Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HSE Integrated Risk Management Policy

Part 3

Managing and Monitoring Risk Registers

Guidance for Managers

HSE Integrated Risk Management Policy

Part 3

Managing and Monitoring Risk Registers

Guidance for Managers

TABLE OF CONTENTS

1. Introduction 4
2. Overview of the Risk Management Process 4
3. Purpose 5
4. Scope 5
5. Definitions 5
6. Roles and Responsibilities 5
7. Maintaining the Risk Register 6
   - **7.1** Updating existing risks on the register 6
   - **7.2** Inclusion of new risks on the register 7
   - **7.3** Reviewing the entirety of the register 7
8. Re-Rating Risk 8
9. Changing the Risk Status 8
10. De-escalating Risk 9
11. Risk Notification 9
12. Related Policy and Guidance 9

Appendix 1: Definitions 10

1. Introduction

Risk management seeks to identify and manage those things that, should they occur, would prevent an organisation from achieving its objectives. It does this by estimating both the impact of the risk, i.e. how bad will the outcome of the risk be if it occurs and what is the likelihood that the event will happen. In a nutshell this means that rather than wait for things to go wrong (incidents) we should adopt an approach which anticipates what might go wrong and put in place any actions that may prevent an incident occurring.

The upside of adopting a risk management approach is that we are more likely to achieve our objectives and less likely to have negative outcomes. It is however important to note that positive risk taking (as opposed to risk avoidance) within a framework of safety can and should be encouraged in order to support Service Users attain their potential. This is particularly relevant in social care settings where the ethos espoused is one of service user self-determination.

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

The HSE is committed to developing a risk management culture, where a proactive approach to risk is integrated and embedded into management processes at all levels in the organisation and where all staff are alert to risks, capable of an appropriate level of risk assessment and confident to report risk or opportunities perceived to be important in relation to priorities.

To support Managers in delivering on their commitments in relation to the HSE's Integrated Risk Management Policy a number of pieces of guidance have been developed.

A range of tools are also available, detail of which can be found on http://hse.ie/eng/about/QAVD/

2. Overview of the Risk Management Process

The HSE's approach to risk management is aligned to the ISO 31000 an overview of which is provided at Figure 1 below.

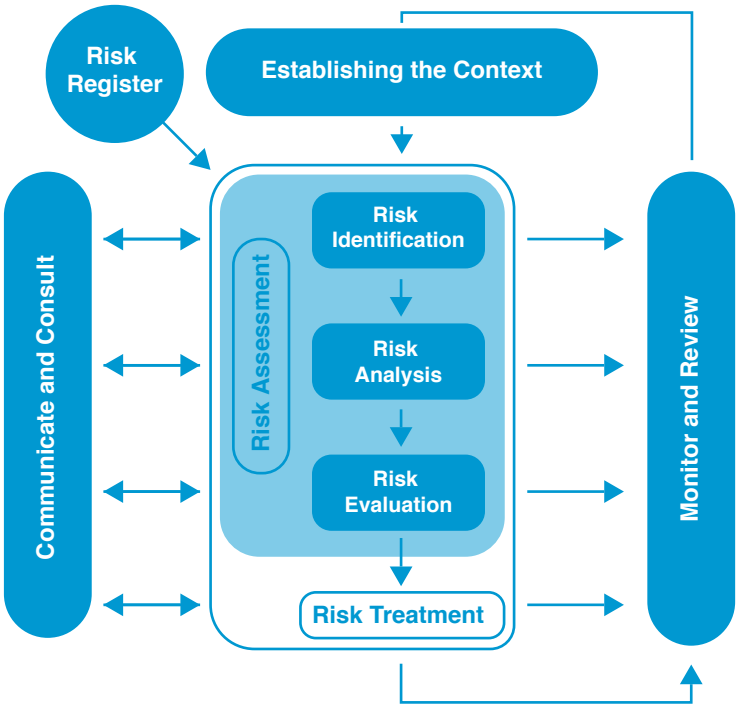

Figure 1. Risk Management Process

The process adopted requires Managers, within the context of their area of responsibility and in consultation with their staff, to identify analyse and evaluate risks and to put in place any treatment (actions) required to reduce those risks.

Where a formal management plan is required the outcome of this process is documented in the relevant risk register and monitored and reviewed by the relevant Management Team.

3. Purpose

The HSE has developed a number of pieces of guidance to support staff in complying with the HSE's Integrated Risk Management Policy. These are

Part 1 Managing Risk in Everyday Practice

Part 2 Risk Assessment and Treatment

Part 3 Managing and Monitoring Risk Registers

This is **Part 3** of the guidance suite. The purpose of this guidance is to assist you and your Management Team with the process for managing and monitoring your risk register.

4. Scope

This guidance is for use in the management of service and organisational related risk and applies to all staff that holds a management role at any level of the organisation. It applies to both HSE and HSE-funded services.

5. Definitions

A full list of definitions relating to risk management terms used in this and supporting documents is contained in **Appendix 1**.

