Organisational Risk Management

Policy and Procedure

TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

Document Information and Revision History

Document Reference Number	PPPG 15/2016
Revision Number	1.0
Approval Date	July 2016
Next Revision Date	July 2018
Document Developed By	Quality Assurance Directorate
Document Approved By	Tusla Board
Responsibility for Implementation	All Tusla Employees
Responsibility for Review and Audit	Senior Managers and the Director of Quality Assurance

Table of Contents

1.0 INTRODUCTION

Organisations are affected by a wide range of internal and external factors that make their operating environments uncertain. These factors create uncertainty as to whether, and to what extent objectives can be met. The effect this uncertainty has on the achievement of an organisation's objectives is known as 'risk'.

When the management of risk is effective it generally goes unnoticed. Conversely, when it is absent or fails, the impact is often highly visible and felt across the entire organisation, rather than just at individual service or project level or by individual staff. The consequences may also be publicly embarrassing, politically damaging or compromising to the organisation.

The aim is not to eliminate risk, but to manage it. Risk management refers to the coordinated set of activities an organisation takes to direct and control risk.

Adopting good risk management ensures that an organisation can undertake its activities in the knowledge that appropriate and adequate measures are in place to maximise the opportunities, and minimise the negative or unanticipated effects of risk on the achievement of the organisation's objectives.

2.0 POLICY STATEMENT

The Child and Family Agency (Tusla) is committed to ensuring that risk management principles and practices form an integral part of its:

- Culture
- Governance and accountability arrangements
- Decision-making processes
- Strategic and operational planning
- Reporting, review, evaluation and improvement processes

Staff and managers at all levels across Tusla have an individual and collective responsibility for identifying and managing risk in day-to-day decision making and planning. In order for risk management to become part of everyday practices each person must recognise and accept this responsibility.

Risk management is not optional; it is a necessary consideration each time a decision is made, whether it is a decision which is taken in everyday operations (such as deciding work priorities, making budget or staffing decisions) or a decision taken about major policies, strategies or projects.

Risk management is not a static one-time process; it is a continual process that must be capable of adapting to changing internal and external environments.

Tusla is committed to establishing and providing the necessary structures, processes, training and other supports required to implement this policy and procedure.

Tusla requires the commitment of all staff in supporting this policy and in return will promote a positive and supportive environment that encourages individuals to identify risks and report adverse events promptly.

Risk management practices are required to be within the Agency's risk appetite which is currently under development. This will be made available to staff when completed.

2.1 Roles and Responsibilities

Risk Management (identification, measurement, assessment and management) is a line management function. Each Service Lead/Regional Manager/National Manager is responsible for the accountability arrangements for managing risk at all levels within Tusla. These arrangements should be part of the normal reporting mechanism to ensure that risk management is embedded into the business/service process.

At Tusla Board level, the Quality Assurance and Risk Committee is a subcommittee of the Board. It focuses principally on assisting the Board in fulfilling its duties by providing an independent and objective review in relation to non-financial risks. This is achieved through presenting the Corporate Risk Register and associated papers to the Board.

The National Quality, Risk Governance and Service Improvement Action Group comprises of senior managers who have an oversight and review function to support practice development by identifying trends through the monitoring of Quality Improvement Plans with the aim of providing assurances to the executive/senior management team.

At a national level, the Quality, Risk and Service Improvement Working Group provides assurances that risk management activity for all services is taking place in accordance with the Agency's risk management policy.

3.0 PURPOSE

The purpose of this policy and procedure is to formally affirm Tusla's commitment to building a risk management culture in which risks and opportunities are identified and managed effectively and to set-out Tusla's approach to the management of risk.

This policy and procedure:

- Communicates that risk management is everyone's responsibility
- Sets out respective responsibilities for the management of risk for all staff throughout Tusla
- Describes Tusla's approach to the management of risk i.e. procedures to be used in identifying, analysing, evaluating and controlling risks that can impact on the achievement of its objectives
- Provides guidance on the development and maintenance of risk registers
- Describes the procedure for the escalation of risks to the next management level.

4.0 SCOPE

This policy and procedure applies equally to the management of risks that arise at an organisation wide or strategic level, at an operational or day-to-day business level, or for new projects and new initiatives.

This policy does not apply to the management of individual client or service user risks. They should be held by individual departments and actioned through normal supervision and risk escalation procedures.

This policy and procedure applies to all staff and managers in all services and functions under Tusla's remit.

A glossary of terms and definitions can be found in Appendix I.

5.1 ACCOUNTABILITY AND RESPONSIBILITY ARRANGEMENTS

Figure 1 outlines the accountability and responsibility arrangements in relation to risk management in Tusla.

