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

Organisational Risk Management Policy

January 2022

Organisational Risk Management Policy

Incorporating an overview of the Risk Management process

Document Reference Number	
Revision Number	4.0
Approval Date	
Next Revision Date	December 2025, unless deemed appropriate to review sooner
Document Developed By	Quality and Regulation (Q&R) Directorate
Document Approved By	Tusla Board
Responsibility for Implementation	All Tusla Employees
Responsibility for Review and Audit	Senior Managers and the Director of Quality and Regulation

1.0 Glossary of Terms

TERM	DEFINITION
Action	An action is an additional/future control measure that is currently being put in place. It will further reduce either the likelihood of the risk occurring or potential impact of the risk.
Business Continuity	Capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption[1]
Control	A control is measure that maintains and/or modifies risk i.e. process, policy, device, practice, or other conditions, and or actions which maintains and/or modifies risk[2].
Controlled Risk:	Level of risk, taking into account the adequacy and effectiveness of the controls in place.
Event	Event is defined as the occurrence or change of a particular set of circumstances. It can have one or more occurrences and can have several causes and several consequences. An event can also be something that is expected which does not happen, or something that is not expected which does happen or it can be a risk source[3].
Harm:	There are 3 types of harm 1. Harm to a person: Any physical or psychological injury or damage to the health, wellbeing or development of a person, including both temporary and permanent injury 2. Harm to an asset: Damage to a thing may include damage to facilities or systems; for example, environmental, financial, data protection breach, etc. 3. Harm to a child as defined by Children First Act 2015: 'assault, ill treatment or neglect of the child in a manner that seriously affects or is likely to seriously affect the child's health, development or welfare or sexual abuse of the child'
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.
Impact:	Outcome of an event affecting objectives[4]
Mitigation	A mitigation is a plan or activity completed to reduce the impact of the risk when the risk occurs.[5]
Risk:	Risk is defined as the effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected. Risk is usually expressed in terms of risk sources, potential events, their consequences (impact) and their likelihood[6]
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.

[1] Taken from Clause 3.3 'Business Continuity' International Organization for Standardization: ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

[2] Taken from Clause 3.8 'Control' International Organization for Standardization: ISO 31000:2018 Risk Management Guidelines

