risk Evaluation

1. What do I do after I've assessed the Inherent and Residual risk rating?

Section 3.4 Procedure: Risk Evaluation of the HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance in relation to risk evaluation. It states '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.'

Simply put, decide whether the risk rating is acceptable or unacceptable. If acceptable, there is a requirement to monitor the risk going forward. If the risk rating is unacceptable, the risk is treated/reduced, transferred or avoided. The majority of risks in the HSE will require treatment, meaning a plan must be put in place to reduce the likelihood and/or impact of the risk event occurring.

2. What is an acceptable level of risk?

Section 3.4 Procedure: Risk Evaluation of the HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance in relation to risk evaluation. It states '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.'

Simply put, at national or Senior Management level, risks to the strategic objectives of the

Enterprise Risk Management Policy and Procedures 2023

organisation are considered against the HSE's Risk Appetite Statement to determine what level of risk is acceptable. At a regional, service, or individual unit level, the risks to the objectives or goals would be assessed against the desired target risk rating. If you are unsure please discuss with your line manager in the first instance.

3. What is target risk rating?

Section **1.4 Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines target risk as 'the planned level of risk after consideration of both control and action measures

Simply put, the target risk rating is risk remaining following the finalisation of all actions on the plan to reduce the risk.

4. What do you mean by accept, reduce, transfer or avoid?

Section **2.2.3 Risk Evaluation** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on risk evaluation. It states, '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.'

Simply put,

1. To **reduce** risk means to put a plan in place to reduce the likelihood and/or impact of the risk event occurring.
2. To **transfer** risk in the HSE usually means to escalate it to next level of management.
[See Communication and Consultation for more information on risk escalation]
3. To **avoid** risk, simply means to stop the risky activity altogether.

5. What is the HSE Risk Assessment Tool and where do I use it?

The **HSE Risk Assessment Tool** is provided in Appendix 2 of the HSE Enterprise Risk Management Policy and Procedures 2023.

Simply put, the HSE Risk Assessment Tool is a standardised approach to the assignment of likelihood and impact scores and the rating of risk. This tool should be applied uniformly to all processes where risk assessment is required.

Enterprise Risk Management Policy and Procedures 2023

G. Responding to Risk

1. How do we manage risks?

Section **3.3.8 Effectiveness of Controls** from the HSE Enterprise Risk Management Policy and Procedures 2023 provides examples of each control type.

Proactive Controls:

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.

Reactive Controls

Detective controls aim to identify a breach after the event. Examples include internal audits, clinical audits, and 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 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 controls.'

Simply put, having clarity on the Risk Event, its Cause(s) and Impact, we then need to put in place measures, which is Controls, aimed at either eliminating the threat, or reducing it.

2. What are examples of risk 'controls'?

Section **3.3.8 Effectiveness of Controls** from the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on control effectiveness. It states '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.'

Simply put, 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. A control must be verifiable [evidence of it working]. Controls are important because when they are designed and operating effectively they reduce the likelihood and/or consequence of a risk event occurring.

3. What are some of the essential conditions of 'controls'?

Section **1.4 Key Definitions** of the HSE Enterprise Risk Management Policy and Procedures 2023 defines control as '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

Enterprise Risk Management Policy and Procedures 2023

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.'

Simply put, the essential conditions of a control are that they *must: be in place, designed appropriately; working effectively and have a direct influence on reducing the likelihood and/or impact of the risk.*

4. Who is responsible for managing risk?

Section **1.5 Roles and Responsibilities** of the HSE Enterprise Risk Management Policy and Procedures 2023 sets out the roles and responsibility in relation to risk management in the HSE, from the HSE Board to individual staff members. It states '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.'

Simply put, responsibility for identifying and managing risk lies at the level the risk is expected to occur. There may be occasions where responsibility for managing the risk transfers to a higher level of management. Any transfer of responsibility for risk is however subject to a formal decision and acceptance of responsibility by the person to whom it transfers.

H. Measuring Risk

1. Why do we measure risk?

Section **3.3.1 Rating a Risk** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, measuring the level of risk helps to understand how serious the risk is. This means we can focus our efforts on managing the most serious risks.