6. Roles and Responsibilities

Whereas every staff member is responsible for identifying risk within the context of their work, risk management is a line management responsibility and is a core management process. The Line Manager is also responsible to check that the risk register in their area of responsibility is compliant with the HSE Integrated Risk Management Policy and supporting Guidance.

The role of the risk management professionals for example Risk/QPS Advisors is to support, facilitate and advise Line Managers on the technical aspects of the risk management process i.e. they are not responsible for managing risk identified within a service area.

7. Maintaining the Risk Register

Updating the risk register is an ongoing process and updates can occur at any time however to ensure the register is actively reviewed and updated a scheduled process should be in place to ensure effective monitoring at Management Team.

Whilst it is not the purpose of this guidance to dictate the frequency of review of the risk register there are three processes outlined which should attach to the maintenance of the register:

7.1 Updating existing risks on the register

7.2 Identifying and adding risks to the existing register

7.3 Reviewing the entirety of the register

The following provides guidance in relation to each of these processes.

7.1 Updating existing risks on the register

To enable this, the Risk Lead should facilitate in association with Risk Coordinators the following steps for existing risks on the register.

7.1.1 'Action owners' assigned must provide an update on progress to the Risk Owner on any action assigned to them where the 'due date' is due. Staff who identified the risk may also request an update on progress.

7.1.2 Where evidence is available that an action is implemented/complete and added control is evident this will be reflected in the risk register. In such an instance the 'additional control required' should be closed and the new control should be reflected in the 'existing control' section of the register.

7.1.3 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.

7.1.4 When the action updates have been reflected on the register, the revised register should, in advance of the Management Team meeting, be sent to Managers identified on the register as Risk Coordinators. Risk Coordinators in advance of the meeting must review each of the risks for which they are assigned a coordinating responsibility. This must include a review of the risk description to ensure it remains valid and a review of the 'existing controls'. As the internal or external context may have changed since the risk was previously reviewed what were considered 'strong' controls may no longer be applicable or some new ones may be now in place which are not related to the action plan and require inclusion in the register. Any areas requiring amendment should be notified immediately to the Risk Lead so that these may be reflected in the register.

7.1.5 The Risk Lead in consultation with Risk Coordinators should also review the risk rating in context of the above and be in a position to recommend re-rating of the risk at the Management Team meeting if relevant. (Re-rating Risk – see **Section 8 below**). 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, recommendations for re-rating (Re-rating Risk – see **Section 8 below**)/changing the risk status of existing risks (Changing the Risk Status – see **Section 9 below**)/de-escalation (Risk De-escalation **–** see **Section 10 below**).

7.1.6 The following will be agreed at Management Team in relation to the report

- Amended time frames for 'actions due and incomplete' will be agreed
- Responsibility for identifying actions relating to any existing controls whose status has changed will be assigned to a member of the Management Team.
- Decide if any additional actions/controls above those already identified on the register are required.

- Acceptance/rejection of recommendations for re-rating/de-escalation/changes to the risk status of existing risks.
- Consider whether any risks require notification to the Manager to which your service reports (Risk Notification – see **Section 11** below)

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

Top Tip: To ensure effective use of time at the Management Team meeting updating of the register should be done in advance of the meeting. This will mean that the report brought can form the basis of any decision making required. To facilitate this, the Risk Lead will require the timely cooperation of Risk Coordinators and Management Team members.

7.2 Inclusion of new risks on the register

7.2.1 The Management Team should agree the criteria for inclusion of new risks on the register. Such criteria may include risks that require a Management Team 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.

7.2.2 Proposals for the addition of new risks onto the register can be made at any time but the decision to include these should be made at the Management Team. In such instances if it is decided that the risk should be included on the register, the Senior Manager will nominate a Risk Coordinator 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.

Top Tip: Prior to commissioning the assessment of a new risk the Management Team should take time to clearly define the risk (see describing risk in Part 2 Risk Assessment and Treatment Guidance for Managers). Time taken at this point will assist the Risk Coordinator and Risk Lead with the process for Risk Analysis and Evaluation.

7.3 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 on a minimum of a bi-annual basis.

Top Tip: As the definition of risk is 'the effect of uncertainty on objectives', one of these sessions should be linked to the business/service planning cycle i.e. what are your objectives for the coming year and what are the risks attaching to their achievement?

8. Re-Rating Risk

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

For example, if a risk originally rated as having an 4 impact (major) x 5 likelihood (almost certain) before any additional controls were implemented it would have a risk score of **20 Red.**

3. RISK MATRIX

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

Where following the implementation of additional controls the likelihood of the risk occurring was reassessed as having reduced from 5 (almost certain) to 4 (likely) but the impact stayed at 4, the overall risk rating will still be red but the numeric rating will have reduced from **20 to 16.**

3. RISK MATRIX

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

Top Tip: In general, on re-rating it is the likelihood score that will reduce with the implementation of additional controls for example the better 'controlled' a risk is the less likely it is to happen. Conversely, the impact score often stays the same as on the original assessment as if it does happen 'the impact remains the impact.'