[3] Taken from Clause 3.5 'Event' ISO 31000:2018 Risk Management Guidelines

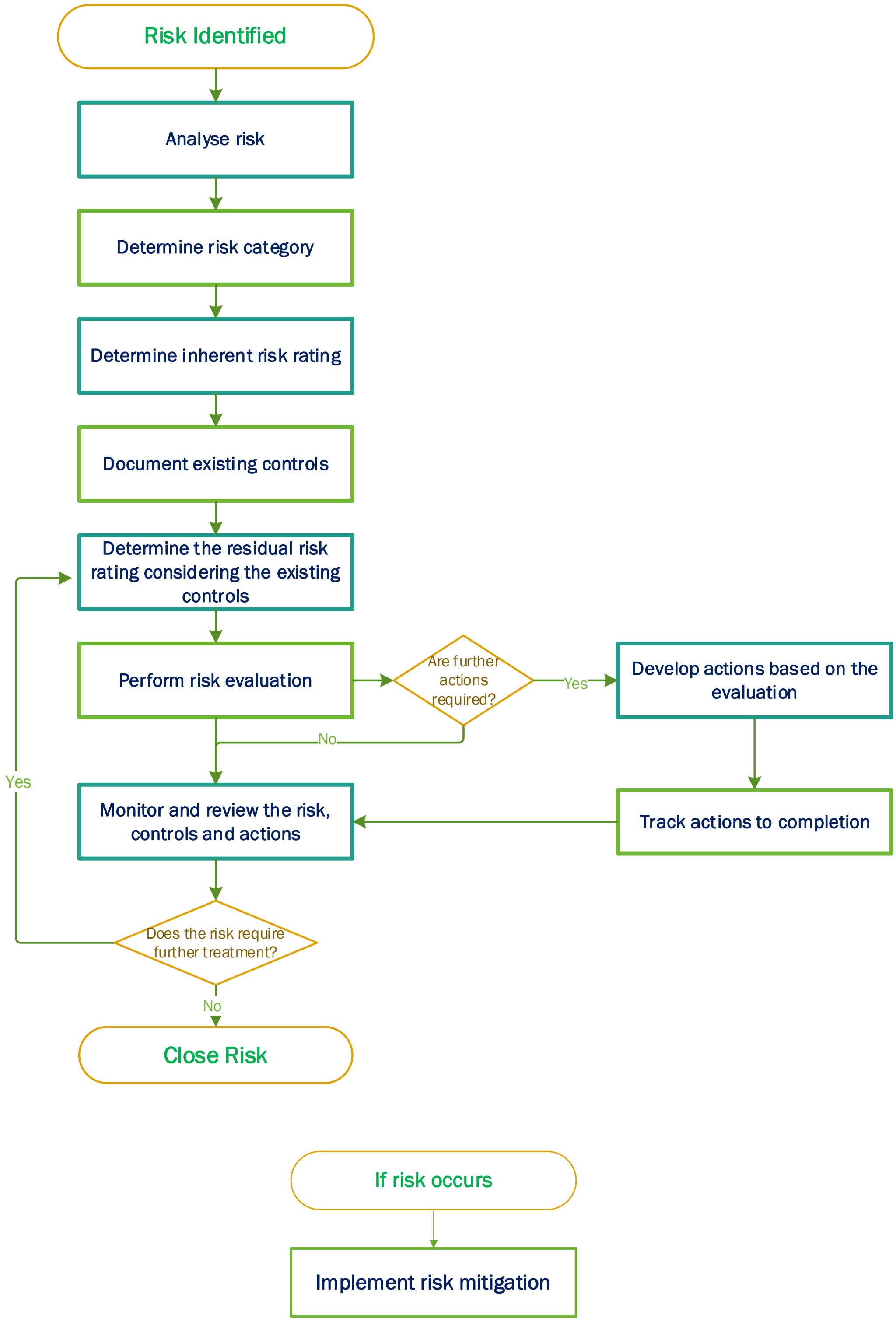
[4] Taken from Clause 3.6 'Consequence' ISO 31000:2018 Risk Management Guidelines

[5] Adapted from Risk Management Guidance for Government Departments and Offices (February 2016) Department of Public Expenditure and Reform (DPER)

[6] Taken from Clause 3.1 'Risk' ISO 31000:2018 Risk Management Guidelines

TERM	DEFINITION
Risk Notification:	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 communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Owner:	Person(s) or entity that has been given 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 a manager 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:	Where the level of risk is unacceptable after controls are applied, risk treatments are additional strategies/activities required to be developed and implemented. Generally, treatments are specific to a risk.
Strategic Risks:	Risks connected with the long-term strategic objectives of the Agency. They may be external or internal to the organisation.

2.0 Process Map


Risk Identified
Analyse risk
Determine risk category
Determine inherent risk rating
Document existing controls
Determine the residual risk rating considering the existing controls
Perform risk evaluation
Are further actions required?
Yes
Develop actions based on the evaluation
No
Track actions to completion
Monitor and review the risk, controls and actions
Yes
Does the risk require further treatment?
No
Close Risk
If risk occurs
Implement risk mitigation

3.0 Introduction

The approach by which Tusla – Child and Family Agency (herein known as Tusla) manages risk is aligned to the ISO 31000:2018 Risk Management –Guidelines[7] and replaces Tusla Organisational Risk Management Policy 2017.