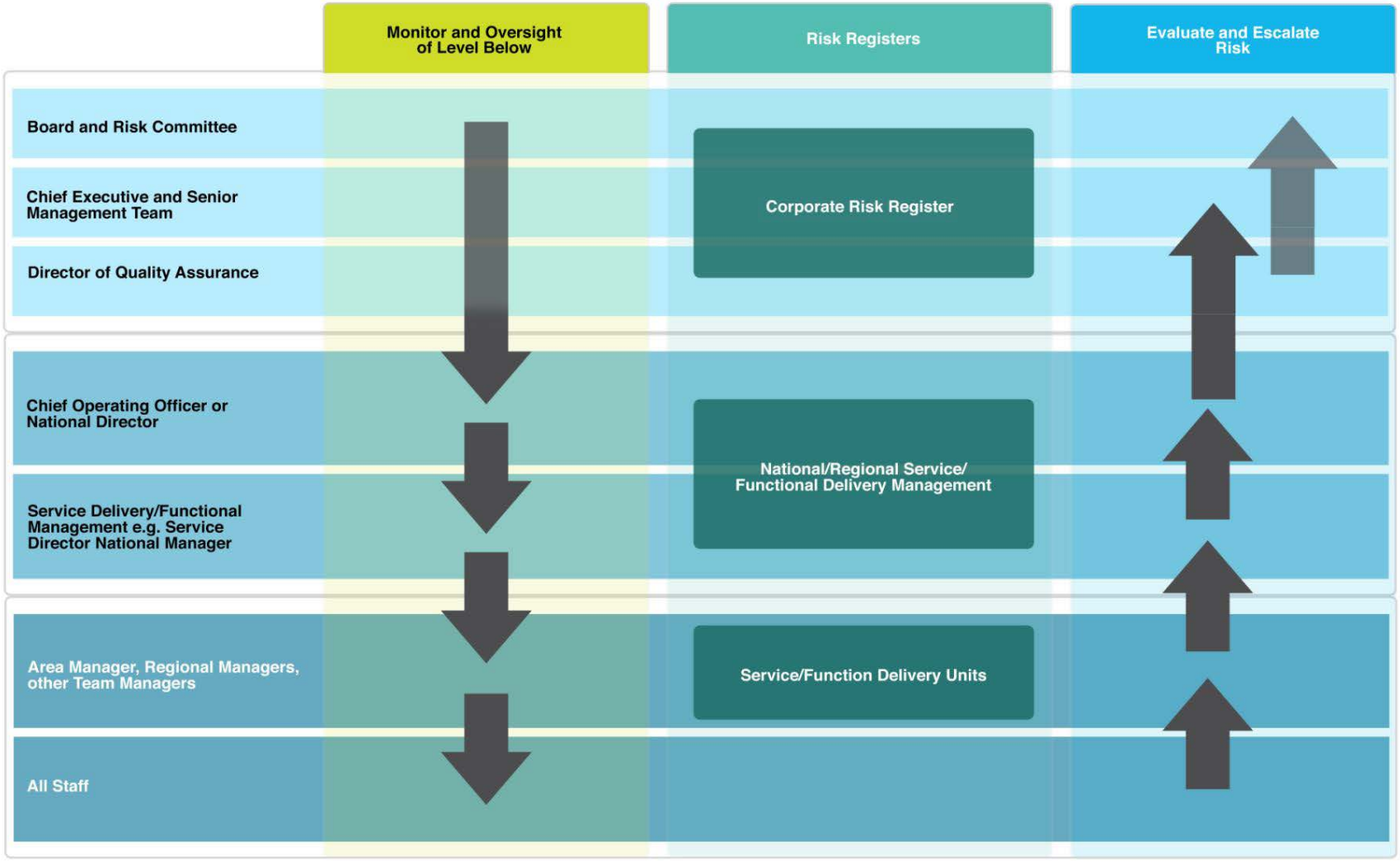
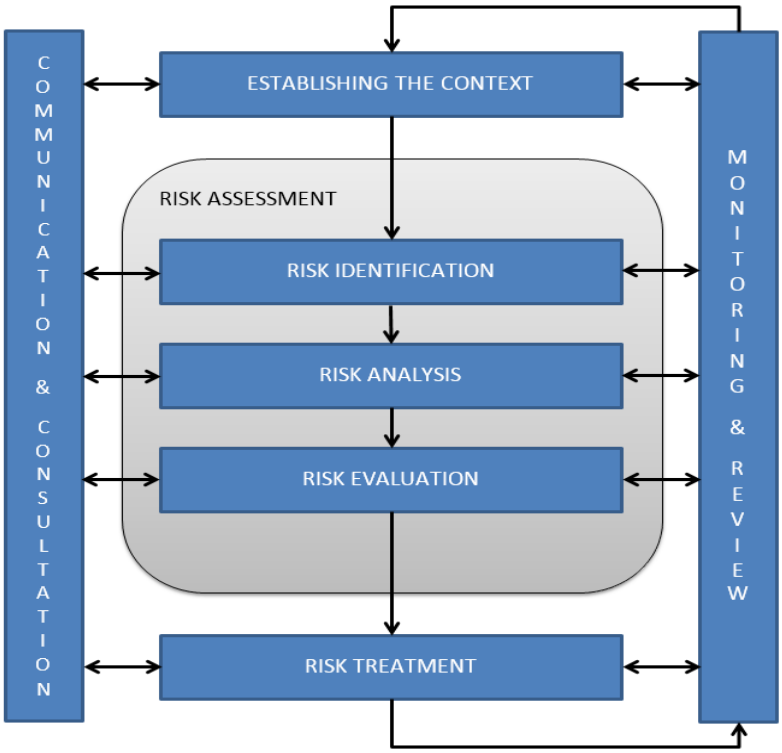


Figure 1: An Overview of Risk Accountability and Responsibility within Tusla.

6.1 RISK MANAGEMENT PROCESS

The risk management process adopted by Tusla is based on the Australia/New Zealand Standard for Risk Management (AS/NZS ISO 31000:2009)[1] and presented graphically in Figure 2. It enables a consistent and comprehensive approach to risk management across Tusla.

Figure 2: Risk Management Process (AS/NZS ISO 31000:2009)



It comprises five key steps which are taken sequentially:
Step 1: Establishing the context
Step 2: Risk Identification
Step 3: Risk Analysis
Step 4: Risk Evaluation
Step 5: Risk Treatment

} Risk Register

Two elements 'Communication and Consultation' and 'Monitoring and Review' occur continually throughout the process. The entire process is on-going, enabling it to be repeated many times leading to on-going service improvement.

All services / functions will use this standardised approach and record the outcome in a series of risk registers. These risk registers will be collated at key organisational levels allowing for risks to be managed at the most appropriate level in the organisation, i.e. risks that fall outside the control of a line manager may be escalated to the appropriate level of management.

This process should be applied to decision making at all levels for any activity or function of Tusla. It should be particularly applied when planning and making decisions about significant issues, e.g. changes in policy, introducing new strategies and procedures, managing projects, expending large amounts of money or managing potentially sensitive issues.

The next section of this document provides guidance on each of the steps involved.

[1] AS/NZS ISO 31000:2009

❖ STEP 1: ESTABLISH THE CONTEXT

The first step in the risk management process is to establish the context. As part of the planning process, it is an important and essential step, and sets the framework within which the risk assessment is undertaken. It involves:

- Establishing key information related to the subject (e.g., activity, strategic or operational plan, administrative process, project or other management initiative etc.) to which the risk assessment process is being applied
- Establishing the scope of the risk assessment activity being undertaken
- Developing a structure for the risk identification activities.

To establish the context consider and define the following elements. The depth of information required relates to the size and complexity of the risk assessment activity being undertaken.

- **Subject of the risk assessment activity** i.e., plan, process, project etc.
- **Goals and objectives of the subject being assessed**
- **Goals and objectives of the risk assessment activity** i.e., the reason for the risk assessment e.g., an operational change, new policy, project etc.
- **External parameters within which the risk should be managed** e.g., legal regulatory, political, cultural, economic and social aspects.
- **Internal parameters within which the risk should be managed** e.g., goals and objectives of the organisation; structure, function and key processes; prevailing culture; the capabilities, strengths and weaknesses of the organisation in terms of resources, people, systems and processes.
- **Relevant stakeholders (internal and external)** including their objectives and expectations. They can be both bearers of risk and sources of risk.
- **Who will be involved in the risk assessment process** – there should be a cross section of staff relating to the organisational setting where the assessment is being undertaken as well as any staff with particular expertise in conducting risk assessments.
- **Risk assessment approach to be used** (the approach to be used should be documented in the following sections).