2. Does this mean I don't have to worry about the less serious risks?

Section **3.4 Procedure: Risk Evaluation** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance in relation to risk evaluation.

It states '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)

Enterprise Risk Management Policy and Procedures 2023

- The level of risk is Low and does not warrant using resources to treat.
- The opportunities involved significantly outweigh the threats'

Simply put, while it may not be necessary to focus our efforts on the less serious risks, we may need to monitor them as a risk may change quickly and our ability to respond quickly to that change may be critical.

3. What are we measuring?

Section **3.3.1 Rating a Risk** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, when measuring risk we look at two things: the likelihood or probability of it materialising and its potential impact if it does. Understanding the speed at which a threat could materialise, or our expected response time if it does, can also be an important consideration.

4. How do we measure risk?

Section **3.3 Procedure: Risk Analysis (including Risk Rating)** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance on how to rate a risk. It states 'The process for rating risk is:

- 1) Using the Likelihood Table, in 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, in 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, in 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, in 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.

Simply put, a scoring system is used to measure the level of risk. Both the likelihood and impact of the risk are scored on a scale of 1 to 5, multiplied, and then mapped onto a 5x5 matrix. This means the lowest possible score is 1 [low risk] and the highest is 25 [High risk]. 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 risk], the level after we put

Enterprise Risk Management Policy and Procedures 2023

effective controls in place [residual risk] and how far we want to reduce the level of risk through the controls we put in place [target risk].

5. Is the measurement of risk subjective?

Section **2.2 Risk Management Process** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on risk assessment. It states ‘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.’

Simply put, the scoring of risks should be informed by objective data. This may be performance, incident, financial or other forms of data.

I. Essential Risk Information

1. What is the essential information I should have in relation to a risk?

Section **3.2 Procedure: Risk Description** of the HSE Enterprise Risk Management Policy and Procedures states that ‘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.’ The procedure document sets out the steps to follow in arriving at a good risk description.

Simply put, the minimum information we should have in relation to a risk is the objective the risk relates to; a precise description of the risk [Event, Cause, Impact], what we are trying to control [Likelihood and/ or Impact], how serious the risk is [risk rating of High, Medium or Low], the measures we have in place to manage the risk [Controls].

2. What is a risk register?

Section **3.6 Procedure: Recording and Reporting** of the HSE Enterprise Risk Management Policy and Procedures 2023 states ‘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 etc.]’

Simply put, in the same way, we also rely on a report - the Risk Register - that brings together in a summary form, all the essential information relating to the risks being managed. This includes a clear description of the risks, ranks those risks by how serious they are, the measures that are in place to control the risk, the additional controls required to further reduce the risk and the measurement of the current level of risk. A good Risk Register is therefore more than a list of the risks we face. It is an essential repository and resource that summarises the critical

Enterprise Risk Management Policy and Procedures 2023

information we need to understand and manage the risks we face and serves as a means of reporting on our 'performance' in reducing those risks.

J. Risk Recording and Reporting

1. Where do I record my risk?

Section **3.6 Procedure: Recording and Reporting** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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.'

Simply put, a risk assessment form is available for recording individual risk assessments. Completed risk assessments are recorded in a risk register.

2. How do I complete my risk register?

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

The HSE Enterprise Risk Management Policy and Procedures 2023 provides detailed guidance and states that 'Training on how to complete the HSE Excel Risk Register Tool is available on HSELand via the following link: <http://bit.ly/2N4bpPE>. Where the electronic risk register has been made available to your area, this must be used over the excel risk register.'

Simply put, training on how to complete the HSE Excel Risk Register Tool is available on HSELand via the following link: <http://bit.ly/2N4bpPE>. On sign in to HSELand, the module can be accessed through the new **Risk Management** folder in the **Quality, Leadership & Management** section. There is also an Excel Risk Register training manual available at the following link: <https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/hse-enterprise-risk-management-supporting-tools/erm-risk-register-training-manual1.pdf>

3. Who reviews the risk register and how often?

Section **3.8 Procedure: Monitoring and Review** of the HSE Enterprise Risk Management Policy and Procedures 2023 states '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 quarterly basis.'