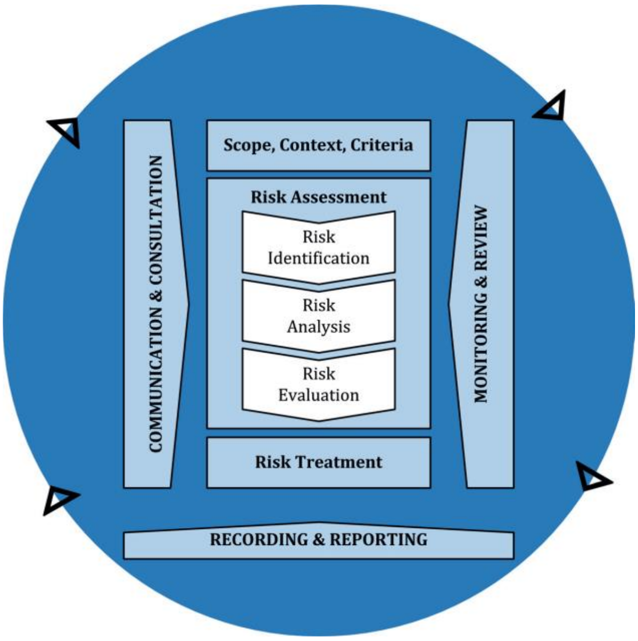


Figure 1[8] ISO Risk Management

Risk management refers to coordinated activities to direct and control an organization with regard to risk[9]. This policy aligns to the Tusla risk management framework including risk reporting and risk appetite statement.

Tusla is committed to:

- adopting a proactive approach to the management of risk to support both the achievement of objectives and compliance with governance requirements,
- ensuring that risk management is seen as the concern and responsibility of everyone and embedded both as part of normal day-to-day business,

[7] International Organization for Standardization: ISO 31000:2018 Risk Management Guidelines, provides guidelines, framework and a process for managing risk. It can be used by any organisation regardless of its size, activity or sector.

[8] Taken from Clause 6 'Process' ISO 31000:2018 Risk Management Guidelines

[9] Taken from Clause 3.2 ISO 31000:2018 Risk Management Guidelines

- ensuring risk management principles and practices form an integral part of its culture, governance and accountability arrangements, decision-making processes, strategic and operational planning and reporting, review, evaluation and improvement processes,
- establishing and providing the necessary structures, processes, training and other supports required to implement this policy,
- a high standard of governance and compliance by ensuring risk is managed in line with the Code of Practice for the Governance of State Bodies.

4.0 Scope

This policy applies to all staff and managers in all services and functions under Tusla's remit. It also applies to staff seconded to Tusla, students and volunteers and Board members. This policy is for application at national, directorate and sub-directorate levels. It is not intended for use in the assessment of risk involving the management of children and families and treatment relating to individual Service Users, where other risk assessment methods are available e.g. Need to Knows (NTKs).

5.0 Purpose

The purpose of this policy is to:

- Outline Tulsa's proactive management of risk in line with the ISO 31000:2018 Risk Management Guidelines.
- Set out the systems and processes, including staff's role in them, that are required to ensure that risks are managed consistently across Tusla.

The policy supports the purpose by:

- Defining the roles and responsibilities for risk management.
- Outlining a consistent risk management process including the communication and notification of risk
- Seeking to embed risk management as part of the normal day-to-day activities in delivering our services rather than as a separate activity.
- Outlining the process to be adopted at all agency levels which requires that risks identified are assessed, prioritised for action and are recorded in a consistent manner.
- Ensuring that all risks have clear ownership.
- Actions identified to minimise a risk are recorded and have a due date for completion.

- Ensuring that, where actions to manage a particular risk are not within the control of the local Manager, these actions can be notified to the next line of management for review and decision making.
- Reporting risks against objectives; this demonstrates the value of resourcing being consistent with policies and statements, see Figure 2 below.

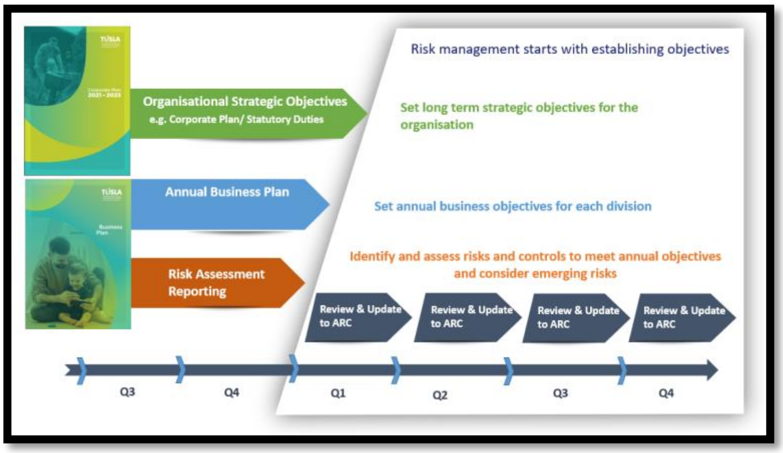

TUSLA
2021 - 2023
TUSLA
Business Plan
Organisational Strategic Objectives
e.g. Corporate Plan/ Statutory Duties
Annual Business Plan
Risk Assessment Reporting
Risk management starts with establishing objectives
Set long term strategic objectives for the organisation
Set annual business objectives for each division
Identify and assess risks and controls to meet annual objectives and consider emerging risks
Review & Update to ARC
Review & Update to ARC
Review & Update to ARC
Review & Update to ARC
Q3
Q4
Q1
Q2
Q3
Q4