❖ STEP 2: RISK IDENTIFICATION

Risk identification involves identifying sources of risk, areas of impact, events and their causes and consequences.

GUIDANCE NOTE

Identifying risks involves considering what, when, why, where and how things can happen:

- **What are the sources of risk or threat** – i.e., the things that have the inherent potential to harm or facilitate harm
- **What could happen** - events or incidents that could occur whereby the source of risk or threat has an impact on the achievement of objectives
- **How could it happen** - the manner or method in which the risk event or incident could occur
- **Where could it happen** - the physical location/assets where the event could occur or where direct or indirect consequences may be experienced
- **When could it happen** - specific times or time periods when the event is likely to occur and/or the consequences realised
- **Why could it happen/causes** - what are the direct and indirect factors that create the source of risk or threat
- **What might be the impact were it to happen/consequences** - what would be the impact on objectives if the risk was realised. What parts of the organisation and what stakeholders might be involved or impacted?

There is no easy scientific method to guarantee that all risks will be identified. Some approaches to and sources of information for identifying risks include the following:

Sources of Information	
Risk registers	Incident reports
Activity information (e.g., referrals, waiting lists)	Analysis of client feedback – complaints, client satisfaction, surveys, compliments
Audit reports	Claims data
Media reports	Minutes of team meetings
Parliamentary questions	National reviews of major incidents
Internal/external inspection reports	Research/literature reviews

Approaches to Identifying Risks	
SWOT analysis (Strength, Weakness, Opportunity, Threats)	PESTLE analysis (Political, Economic, Sociological, Technological, Legal, Environment)
Brainstorming	Surveys Questionnaires
One-to-one interviews	Stakeholder analysis
Working groups	Process analysis
Look at other jurisdictions (if it can happen to them, it can happen to us).	

The aim is to generate a comprehensive list of threats and opportunities that may impact (enhance, prevent, degrade, accelerate or delay) the achievement of the objectives identified in the context.

The objective of risk description is to display the identified risks in a structured format. A good risk statement must be clear, comprehensible and unambiguous. The risk description should encompass:

- The uncertain event – what could occur, area of uncertainty
- Its cause – trigger, source, factor contributing to risk occurring or increasing the likelihood of it occurring
- Its effect – consequence, impact, effect on objectives.

The three elements of a risk statement can be stated in any order, depending on how the information is used. However, it is recommended that the risk (uncertain event) be placed at the beginning to enable the reader to understand the major risk detail.

"There is a risk that *[uncertain event]* due to *[cause]* which may lead to *[effect]"*

In stating risks, avoid:

- Stating impacts which may arise as being the risks themselves
- Including risks that do not impact on objectives
- Including risks that are simply the converse of the objectives.

Risk Category: risks identified during this initial phase of the process should be allocated a risk category. Risk categories are based on the 'cause' of the risk. Grouping risks this way helps understand where the largest risk exposure originates from.

The following categories have been identified for use. Risks should be allocated to one category only:-

- Reputational and Profile
- Financial Loss
- Injury to Service User/Staff/Public/Volunteer
- Service User Experience
- Compliance with Standards/Regulations/Legislation
- Operational
- Projects and Objectives

Risk Owner: once risks are identified, they should be assigned a risk owner who has the responsibility for ensuring that the risk is being managed and monitored on an on-going basis.

All identified risks should be documented on a Risk Assessment/Risk Register Form (Appendix II). The documentation at this point should include a brief description of the risk, potential impact of the risk, the risk owner and the category of the risk.

Completed Risk Assessment/Risk Register Form forms should be held locally. Individual risks will form the basis of a risk register (for guidance on developing a risk register refer to page 19) and the Risk Register Catalogue (See Appendix III).

❖ STEP 3: RISK ANALYSIS

Through risk analysis, causes and effects of risks are identified, along with the likelihood of their occurrence. It also provides input into determining whether treatments are required. Risks are rated in terms of the likelihood and the consequences of the risk occurring.

Stages involved include:

1. Assessing the adequacy of existing controls: In subjecting a risk to analysis it is essential that account is taken of the existing control measures in place to mitigate the impact of the risk. Controls are any pre-existing process, policy, device, practice or other action that acts to minimise negative risk or enhance positive outcomes. They can be strong or weak. Each control needs to be evaluated to ensure that it is effective, reliable and being applied. When controls are working effectively and as intended, they will reduce the risk level.

All existing control measures in place to mitigate the impact of the risk should be documented on the Risk Assessment/Risk Register Form (Appendix II).

GUIDANCE NOTE

To assess the adequacy and effectiveness of existing controls in place to mitigate the impact of risk, consider the following factors:

- **Is the control 'fit for purpose'?**
- **Is the control relevant?**
- **Does it work as intended?**
- **Is the control documented?**
- **Is the control being used?**
- **Is the control up to date?**

Refer to Appendix III for further information on control measures

2. Determining the likelihood (frequency or probability) of the risk occurring taking into account the adequacy of existing controls using the Risk Likelihood Table below.

The likelihood is scored in terms of a number from 1-5 with 1 indicating that there is a remote possibility of it occurring and 5 indicating that it is almost certain to occur. Likelihood scoring is based on the expertise, knowledge and experience of the group scoring the likelihood. In assessing likelihood, it is important to consider the nature of the risk. Risks are assessed on the probability of future occurrence; how likely is the risk to occur? How frequently has this occurred? Generally the higher the degree of controls in place, the lower the likelihood.

Table 1: Risk Likelihood

	Rare / Remote	Unlikely	Possible	Likely	Almost Certain
Likelihood Score	1	2	3	4	5
Actual Frequency	Every 5 years or more	Every 2 – 5 years	Every 1 – 2 years	Bi-annually	At least monthly
Probability	1%	10%	50%	75%	99%

3. Determining the consequence (impact or magnitude of the effect) of the risk should it occur, taking into account the adequacy of the existing controls, using the Risk Assessment Impact Table presented in Appendix IV.

To determine the impact of this harm should it occur each type of harm has been assigned descriptors over 5 levels ranging from negligible to extreme harm. In scoring impact, the anticipated outcome of the risk is graded from 1-5 with 5 indicating a more serious impact (for further guidance on how to use the Impact Table refer to Appendix V).

4. Assigning a risk level (rating) taking into account the adequacy of the existing controls using the 5 x 5 Risk Matrix below. This is done by plotting the likelihood and consequence scores determined above and translating this information into a risk level (rating). For example a risk with a likelihood score of 3 (possible) and an impact score of 3 (moderate) will have a risk rating of 9 (medium).