Simply put, risk is monitored on an ongoing basis by the Risk Owner, Risk Lead and local manager. Risk Management should be an agenda item at all management and committee meetings. It is recommended that the risk register should be reviewed in its entirety by the

Enterprise Risk Management Policy and Procedures 2023

management team at least on a quarterly basis.

4. What does a good risk register look like?

Section **3.6 Procedure: Recording and Reporting** of the HSE Enterprise Risk Management Policy and Procedures 2023 states ‘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 etc.]’.

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.

5. How many risks should be on my risk register?

Section **3.6 Procedure: Recording and Reporting** of the HSE Enterprise Risk Management Policy and Procedures 2023 states ‘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 etc.]’.

Simply put, think quality over quantity. It should be a manageable amount of risks. It should contain key significant risks as opposed to ongoing issues.

6. Who is responsible for the Risk Register and identification of risks?

Section **3.1 Procedure: Risk Identification** of the HSE Enterprise Risk Management Policy and Procedures 2023 provides guidance on risk identification. It states ‘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.’

Section **1.5 Roles and Responsibilities** of the HSE Enterprise Risk Management Policy and Procedures 2023 sets out the roles and responsibility in relation to risk management in the HSE, from the HSE Board to individual staff members.

Simply put, the area Manager is the risk custodian tasked with the review of the risk register, he/she is not solely responsible for identification of all risks. Identification, analysis and evaluation of key risks is the collective responsibility of all Managers within the HSE, to identify key risks events that may impact their area of responsibility. Each risk should be assigned to a Risk Owner who is responsible for ensuring that the risk is managed appropriately.

7. I don't currently have a risk register, should I implement one?

Section **2.5 Communication and Consultation** of the HSE Enterprise Risk Management Policy and Procedures states ‘a fundamental principle is that risk is managed at the level at which it is expected to materialise.’

Enterprise Risk Management Policy and Procedures 2023

Simply put, if you have identified a risk which is being managed locally, the risk assessment should be completed and recorded on a local risk register. It is important to note that risk registers are also relevant for Projects, Committees, and Oversight Groups etc. outside of the standard organisational structure.

8. What is the Corporate Risk Register?

Section 2.7.2 **HSE's Corporate Risk Register** of the HSE Enterprise Risk Management Policy and Procedures states the HSE's principal risks are recorded on the HSE's Corporate Risk Register (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.'

Simply put, the Corporate Risk Register refers to the principal risks and uncertainties of the HSE, which are published annually in the Annual Report. Some Hospitals/Hospital Groups/other local organisations/functions also use the term Corporate Risk Register to refer to the principal risks and uncertainties of that organisation/function.

9. Will there be a new electronic risk register system in place for the HSE?

This is being explored currently – an electronic risk register, separate from the excel risk register, is being piloted. Roll out of the system will be communicated on availability.

Simply put, we're currently testing an electronic risk register. Once it's ready to go, we'll let you know when the system will be implemented.

K. Communicating Risk

1. Why is communication important in the risk management process?

Section 3.7 **Procedure: Communication and Consultation** of the HSE Enterprise Risk Management Policy and Procedures 2023, states '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 it that are within their span of control. The risk, therefore, remains on their risk register.'

Enterprise Risk Management Policy and Procedures 2023

Simply put, communication and consultation is essential to the process of identifying, assessing and responding to a risk. 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.

2. What responsibilities do Line Managers have?

Section **1.5 Roles and Responsibilities** of the HSE Enterprise Risk Management Policy and Procedures 2023 sets out the roles and responsibility in relation to risk management in the HSE, from the HSE Board to individual staff members.

Simply put, line managers have a particular responsibility to understand the risks within their area of responsibility and to ensure they are being effectively managed.

3. Are there more formal mechanisms for risk communication?

Section **3.7 Procedure: Communication and Consultation** of the HSE Enterprise Risk Management Policy and Procedures 2023, provided detailed guidance on the formal mechanisms for risk communication and states '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 it that are within their span of control. The risk, therefore, remains on their risk register.'

Simply put, communication of risk may also serve a more formal purpose.

Notification to the next level of management that a new and serious risk has emerged or that an existing risk has become more serious.