Figure 2: Alignment of risk management to objectives

6.0 Roles and Responsibilities

Appendix 1 provides a high-level overview of the governance arrangements for Tusla in relation to risk management.

Whereas every staff member is responsible for identifying and managing risk within the context of their work, risk management is a line management responsibility and is a core management process. It must therefore be a focus of management teams at all levels in Tusla. The roles and responsibilities for staff at all levels in Tusla are outlined in **Appendix 2.**

Each management area (e.g. directorate, service, region, area) must clearly outline the governance arrangements for risk management to include roles and responsibilities (**Appendix 2**) and the process for notification and communication of identified risks and actions.

7.0 Risk Assessment

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

- Risk Identification
- Risk Analysis
- Risk Evaluation

These three steps are detailed below.

7.1 Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent an organisation achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks. An important aspect of risk identification is to generate a comprehensive list of threats and opportunities that may impact (enhance, prevent, degrade, accelerate or delay) the achievement of those objectives identified in the context.

The organisation can use a range of techniques for identifying uncertainties that may affect one or more objectives. There is no easy scientific method to guarantee that all risks will be identified. Some sources of information for identifying risks and Approaches to Identifying Risks are included in **Table 1**.

7.2 Risk Analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis should consider, amongst other factors:

- the category in which the risk can be recorded
- the likelihood of events (**Appendix 3**)
- the impact and consequences (**Appendix 3**)
- the effectiveness of existing controls

7.2.1 Risk Category

This policy requires that the risks be categorised to the area upon which they impact. For this purpose, Tusla has identified the following risk impact categories: Reputational and Profile, Financial, Physical and/or psychological harm, Service User Experience, Compliance, Business Continuity and Operational. See **Appendix 3** for examples of risk category areas which relate to each of the impact categories.

Whereas a risk may impact on a number of the areas listed above (secondary impacts) only one should be chosen as the primary category (area of primary impact), e.g. a risk that relates to physical harm may also result in poor service user experience and a loss of public confidence but if the physical harm was prevented the other two impacts would not have occurred. This will become important when it comes to assessing the risk.

Sources of Information	Approaches to Identifying Risks
Risk registers Activity information (e.g., referrals, waiting lists) Audit reports Media reports Review reports Complaints/Investigation reports Parliamentary questions Internal/external inspection reports A “Need to Know” (NTK) Incident reports Analysis of client feedback – complaints, client satisfaction, surveys, compliments Claims data Minutes of team meetings National reviews of major incidents Research/literature reviews	SWOT analysis (Strength, Weakness, Opportunity, Threats) Brainstorming One-to-one interviews Working groups Look at other jurisdictions (if it can happen to them, it can happen to us) PESTLE analysis (Political, Economic, Sociological, Technological, Legal, Environment) Surveys/Questionnaires Stakeholder analysis Process analysis Performance Management processes Review reports

Table 1 Sources and Approaches

7.2.2 Likelihood and Impact

Likelihood scoring is based on the expertise, knowledge, and experience of the risk owner. 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.

Determining the likelihood (frequency or probability) of the risk occurring 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 (for further guidance see **Appendix 3**).

Impact of the risk should be determined by the consequence (impact or magnitude of the effect) of the risk, should it occur, taking into account the adequacy of the existing controls.

Determining the impact 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 see **Appendix 3**).

It is responsibility of Risk Owner to define, determine, or measure objectively or subjectively the likelihood and impact scoring.

Each risk should be assigned a risk level (rating), taking into account the adequacy of the existing controls using the 5 x 5 Risk shown in **Appendix 3**. 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).

This rating will assist both in the evaluation of risk and the prioritisation of the management of risks.