Table 2: Risk Matrix (5 x 5)

	Impact Score				
Likelihood Score	**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

- **High risk is scored between 15 and 25 and coloured RED**
- **Medium risk is scored between 6 and 12 and coloured AMBER**
- **Low risk is scored between 1 and 5 and coloured GREEN**

The risk rating determined provides an estimate of where the most serious risks lie. In analysing risk it is important to consider not only the issue of minimising risk but also maximising opportunity.

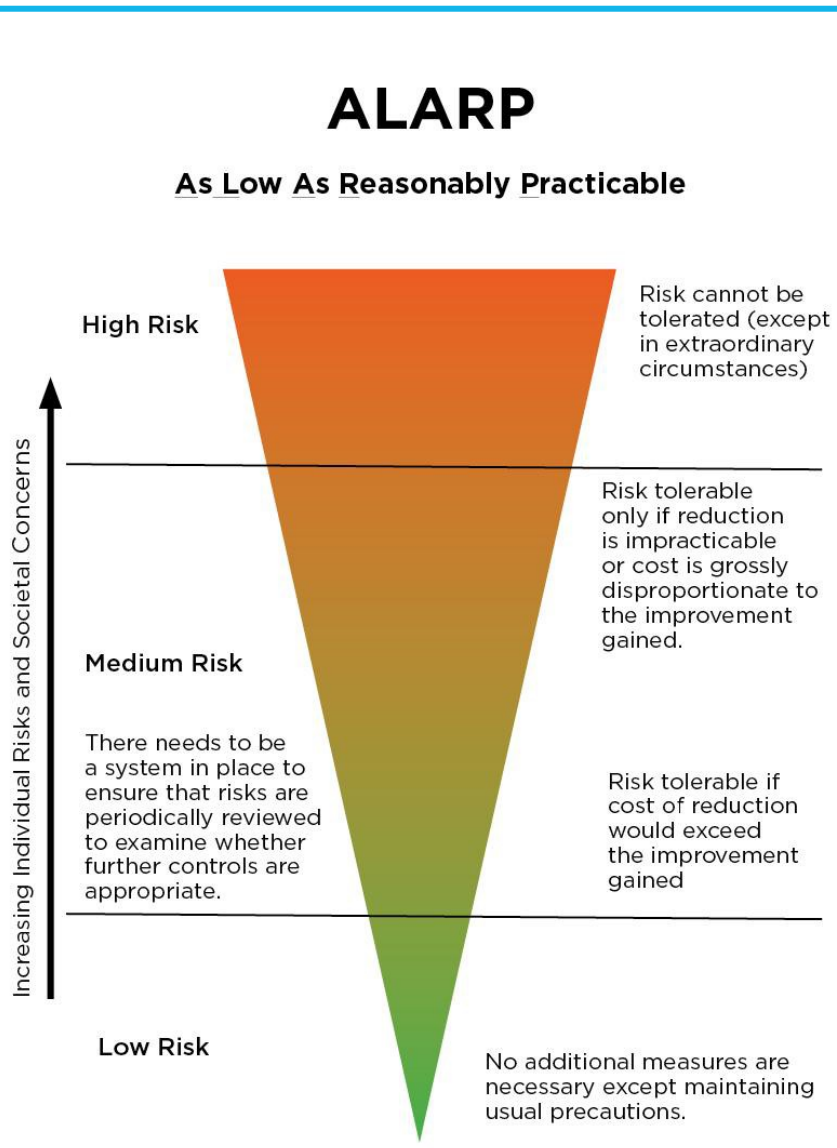
The resultant analysis should be recorded on the Risk Assessment/Risk Register Form (Appendix II) i.e., existing control measures, likelihood, impact and initial risk rating.

❖ STEP 4: RISK EVALUATION

Risk evaluation is about deciding whether risks are acceptable or unacceptable. Based on the initial risk rating and the adequacy of the existing controls in place an evaluation must be made on whether to accept the risk or that additional controls or other actions are required to mitigate the risk e.g., risk treatment. This enables risks to be ranked so as to identify management priorities.

Whether a risk is acceptable or unacceptable relates to the willingness to tolerate the risk; that is, the willingness to bear the risk after it is treated in order to achieve objectives. The evaluation should take account of the degree of control over each risk and the cost impact, benefits and opportunities presented by the risks. The significance of the risk and the importance of the policy, program, process or activity, need to be considered in deciding if a risk is acceptable.

It is accepted that risk will never be eradicated from services, however it is important that managers seek to minimise risk to the lowest reasonably practicable level (ALARP Principle).



ALARP stands for "as low as reasonably practicable".

The width of the cone indicates the size of the risk. In general, two criteria can be defined. A level where risk is negligible and can be accepted without specific treatment other than monitoring (these risks are often rated as green) and the level which is intolerable and the activity must cease unless the risk can be reduced (these risks are often rated red). Between these levels is the region where costs and benefits are taken into account. When risk is close to the intolerable the expectation is that the risk will be reduced unless the cost of reducing the risk is grossly disproportionate to the benefits gained. Where risks are close to the negligible level then action may only be taken to reduce risk where benefits exceed the costs of reduction.

A risk is called acceptable if it is not going to be treated, accepting risk does not imply that the risk is insignificant. A risk may be accepted for a number of reasons as follows:

- The level of the risk is so low that specific treatment is not appropriate within available resources;
- The risk is such that no treatment option is available within the control of the organisation. For example the risk that a project might be terminated following a change of government is not within the control of the Agency;
- Treatment costs are prohibitive (particularly relevant with lower rated risks);
- The opportunities presented outweigh the threats to such a degree that the risk is justified.

Once a decision has been made to accept the risk a process needs to be put in place to monitor and review the risk. The review date and risk status 'Monitoring' need to be documented on the Risk Assessment/Risk Register Form (Appendix II).

For risks that are deemed unacceptable, treatment options (additional controls) need to be considered (see Step 5 below).

❖ STEP 5: RISK TREATMENT

This stage of the process is about dealing with risks determined as being unacceptable at the initial risk level (rating).

Risk treatment involves identifying the range of options for controlling or treating the risk, assessing those options, preparing risk treatment plans (action plans) and implementing them.