Escalation where responsibility for managing the risk is accepted by the next level of management. This may be due to the nature of the risk, that the risk is more systemic or because the measures required to modify the risk are not within the control of the original owner of the risk. Communicating risk must always have a clear objective and outcome.

4. What is risk communication?

Section **3.7.1 Risk Communication** of the HSE Enterprise Risk Management Policy and Procedures 2023, states '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

Enterprise Risk Management Policy and Procedures 2023

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.’

Simply put, there are three levels of communication, each of which increases the formality associated with the communication, these are risk communication, notification and escalation. Risk communication is the sharing or exchanging of information and gaining a common understanding relating to risk events.

5. What is risk notification?

Section **3.7.2 Risk Notification** of the HSE Enterprise Risk Management Policy and Procedures 2023, states ‘risk notification is an exchange of information to support the decision-making process. A risk notification is not a formal escalation of risk.’

Simply put, risk notification is formally recognising the risk is increasing or is not being managed effectively, and it requires notification to the next level of management.

6. What is risk escalation and when do I escalate risk?

Section **3.7.3 Risk Escalation** of the HSE Enterprise Risk Management Policy and Procedures 2023, states ‘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.’

Simply put, risk escalation is required in certain circumstances. These could include when a risk

Enterprise Risk Management Policy and Procedures 2023

can no longer be managed at the level in which it is expected to materialise.

7. How and when do I escalate a risk?

Section **3.7.3 Risk Escalation** of the HSE Enterprise Risk Management Policy and Procedures 2023, states '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.'

Simply put, a fundamental principle is that risk is managed at the level at which it is expected to materialise. Risk escalation is required in certain circumstances. Risks proposed for notification, escalation or inclusion on another risk register are subject to a formal request for consideration.

A 'Proposed risk for inclusion' form is available on the Risk Management Support Tools website page at: [Risk Management Support Tools - HSE.ie](#)

8. What will my line manager do when they receive the escalated risk for consideration?

Section **3.7.3 Risk Escalation** of the HSE Enterprise Risk Management Policy and Procedures 2023, states '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.

Enterprise Risk Management Policy and Procedures 2023

Simply put, when a risk is proposed for consideration to a more Senior Manager, that Manager may:

- Review the risk and decide not to accept it but seeks assurances in relation to the adequacy of its management within the referring service area. This can include the provision of resources/authorities to assist in its mitigation.
- Decide that the risk should be included on their risks register. Reasons for inclusion are generally due to one of two reasons:
 - That the significance of the risk is such that it requires oversight on their register, or
 - Though the risk was identified by the area of the service that notified it, that it has resonance across the service as a whole and rather than just manage it on each individual register that many of the actions identified as required are better managed collectively. For example, if an overarching policy or process is required. If there are multiple services that could be impacted by this risk, this may involve informing and/or consultation with other services that may be impacted by a similar risk on how to best mitigate this risk.

On accepting the notified risk, the 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,
- to members of their Management Team or
- to their own Line Manager.

9. How will I be notified if my request from ‘Proposed risk for consideration’ was accepted?

Section **3.7.3 Risk Escalation** of the HSE Enterprise Risk Management Policy and Procedures 2023, states ‘the outcome will be communicated back to the service that proposed the risk for consideration.’

Simply put, the decision will be communicated back to the service that proposed the risk for consideration.

10. How and when do I de-escalate a risk?

Section **3.8.4 De-escalating Risk** of the HSE Enterprise Risk Management Policy and Procedures 2023, states ‘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.’

Enterprise Risk Management Policy and Procedures 2023

Simply put, if a risk had been accepted onto a higher register and treatment has reduced the risk to an acceptable level, then 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.

L. Monitoring and Review

1. How do I monitor risk in my area of responsibility?

Section **3.8.1 Reviewing the entirety of the Register** of the HSE Enterprise Risk Management Policy and Procedures 2023, states ‘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 quarterly basis.’

Simply put, line managers have a responsibility to understand the threats and opportunities within their area of responsibility and each area should have in place a process to review and report on risk regularly. Some communications may not use the word ‘risk’ but items may be discussed and topics covered where questions are asked such as ‘what is the worst case scenario?’ 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.