Re-rating the risk should be done by the Risk Lead in consultation with the person who acted as the Risk Coordinator at the time the risk was initially assessed. This is because it is the Risk Coordinator that has the expertise in relation to the subject matter of the risk and will be able to 'evaluate' the extent to which the completion of additional controls serves to reduce or 'control' the risk.

Where implementation of actions does not appear to be serving to reduce the risk, consideration should be given to reviewing the appropriateness of the actions identified and revising the actions planned. Re-rating the risk assists in evidencing that the risk is being actively managed.

9. Changing the Risk Status

Whilst under active management, a risk has a 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'.

Risks with a status of 'monitor' undergo periodic review for example quarterly or six monthly depending on the nature of the risk, to ensure that they remain mitigated 'as far as is reasonably practicable'. Risks that have all required actions completed and require no further action are assigned a 'closed' status are archived onto a 'closed register' for audit purposes.

10. 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 may have reduced to an acceptable or tolerable level or where 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.

11. Risk Notification

It is essential that there are clear routes and processes for the communication and notification of risk from one level of the organisation to another. However it is also important to realise that such communication and notification does not absolve the responsibility of the Service 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 register. When a risk is notified to a more Senior Manager, that Manager can:

- 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:
    1. That the significance of the risk is such that it requires oversight on their register, or
    2. Thought 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.

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 Line Manager.

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

12. Related Policy and Guidance

HSE Integrated Risk Management Policy, 2017

Managing Risk in Everyday Practice Guidance for Managers – (Risk Management Guidance Part 1, 2017)

Risk Assessment and Treatment Guidance for Managers – (Risk Management Guidance Part 2, 2017)

Policy and guidance are available at http://hse.ie/eng/about/QAVD/

Appendix 1: Definitions

These definitions are predominantly based on the terms and definitions from the International Risk Management Standard ISO 31000:2009.

Controls	A mechanism, process, procedure or action which can be verified, which seeks to reduce the likelihood and/or consequence of a risk. Controls include any process, policy, device, practice, or other actions which modify risk. They can exist or be required as additional in order to further mitigate the risk.
Establishing the Context	Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.
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.
Likelihood	The chance of something happening (also described as the probability or frequency of an event occurring).
Line Manager	A person with responsibility for directly managing individual employees or teams. In turn, they report to a higher level of management on the performance and well-being of the employees or teams they manage.
Monitor	To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change.
Operational Risk	Operational risks relate to the day-to-day delivery of activities, operational business plans and objectives. Operational risks typically have a short-term focus. Whilst they may impact a number of areas of the service, this does not necessarily make them a strategic risk. Operational risks may have the ability to impact strategic and other operational risks.
Project Risk	Project risks relate to the achievement and delivery of the project objectives and outcomes. The majority of project risks are short term in nature and exist for the term of the project, whilst some will be on-going and re-classified at the end of the project. Projects can be defined as temporary, with the aim of delivering outcomes within a specified timeframe.
Residual Risk Rating	The remaining level of risk after all treatment plans have been implemented.

Risk	Risk is the effect of uncertainty on objectives. It is measured in terms of consequences and likelihood. In the context of the HSE and its services, it is any condition or circumstance which may impact on 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 Acceptance	Informed decision to take a particular risk.
Risk Appetite	Amount and type of risk that an organisation is willing to pursue or retain.
Risk Assessment	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 Criteria	Terms of reference against which the significance of a risk is evaluated.
Risk Description	Structured statement of risk usually containing three elements: impact, cause and context.
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
Risk Identification	A systematic process applied to the organisation's objectives and activities to identify possible risk sources and causes and potential consequences or impacts should a risk occur.
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 Matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood.
Risk Owner	Person with the accountability and authority to manage a risk.
Risk Profile	A risk profile is a written description of a set of risks. A risk profile can include the risks that the entire organsation must manage or only those that a particular function or part of the organisation must address. (In the HSE, a services risk profile is set out in their risk register).
Risk Rating	The estimated level of risk taking into consideration the existing controls in place.

Risk Source	The source from which the risk was identified for example Incident Management, Audit, Health and Safety Risk Assessment, Inspection Report, Complaint
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	An organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.
Strategic Risk	A strategic risk has the ability to impact on the achievement/delivery of the HSE's strategic objectives/directions. Strategic risks relate to the highest level of objective for the HSE, which typically have a long-term focus and are linked to the HSE's Strategic Plan.
Treatment	Additional mechanisms, processes, procedures or actions to be implemented, which seek to reduce the current likelihood and/or consequence and reach the Residual Risk Rating.
Directorate	The Directorate is the governing authority of the HSE established following the enactment of the Health Service Executive (Governance) Act 2013.

Contact details:

Quality Assurance and Verification Division,
Dr. Steevens' Hospital,
Dublin 8.

Phone: 01 6352619

Publication Date: March 2017

Our Values
Care Compassion Trust Learning