The options available for the treatment of risks are:

- **Avoid the risk** – this is achieved by either deciding not to proceed with the activity, choosing an alternate more acceptable activity which meets the goals and objectives of the organisation, or choosing an alternative less risky methodology or process
- **Transfer the risk** – this is achieved by transferring the risk to an outside party (e.g., insurer, out-sourcing, contractor etc.)
- **Control the risk / risk reduction** - this is the most commonly used treatment option. It is focussed on reducing the likelihood of the risk occurring or the impact of the risk if it occurs, or both. There may be a trade-off between the level of risk and the cost of reducing those risks to an acceptable level. The most effective methods for risk control are those which redesign the system and processes so that the potential for the adverse outcome is reduced. In choosing additional internal controls the hierarchy of controls should be considered (refer to Appendix IV).

The treatments chosen should target the impacts/vulnerabilities and are only considered controls when they are effectively implemented.

After the additional controls required have been agreed, a named person should be identified and assigned responsibility for ensuring that these additional controls are implemented via a treatment/action plan. For those additional controls that can be managed within the service the name of the person who has been assigned responsibility for ensuring that these additional controls are implemented and the timeframe for implementation should be captured on the Risk

Assessment/Risk Register Form (Appendix II). The risk status should also be recorded as 'open' on this form.

The person assigned responsibility for ensuring that the additional controls are implemented will be required to develop an action plan (treatment plan) and provide an update to the Area Manager/Service Manager/National Manager on the status of implementation of these additional controls on a regular basis, no greater than 3 monthly.

GUIDANCE NOTE

Action plans/treatment plans should include:

- The specific cost-effective actions to be taken
- Resource requirements
- The person responsible for the action
- The timeframe for action.

In order to ensure that action plans are implemented they should be subjected to on-going monitoring and review as part of the normal business process of the service/area in which the risks are treated.

For additional controls that are not within the span of control of the service to implement the action should be escalated to the person responsible at the next level of management (for guidance on risk escalation refers to page 19).

At the end of this step in the process a Risk Assessment/Risk Register Form (Appendix II) for each risk identified will have been completed. These will form the basis for the development of a Risk Register (refer to page 19 for guidance on developing a risk register).

GUIDANCE NOTE

At this stage of the process:
Each of the risks identified should be assigned a risk status and it should be recorded on the Risk Assessment Form (Appendix II). The options are:

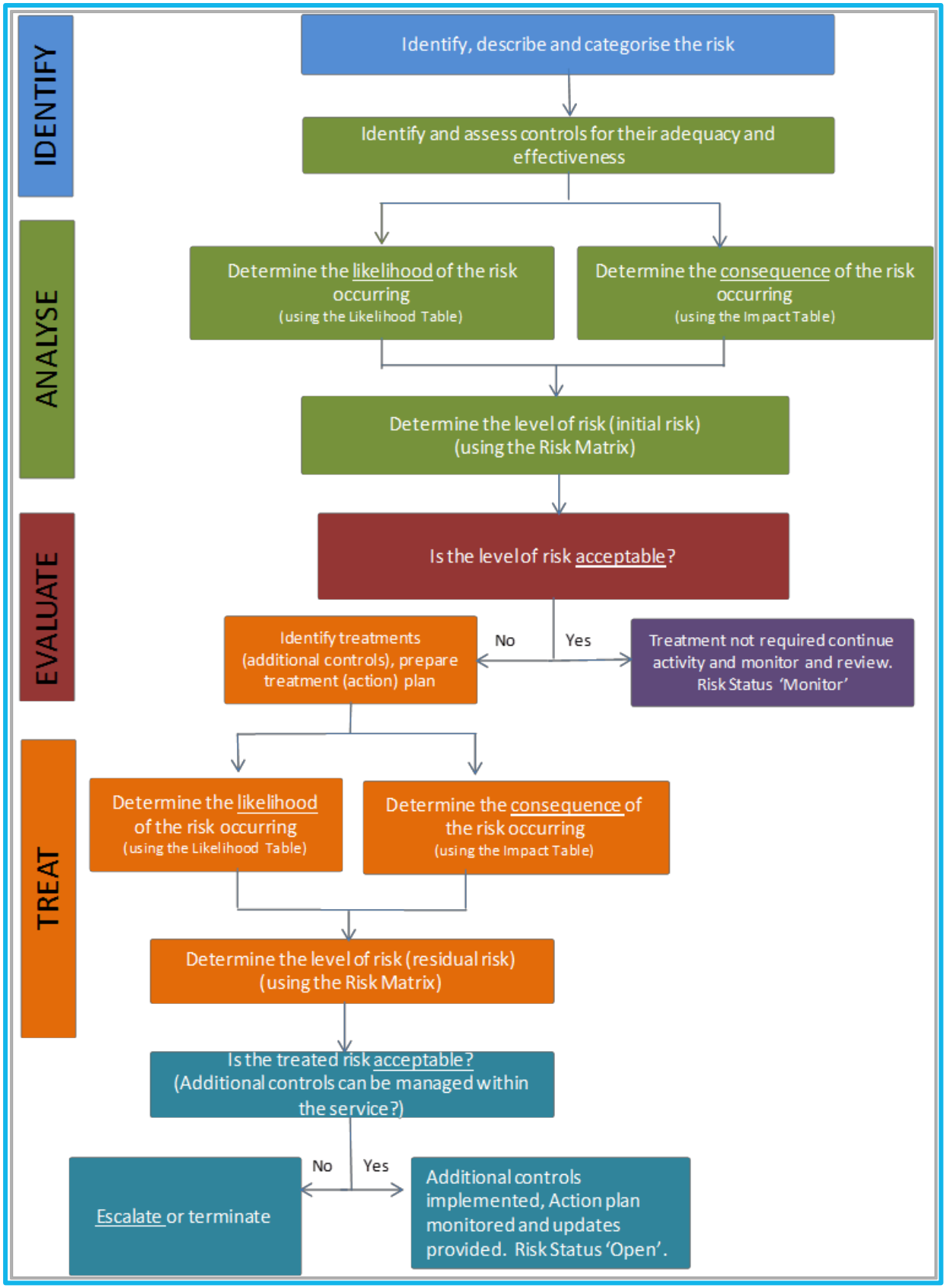
- **'Monitor'** i.e., existing controls are deemed adequate to manage the risk but these need to be periodically reviewed
- **'Open'** i.e., additional controls have been identified as necessary
- **'Closed'** i.e., that the risk no longer exists e.g., where an unsuitable premises is replaced by a suitable one.

Three categories of assessed risk will have been identified:

1. Those **risks that require monitoring and review** within the service they were identified i.e., risks where no further additional control(s) have been identified as necessary.
2. Those **risks where the additional control(s) can be managed at local level** and the responsibility for managing those additional control(s) has been assigned to person(s) within the service.
3. Those **risks where the additional control(s) cannot be managed at local level** and these have been identified as requiring escalation up to the person responsible at the next level of management. **It is these risks that form the basis of the development of the risk register for the Area Manager/National Manager/Service Manager.**

A summary of the actions and decisions within the risk identification, analysis, and evaluation and treatment steps is presented in Figure 3.