M. Risk Management Training

1. Where can I get further training?

Please refer to the dedicated page on Enterprise Risk Management training on the HSE website for further training details, which includes an introductory video to the policy and recording of a national webinar of the policy launch. This is at the following location: <https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/2023-hse-enterprise-risk-management-training/>

The ‘**Fundamentals of Enterprise Risk Management**’ eLearning module on HSELand is designed to support staff in understanding each of the steps in the risk management process. This course is aimed at all staff who have a role in risk management.

Login to HSELand at <https://www.hseland.ie/dash/Account/Login> and search for ‘Fundamentals of Enterprise Risk Management’ in the course catalogue. Alternatively, the module is accessible through Quality, Leadership & Management section, in the ‘Risk Management’ folder.

In addition, there were a series of ‘**Overview on Key Policy Changes**’ train the trainer sessions including dedicated Q&A time, hosted in October 2023. Presentation slides and speaking notes of this session were shared with all attendees. This session continues to be available to Quality, Patient Safety and Improvement Managers, Advisor and Leads throughout the HSE by contacting erm.queries@hse.ie.

Supporting tools including this **FAQ document**, the Risk Assessment Form template in MS word format and is available to print (in colour or black-and-white) and download, and

Enterprise Risk Management Policy and Procedures 2023

additional support tools including the PESTLE and Bow-tie tools and Horizon scanning are available as individual documents on the HSE website

<https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/hse-enterprise-risk-management-supporting-tools/>

Excel Risk Register:

Excel Risk Register training is available as an eLearning module on HSElanD: Using the HSE Excel Risk Register <https://www.hseland.ie/> The module can be accessed through the new Risk Management folder in the Quality, Leadership & Management section or Access HSElanD: <http://bit.ly/2N4bpPE>

A copy of the 2023 Excel Risk Register Template is on the HSE website:

<https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/risk-management-support-tools.html>

If you require support regarding the Excel Risk Register, please contact: erm.queries@hse.ie

N. Other

1. What is the implementation date for the policy?

The policy's implementation date is 1st November 2023. From the 1st November 2023, each newly identified risk should be assessed and reported in line with the updated policy, risk assessment form and excel risk register. Additionally, from the 1st November each new risk will have the three risk levels. Each area should develop an implementation plan, that sets out a timeframe for when the current risk assessment forms and risk register will be reported using the updated format.

Simply put, from 1st November 2023, all new risks must be assessed and reported using the new policy, risk assessment form and Excel risk register. Also, each new risk should have three risk levels. Each area needs a plan for when they'll start using the updated forms and register, following a set timeline.

2. When do I commence using the new risk assessment form?

From the 1st November 2023, each newly identified risk should be assessed in line with the updated policy using the 2023 risk assessment form. Blank templates of this risk assessment form are available to print - in colour and in black-and-white - and to download from the HSE website in the 2023 HSE Enterprise Risk Management Supporting Tools section <https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/hse-enterprise-risk-management-supporting-tools/>

A worked example is also available on the HSE website.

Simply put, from 1st November 2023, all new risks must be assessed using the 2023 HSE risk assessment form.

Enterprise Risk Management Policy and Procedures 2023

3. What is risk appetite and do I need to apply it?

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. The policy therefore sets out what Risk Appetite is, what a risk appetite statement is and how it is to be used. It is recognised that Risk Appetite is not yet in place throughout the organisation and will progressively become a feature of the HSE's Enterprise Risk Management approach as risk maturity evolves.

Simply put, risk appetite is how much risk the HSE is comfortable taking.

4. My question is not listed, where can I find further guidance?

Further support tools can be found at the following location:

<https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/hse-enterprise-risk-management-supporting-tools/>

Please contact the ERM Programme at erm.queries@hse.ie if you have any queries regarding the implementation of the Enterprise Risk Management Policy and Procedures 2023.

Simply put, please refer to the HSE website for further details to access the ERM policy and supporting documents <https://www.hse.ie/eng/about/who/riskmanagement/risk-management-documentation/>. If you have questions about implementing the Enterprise Risk Management Policy and Procedures 2023, email erm.queries@hse.ie.