7.2.2.1 Inherent and Residual Risk Rating

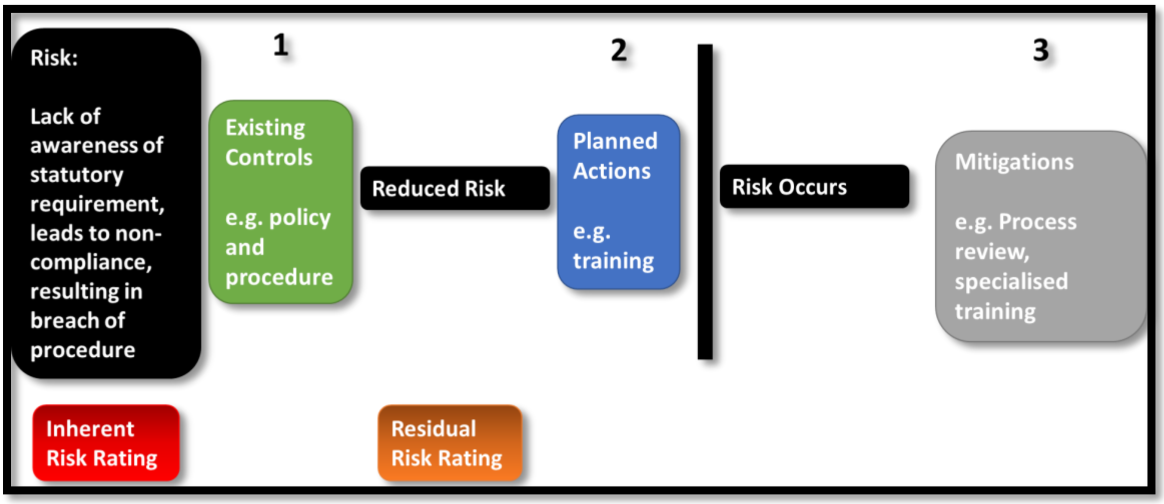

Risk:
Lack of awareness of statutory requirement, leads to non-compliance, resulting in breach of procedure
1
Existing Controls
e.g. policy and procedure
Reduced Risk
2
Planned Actions
e.g. training
Risk Occurs
3
Mitigations
e.g. Process review, specialised training
Inherent Risk Rating
Residual Risk Rating

Figure 3 Inherent and Residual Risk Rating

As Figure 3 above shows, two risk ratings can be applied to a risk. The first, prior to consideration of any controls (inherent risk rating) and the second, after controls have been considered (residual risk rating).

Inherent risk is the assessed level of a risk when there has been no consideration taken of the controls in place to reduce the likelihood or impact of the risk.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Residual risk is the level of risk left over after you have implemented the additional controls or other risk treatment option.

If the residual risk still remains at a high level, consideration may be needed of further risk treatment options which could result in the need to have plans developed to further reduce the impact or likelihood of the risk from occurring.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. See **Table 2** for an outline of the risk management elements.

Manage Risk		
Control	A control measure that maintains and/or modifies risk i.e. process, policy, device, practice, or other conditions, and or actions which maintains and/or modifies risk[10]. *Example:* Induction Guidelines and Checklists implemented	Evidence of the existing process, policy, device, practice or other conditions in place. Reviewed for effectiveness on a scheduled frequency
Action	An action is an additional control measure that is currently being put in place that further reduces either the likelihood of the risk occurring or potential impact of the risk. *Example*: In order to address a potential overspend, a cost control action plan is put in place, prior to next quarters risk management meeting, for allocation services within spend limits. Action owner is the Business Support Manager.	Actions should be **SMART** **S**pecific, **M**easurable, **A**ttainable, **R**elevant, and **T**ime-Bound
Mitigation	A mitigation is a plan or activity completed to reduce the impact of the risk when the risk occurs.[11] *Example:* To continue communication with relevant departments on the on-going inter agency collaboration that relies on the provision of particular services	Mitigations should be **SMART** **S**pecific, **M**easurable, **A**ttainable, **R**elevant, and **T**ime-Bound

Table 2: Risk Management Elements

7.3 Risk Evaluation

The purpose of risk evaluation is to support the decision-making process in relation to the management of risks. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further
- consider further risk treatment options
- undertake further analysis to better understand the risk

[10] Taken from Clause 3.8 ‘Control’ ISO 31000:2018 Risk Management Guidelines

[11] Adapted from Risk Management Guidance for Government Departments and Offices (February 2016) Department of Public Expenditure and Reform (DPER)

- maintain existing controls
- reconsider objectives

8.0 Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. ISO 31000:2018 Risk Management Guidelines sets out risk treatment as an iterative process.