Figure 3: Actions and decisions within the risk identification, analysis, and evaluation and treatment steps.



DEVELOPING A RISK REGISTER

Risk Registers are primarily an internal management tool to support service delivery areas and the Agency's directorates in the management of their risks whilst there is an opportunity to raise/escalate particular risks for inclusion on to the Agency's Corporate Risk Register. 'Risk Registers' are a means of logging, tracking and prioritising risks and resources. All risks, of all types, should be managed using this process.

Completed Risk Assessment/Risk Register Forms (Appendix II) populate the Risk Register; Risk Assessment/Risk Register Forms are completed and submitted to the line manager. Each risk should be recorded separately on one form and risks should be grouped on an Area/Regional/Service Risk Register Catalogue (Appendix III). All sections of the form should be completed in order for the line manager to make a full evaluation and subsequent determination regarding whether to accept the risk or those additional controls or other actions are required to mitigate the risk. For those risks that are accepted, a process needs to be established to monitor and review the risk; the review date and status of monitoring will be documented on the Risk Assessment/Risk Register Form.

The assessed risks can be categorised as follows:

1. Those risks that require monitoring and review within the service they were identified i.e. Risks where no further additional control(s) have been identified as necessary.
2. Those risks where the additional controls(s) can be managed at local level and the responsibility for managing those additional control(s) has been assigned to person(s) within the service.
3. Those risks where the additional control(s) cannot be managed at local level and these have been identified as requiring escalation up to the Regional Service Manager.

Figure 4 provides an overview of the Risk Register Development Process.

DIRECTORATE RISK REGISTERS

Each National Director will have oversight of their directorate risk register to enable them understand the nature and extent of the risks facing their directorate, how they are being managed and who is responsible. The results of this process enables risks to be categorised, responses standardised and merged for relevance to the appropriate level of management. Directorate risk registers will inform the Corporate Risk Register.

CORPORATE RISK REGISTER

The Tusla Corporate Risk Register is developed by the Quality Assurance Directorate and is presented to the Senior Management Team on a monthly basis and to the Board every quarter. The structure of the Corporate Risk Register differs from the template and process outlined in this policy and procedure.

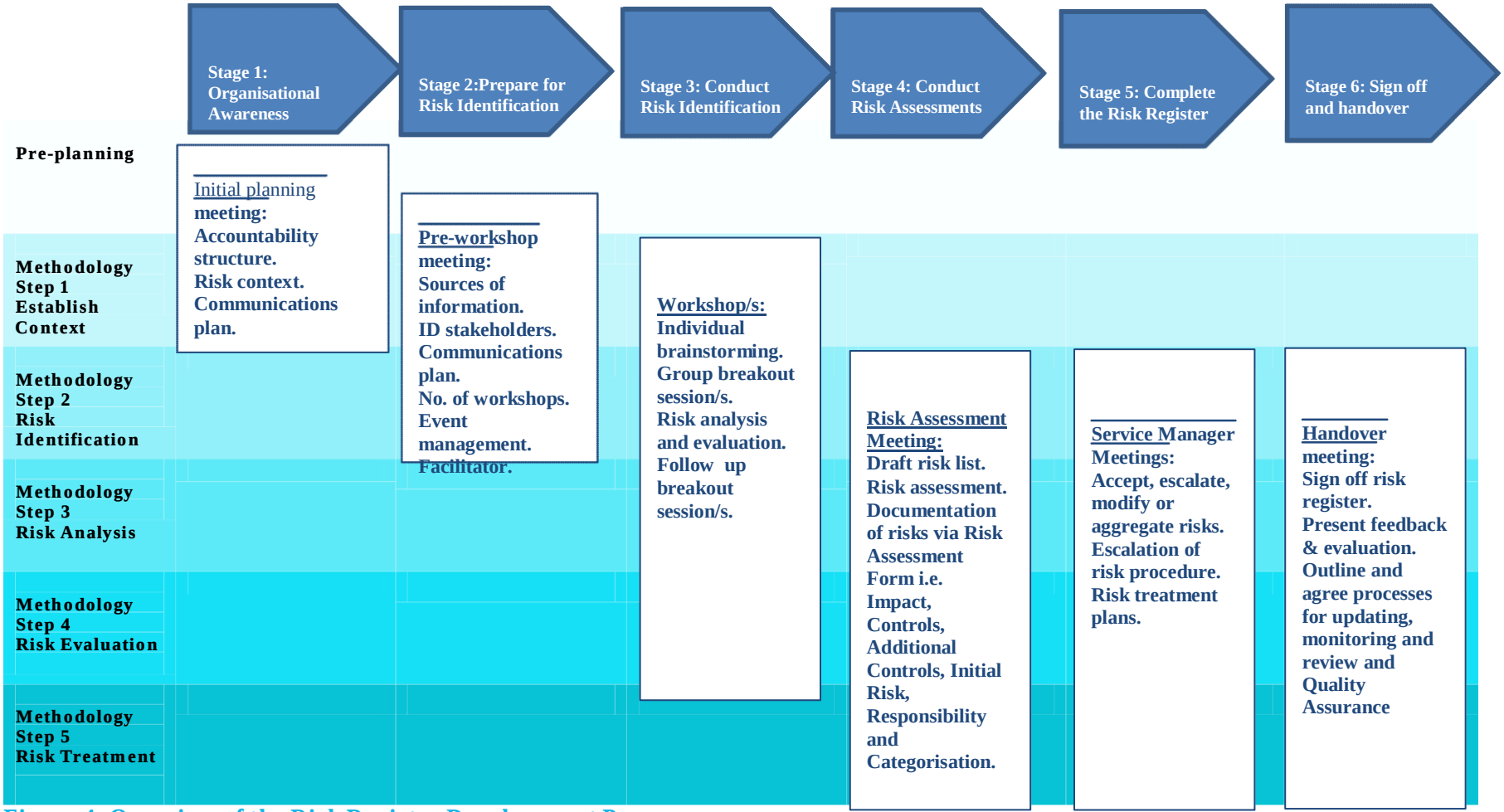


Figure 4: Overview of the Risk Register Development Process

PROCESS FOR RISK ESCALATION

When a risk cannot be managed within the Area/Service or requires additional controls that are outside the scope of the Area/Service to implement, the risk should be escalated to the person responsible at the next appropriate level of management by the risk owner. Managers should be informed of risks escalated to their remit in writing using the Risk Assessment/Risk Register Form in Appendix II. The manager who receives the notification then has three options, namely:

- Accept the risk on to their risk register.
- De-escalate the risk back down for on-going monitoring or management at local level
- Escalate up to the next level of management.

If the risk is accepted this manager becomes the risk owner. He/she must communicate the decision to accept the risk along with any updated actions to mitigate the risk to the manager who escalated the risk. Once the risk is escalated and accepted at the higher level, that manager is responsible for addressing the risk. The local manager is still responsible for managing the risk.

Escalated risks remain "Open and Escalated" at the originating level and should be reviewed on a monthly basis. It is acknowledged that every risk cannot be reduced or eliminated, however neither can they all be escalated. They must be recorded in the risk register along with a list of controls to manage the risks. This process is replicated for all levels of escalation.

MONITOR AND REVIEW

On-going monitoring and review are essential components of the overall risk management process as factors that affect likelihood and consequence of risk may change. A review date and risk status of monitoring must be documented on the risk assessment form. The risk register is a live document and the status of risks is subject to continual change. In addition, new risks will inevitably emerge from time to time. Newly identified risks should be included on the risk register following assessment and the identification of actions required in the same way as those that were identified through the initial risk register development process.

Risk re-assessments should take place on a 3 monthly basis, at a minimum, to take account of any new controls that have been put in place since the original assessment. This will allow for a re-prioritisation of the risk list.

When re-assessing existing risks, services should compare the risk rating from the re-assessment with the risk rating of the original assessment. If the reduction (or maintenance in certain circumstances) of risk levels is not as anticipated in the original assessment, then they need to check why, i.e. have the additional controls been effectively implemented? If they have why are they not reducing the rating? Are they the right controls and if not is there a need to revisit and enhance the control measures?

COMMUNICATE AND CONSULT

The risk management process should involve those who carry out or might be affected by the activities under consideration. It is the responsibility of the risk owners to ensure that risks and the control measures identified are communicated to those who may be affected by the activities. Within the service, good communication is paramount in developing a 'culture' where positive and negative dimensions of risk are valued. Engaging with others serves to embed risk management as a normal part of the way services operate.

Communication efforts must be focused on consultation, rather than one way flow of information from decision makers to stakeholders

7.0 QUALITY ASSURANCE

Each Area/Service should audit and review its compliance with this policy and procedure. The evaluation shall aim to determine adherence to this procedure including:

- The adequacy of the Risk Register in relation to the potential risks
- The accuracy of the impact, likelihood and risk levels allocated to the risks identified
- The implementation of the required controls identified within the Risk Registers
- The monitoring, review and update activities completed on the Risk Register documents.

8.0 TRAINING AND SUPPORT

The following training and supports are available to managers with regard to the development of risk registers in accordance with this policy and procedure document:

- Bespoke advanced risk management training is available to all teams, tailored to their specific needs. This includes advice and guidance on the management of risk in their area, peer reviews and/or support with development of risk registers.
- Tools and supporting guidance is available on the Tusla Hub or by contacting the Quality Assurance Directorate at qa@tusla.ie

APPENDIX I - GLOSSARY OF TERMS AND DEFINITIONS

TERM	DEFINITION
Control:	A control is any process, policy, device, practice or other action that acts to minimise negative risk or enhance positive outcomes. A risk may have more than one control and a control may address more than one risk.
Controlled Risk:	Level of risk taking into account the adequacy and effectiveness of the controls in place.
Operational Risks:	Risks connected with the internal resources, systems, processes and employees of the organisation. They relate to the short to medium term objectives of the organisation.
Likelihood:	Chance or probability of the risk occurring. It can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively.
Risk:	Risk is defined as the effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected. It measured in terms of consequence (impact) of the event and the associated likelihood (probability) of occurrence.
Risk Assessment:	The overall process of risk identification, risk analysis and risk evaluation.
Risk Criteria:	Terms of reference against which the significance of risk is evaluated.
Risk Escalation:	Communication of risks that fall outside the control of a line manager to the appropriate level of management.
Risk Level:	Expression of the effect of a risk, in terms of likelihood of occurring and the consequences if it were to occur. Risk levels are assessed at the controlled and residual (after treatments have been applied) positions.
Risk Management:	Coordinated set of activities to direct and control an organisation with regard to risk.
Risk Management Process:	Systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Owner:	Person(s) or entity that has been give authority to manage a particular risk and is accountable for doing so.
Risk Register:	A database of risks that face an organisation at any one time. It provides managers with a high level overview of the services' risk status at a particular point in time and becomes a dynamic tool for the monitoring of actions to be taken to mitigate risk.
Risk Tolerance:	Readiness to bear risk, after treatment, in order to achieve outcomes.
Risk Treatments:	Additional strategies/activities required to be developed and implemented should the risk level be unacceptable after controls are applied. Generally treatments are specific to a risk. A treatment only becomes a control after it has been fully implemented and deemed effective in modifying the risk to an acceptable level.
Strategic Risks:	Risks connected with the long-term strategic objectives of the Agency. They may be external or internal to the organisation.

APPENDIX II

TUSLA RISK ASSESSMENT/RISK REGISTER FORM

One Risk only per form

Admin Area/Function:		**Date of Assessment:**	
Location:		**Risk Category:**	
Service Type & Name		**Name Risk Owner: (BLOCKS)**	
Service Contact Details		**Signature of Risk Owner:**	
Unique Risk ID No:			

RISK DESCRIPTION	POTENTIAL IMPACT OF THE RISK	EXISTING CONTROL MEASURES	ADDITIONAL CONTROLS REQUIRED	PERSON RESPONSIBLE FOR ACTION	DUE DATE

RISK RATING			STATUS	REVIEW DATE
Likelihood	**Impact**	**Initial Risk Rating**	**Monitor/Open/Closed**	

This form is available separately on the Tusla Hub

APPENDIX III

An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

Risk Register Catalogue

Service Area:	Service Lead:	Risk Register last updated:

Risk No.	Date entered on register	Risk Description	STATUS Open Closed Monitor	Risk Rating	Change since last report*	Action Plan reviewed / updated Yes / No	Issues of note

This form is also available separately on the Tusla Hub

APPENDIX IV - Control Measures

What is a Control Measure?
A control measure is any process, policy, device, practice or other action that acts to minimise negative risk or enhance positive opportunities. It is essential consequently, when seeking to minimise the risk posed by any hazard to have in place sufficient controls.