Options for treating risk may involve one or more of the following[12]:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- retaining the risk by informed decision.

It is important, where possible, to have a combination of the different types of controls that are required to reduce the risk e.g. preventative, directive and detective. Evidence of these controls in operation, e.g. monthly health and safety reviews etc. needs to be included. The effectiveness of a control can be determined through whether the risk is eliminated or reduced by the proposed control measures.

To manage the risk, additional controls/actions may be required. These should be listed as discrete actions that can be assigned to a named individual and the action should relate to a deliverable. The timeframe for completion should be agreed with the Action Owner, see **Table 2** above for an example. Actions can be assigned to the Manager of the service, a member of the service's Management Team or to the person the Manager reports to.

While all possible actions should be taken to reduce or mitigate risk, it may not be possible to complete all actions identified as required. This could be due to a resource or other constraints.

As a Manager, it is important that you have acted to minimise risk in relation to any actions required that are within your span of control and that you have communicated appropriately actions that lie

[12] Taken from Clause 6.5.2, ISO 31000:2018 Risk Management Guidelines

outside of your control. You must be able to demonstrate[13] that you have fulfilled your responsibility to your Manager.

It is legitimate for the agency to 'accept' a level of residual risk if this is done within the appropriate governance framework.

9.0 Communication and Consultation

Communication and consultation should be timely and ensure that relevant information is collected, collated, synthesised and shared, as appropriate, and that feedback is provided, and improvements are made.

9.1 Notification

It is essential that there are clear routes and processes for the communication and notification of risk from one level of Tusla to another. It is also important to note that this communication and notification does not absolve the responsibility of the Risk Owner, to which the risk relates, of taking any actions required to treat the risk that are within their scope of responsibility, authority and budget.

When a risk is notified to a more senior manager, that manager can:

- Review the risk and decide not to accept it for active management on to their risk register.
- Assess that risk in the context of their area of responsibility, include it on their risk register and decide if it or actions relating to it need to be further notified.

It is with the agreement of the relevant line manager/senior manager that a risk can be captured on their risk register. The outcome of these considerations must be formally communicated back to the service that notified the risk.

9.2 National Corporate Risk Register

The Chief Risk Officer (CRO) has overall responsibility for the management of the National Corporate Risk Register (NCRR) with the assignment of the individual risks to relevant risk owner. The addition of a risk to the NCRR must be sent to the CRO for acceptance.

The CRO function, although located in Q&R directorate, is an independent function in respect of the NCRR and has direct access to the CEO and Chair of the Audit and Risk Committee in this regard.

[13] Examples of evidence include emails, action plan updates, meeting minutes etc.

The risk management framework is reviewed by the Board. Risks that are considered to have an impact on a strategic objective are identified and recorded on the National Corporate Risk Register.

The Board established an Audit and Risk Committee (ARC) to give an independent view in relation to risks and risk management systems (**Appendix 1**).

10.0 Monitoring and Review

Risks on the risk register must be subject to ongoing monitoring at risk management meetings by the risk owner to ensure that actions identified as required are completed. With the completion of actions, the level of risk (the rating) may be reassessed in order to consider whether its likelihood or impact score has reduced.

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. Minimally, all risk registers should be reviewed on a quarterly basis.

11.0 Recording and Reporting

The outcome of the risk assessment and treatment should be documented on a risk register and these should be discussed at risk management meetings and when risk is an agenda item at other relevant meetings.

Tusla has deployed an online risk register and where this has been made available to your line manager/senior manager it must be used. In areas where deployment has not occurred and where there is not a system currently available to you, services should use the standardised risk register tool available on the Tusla Quality and Regulation intranet site.

12.0 Closing Risk

When a risk is no longer impacting on an objective as it has passed or merged, it should be recorded as closed.