Classification of Internal Controls
There are two main ways of classifying the nature of internal controls available.

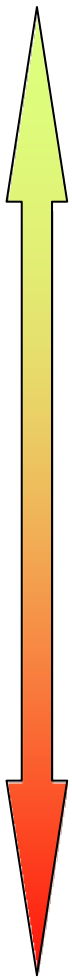
1. By function i.e. what are they attempting to do.
2. By robustness i.e. their level of effectiveness in preventing risks occurring.

Classification by Function

- **Preventative:** These focus on preventing errors or exceptions, examples include:
  - Standards, policies and procedures are the most basic type of preventive control
  - Segregation of duties also acts as a preventive control against fraud
  - Authorisation/Approval levels also prevent the risk of an illegal act and are thus preventive in nature.
- **Detective:** These are designed to detect errors or irregularities that may have occurred, examples include:
  - Reviews
  - Reconciliation
  - Variance Analysis
  - Audit.
- **Directive: These are designed to tell employees what to do, examples include:**
  - Written Policies
  - Reporting lines
  - Supervision
  - Training.
- **Corrective:** These are designed to correct errors or irregularities that have been detected, examples include:
  - Continuity Plans e.g. major incident plans, business continuity plans
  - Insurance
  - Contract terms.

Classification by Robustness
Some controls are better at minimising risk than others and to assist managers in identifying the most robust controls reference should be made to the hierarchy of control measures. The higher on the hierarchy the control is, the greater the potential is that it will minimise the risk. Consideration should be given as to what level on the hierarchy of control the controls are selected from.

The hierarchy of control measures is as follows:

Strength of control	Category of control	Comments/Examples
Strongest control 	**Elimination**	The job is redesigned so as to remove the hazard/contributory factor. However, the alternative method should not lead to a less acceptable or less effective process e.g. stop providing service; discontinue a particular procedure; discontinue use of a particular product or service, e.g. stop using a particular type of equipment. If hazard elimination is not successful or practical, the next control measure is Substitution.
	Substitution	Replacing the material or process with a less harmful one. Re-engineer a process to reduce potential for 'human error'. If no suitable practical replacement is available the next control measure is engineering controls.
	Engineering controls	Installing or using additional equipment. Introduce 'hard' engineering controls, e.g. installation of handling devices for moving and handling people and objects, e.g. Re-engineer equipment so that it is impossible to make errors. If no suitable engineering control is available the next control measure is administrative procedures.
	Administrative procedures.	Introduce new administrative policies, procedures and guidelines e.g. job rotation. If no administrative procedure is available the next control measure is work practice controls.
Weakest control	**Work Practice Controls**	This is the last control measure to be considered. Change the behaviour of staff, e.g. make staff wear personal protective equipment, etc. Work Practice Controls should only be considered after all the previous measures have been considered and found to be impractical or unsuccessful.

APPENDIX V - RISK ASSESSMENT IMPACT TABLE

Impact	Negligible	Minor	Moderate	Major	Extreme
Impact Score	1	2	3	4	5
Reputation and Profile	Rumours, no media coverage or public concern voiced. Little effect on staff morale. No review or investigation required.	Local, short term, media coverage. Some public concern. Minor effect on staff morale / public attitudes. Internal review required	Adverse local media coverage. Significant effect on staff morale and public perception. Public calls for remedial actions. Comprehensive review or investigation necessary.	Adverse national media coverage <3days Long term local adverse media coverage Public confidence undermined Use of resources questioned Possible Dáil questions Public calls for remedial action Possible Tusla review or investigation.	Adverse national or international media coverage >3days Public confidence undermined Use of resources questioned CEO performance questioned Taoiseach or Minister forced to comment or intervene Dáil questions. Public calls for remedial action. Court Action. Public independent inquiry.
Financial	<€1k	€1k > €10k	€10k > €100k	€100k > €1m	>€1m
Injury	Minor injury not requiring first aid. No psychosocial impairment.	Minor injury requiring first aid. < 3 days absence or extended hospital stay Impaired psychosocial functioning >3days and < 1 month.	Significant injury requiring medical treatment. Agency reportable – violent and aggressive acts > 3 days absence, 3-8 days hospitalisation Impaired psychosocial functioning > 1 month and < 6 months.	Major injury/long term incapacity or disability. Impaired psychosocial functioning > 6months.	Death or permanent incapacity. Impacting large number of children or member of the public. Permanent psychosocial functioning incapacity.
Service User Experience	Reduced quality related to inadequate provision of information.	Unsatisfactory experience related to less than optimal care/service provision, inadequate information, not treated like an equal or not treated with honesty, dignity and respect.	Unsatisfactory experience related to less than optimal care/service provision with short term effects < 1 week.	Unsatisfactory experience related to poor care/service provision resulting in long term effects.	Totally unsatisfactory service experience or extremely poor care/service provision and outcome resulting in long term effects.
Compliance	Minor non-compliance with internal standards. Small number of minor issues requiring improvement.	Single failure to meet internal standards or follow protocol. Minor recommendations easily addressed by local management.	Repeated failure to meet internal standards or follow protocols. Important recommendations which can be addressed with appropriate management action plan.	Repeated failure to meet external standards, national standards and regulations. Critical report or large number of significant findings	Gross failure to meet external standards. Repeated failure to meet national standards and regulations. Severely critical report with possible major reputational or financial implications.
Projects and Objectives	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope, quality, objectives or schedule.	Significant project over run.	Inability to meet objectives Reputation seriously damaged.
Operational	Interruption in a service not impacting on delivery, user care or ability to continue to provide the service.	Short term disruption to service with minor impact on service user.	Some disruption to service with unacceptable impact on service user. Temporary inability to provide service.	Sustained loss of service with serious impact on delivery to service user or involving major contingency plans.	Permanent loss of core service or facility. Disruption leading to significant 'knock on' effect.

This form is also available separately on the Tusla Hub

APPENDIX VI - How to Use the Impact Scoring Table

Step 1
Choose the most appropriate Risk Category(s) into which the risk identified falls. In many instances, you will be able to score the risk under a number of categories. All areas should be considered when scoring.

Step 2
Assess the impact of that risk being realised for each risk area. Working along the table, select the Impact that most closely matches each e.g. minor. In instances where several of the risk categories are appropriate, all of these risks should be scored separately and the highest impact category score is the score given to that risk e.g. if it scored moderate for injury and minor for compliance with standards, the overall impact assigned should be moderate (being the higher of the two).

Step 3
Assign an impact score. This is the number assigned to the impact chosen and appears at the top of the selected column i.e. in the case of a moderate impact the scoring is 3.