13.0 Monitoring implementation of and compliance with policy

Each management area is responsible for the implementation of, and monitoring compliance with this policy within their area of responsibility. The Quality and Regulation Directorate will provide implementation support through the Risk Management Team.

To support implementation, training will be developed and delivered. Targeted training will also be available to staff. Ongoing advice and support will be available through the Quality and Regulation Directorate and relevant staff responsible for quality, risk and incidents within service areas at operational levels. Supporting guidance and tools will be made available on the Tusla Hub.

To provide assurance, the Chief Risk Officer (CRO) is responsible, at a national level, for reviewing and reporting on compliance. The CRO reports regularly to the Senior Leadership Team, and Tusla’s Board and Risk and Audit Committees.

14.0 Dissemination

This policy document will be disseminated through the approved management structure of the Agency and will be available on Tusla’s Hub. Its publication will be supported by a broadcast email to all staff.

15.0 Related Policies and Guidance

- Code of Practice for the Governance of State Bodies
- Tusla – Child and Family Agency Code of Governance
- ISO 31000:2018 Risk management – Guidelines

Appendix 1: Risk Management Governance Structure

Structure / Reporting Line	Monitor and Oversight of Level Below	Risk Registers	Evaluation and Notification of Risk
Board, Audit and Risk Committee	↓		↑
Chief Executive and Executive Management Team		National Corporate Risk Register	↑
Chief Risk Officer			
Executive Management Team	↓	National/Regional Service/ Functional Delivery Management	↑
Service Delivery / Functional Management e.g. Regional Chief Officers, Service Directors	↓		↑
Approved Local Management Structures in the Regions and Services	↓	Service/Function Delivery Unit	↑
All Staff			

Appendix 2: Roles and Responsibilities for Risk Management

Board of Tusla	The Code of Practice for the Governance of State Bodies sets out the roles and responsibilities of the Board and Audit Risk Committee. This includes details of the key elements of the Board's oversight of risk management.
Audit Risk Committee (ARC)	The Code of Practice for the Governance of State Bodies sets out the roles and responsibilities of the Board and Audit Risk Committee. The ARC has a particular role, acting independently of the management of Tusla, to ensure that the interests of Government and other stakeholders are fully protected in relation to business and financial reporting and internal control. They provide an independent view in relation to risks and risk management systems.
Chief Executive Officer	The Chief Executive Officer and his/her Leadership Team are responsible for the identification of priority risk management issues and to ensure that the corporate and service planning processes have regard to the priority risk management issues so identified. The Chief Executive Officer has committed to the promotion of a risk management culture which ensures the safe delivery of services within Tusla. The Chief Executive Officer has nominated the National Director for Quality and Regulation as the executive lead for risk.
Executive Management Team	The Executive Management Team is responsible for: ▪ Committing to and promoting culture where risk management is embedded into the planning of safe delivery of services. ▪ Ensuring that the Organisational Risk Management Policy and related guidance are implemented throughout their areas of responsibility.
Chief Risk Officer (CRO)	The Chief Risk Officer is responsible for proactively: ▪ Assisting the Board and senior leadership team in fulfilling their respective risk oversight responsibilities. ▪ Establishing on-going risk management practices suitable for the Agency's needs. ▪ Overseeing risk management ownership within the respective lines of accountability. ▪ Promoting risk management across the Agency and assisting in integrating practices into business plans and reporting. ▪ Escalating identified or emerging critical risk exposures to executive management and the board. ▪ Support the Board in establishing the Agency's risk appetite and risk limits. ▪ Supporting the Board to ensure it is in full compliance with the Code of Governance and its associated requirements.
Quality Risk and Service Improvement Staff	The Quality Risk and Service Improvement Staff are responsible for proactively: ▪ Supporting, facilitating and advising relevant line managers on the technical aspects of the risk management process. ▪ Supporting the continued implementation, compliance and monitoring of the Organisational Risk Management Policy and related guidance throughout the agency. ▪ Supporting risk register development, monitoring and evaluation. ▪ Supporting local teams with advice on matters relating to risk management. ▪ Supporting learning and development in relation to risk management practice in local area.

	▪ Encouraging and supporting staff through change processes as they relate to quality, risk and service improvement. ▪ Reporting on risk.
Managers	All Managers are responsible for: ▪ Implementation of and checking compliance with Tusla's Organisational Risk Management Policy and related guidance in their area of responsibility. ▪ Ensuring that appropriate and effective risk management processes are in place within their delegated areas. ▪ Ensuring that risk assessments are undertaken throughout their areas of responsibility. The risks identified are prioritised and action plans formulated. These action plans will be monitored through the management meetings ▪ Identifying their own and staff training needs to fulfil the function of managing risk. ▪ Ensuring that all staff are made aware of risks within their working environment and their personal responsibilities within the risk management framework. Where appropriate, Managers are responsible for ▪ Maintaining a risk register. ▪ Formally reporting high and extreme risks via the management meetings.
Staff	All Staff are required to: ▪ Be conversant with Tusla's Organisational Risk Management Policy and have a working knowledge of all related risk processes. ▪ Comply with Tusla PPPG's to protect the health, safety, and welfare of any individuals affected by Tusla activity. ▪ Acknowledge that risk management is integral to their working practice within Tusla. ▪ Report any risk issues to their Line Manager. ▪ Attend training appropriate to role.
Risk Owner	All risks require assignment of a Risk Owner and it is the responsibility of the Risk Owner to ensure that the risk is assessed and managed in line with agency policy. This includes ensuring that any controls and actions identified as required to manage the risk have been assigned to a control/action owner along with an agreed date for completion of that control or action. The Risk Owner is normally the Manager of the area/service in which the risk is identified. It is the responsibility of the Risk Owner to notify risks or actions where appropriate.
Action Owner	An action is an additional control measure that is currently being put in place that further reduces either the likelihood of the risk occurring or potential impact of the risk. These should be described in a manner that will result in a tangible deliverable and be capable of being assigned to a specified post holder for implementation. It is the responsibility of the Risk Owner to ensure that due dates for completion of an action are agreed with the relevant Action Owner. The Action Owner is responsible for reporting on progress relating to the achievement of the action assigned to them. Completed actions may then become 'existing controls' in that they exist or are in place and serve to increase the control or management of the risk
Control Owner	A control measure that maintains and/or modifies risk i.e. process, policy, device, practice, or other conditions, and or actions which maintains and/or modifies risk[14]. It is the responsibility of the Risk Owner to assign the Control Owner and to set a future date to review the control to ensure that the control remains effective. Implementation of risk controls reduces the inherent risk level

[14] Taken from Clause 3.8 'Control' ISO 31000:2018 Risk Management Guidelines

Mitigation Owner	A mitigation is a plan or activity completed to reduce the impact of the risk when the risk occurs[15]. All mitigations require assignment of an owner. It is the responsibility of the Risk Owner to ensure that due dates for completion of a mitigation are agreed with the relevant Mitigation Owner. The Mitigation Owner is responsible for reporting on progress relating to the achievement of the mitigation assigned to them.

[15] Adapted from Risk Management Guidance for Government Departments and Offices (February 2016) Department of Public Expenditure and Reform (DPER)

Appendix 3: Impact and Likelihood

Likelihood							
Probability	Actual Frequency	Likelihood Score					
99%	At least monthly	Almost Certain (5)	5	10	15	20	25
75%	Bi-annually	Likely (4)	4	8	12	16	20
50%	Every 1 – 2 years	Possible (3)	3	6	9	12	15
10%	Every 2 – 5 years	Unlikely (2)	2	4	6	8	10
1%	Every 5 years or more	Rare / Remote (1)	1	2	3	4	5
		Impact Score	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
	Impact	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
		Physical and/or psychological harm	• 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 members 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
		Business Continuity	• Minor disruption, solved using standard processes, policies	• Short term disruption, solved using standard processes, policies	• Some disruption to service • High impact on business processes	• Sustained loss of service • Deviation from normal business processes e.g. singular event	• Permanent loss of core service or facility • Reputation seriously damaged • Large scale damaging event
		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

Risk Level	
VH	Very High Risk
H	High Risk
M	Medium Risk
L	Low Risk

TÚSLA

An Ghníomhaireacht um
Leanaí agus an Teaghlach
Child and Family Agency

The Brunel Building, Heuston South Quarter, Saint John's Road West, Dublin 8. D08 X01F
Phone: 01 771 8500 | Email: info@tusla.ie

www.tusla.ie