Risk Management Policy and Procedures

Version Number	1	**Document Owner**	Operational Director
Date of Issue	30th Oct 2020	**Review Body**	The Board
Next Review Date	30th Nov 2025	**Original Date of Issue**	30th Oct 2020
Communication	The Risk Management approach is principally utilised in the programme and project management structures, and, included in management practices.		

Version	Date	Status	Comment
1	30th Oct 2020	Released	Definition of the policy and procedures
1	30th Nov 23	Reviewed	No additions added

Contents

1. Introduction

The purpose of this document and of the following risk management approach is to ensure there is a consistent and effective approach to the process of identification and management of risks across the organisation. Some level of risk is inevitable, but the aim of this policy and procedures document is to ensure that every effort is made to manage risk appropriately by minimising any adverse effects and maximising potential opportunities.

2. Identifying risk to the organisation

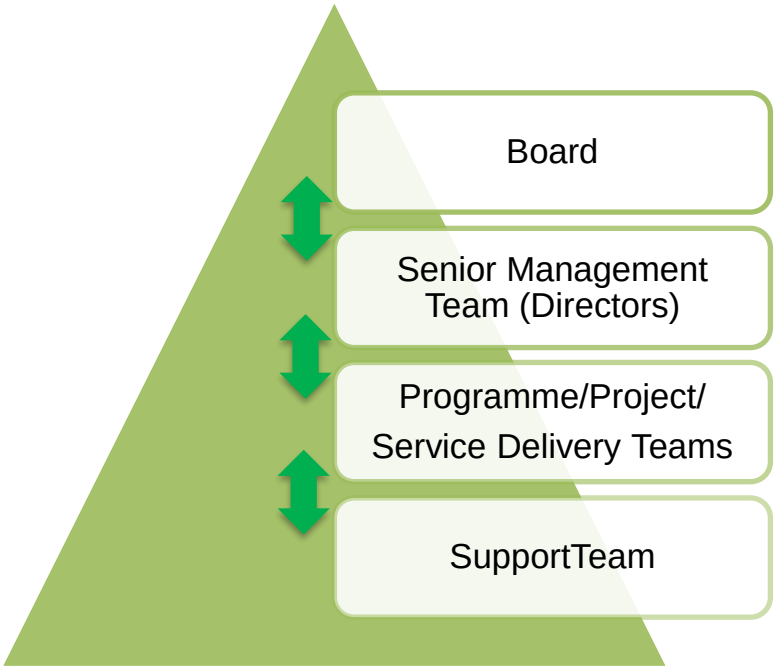
There are many different types of risks that an organisation may face including damage to the organisation's reputation, poor governance, physical risks to people, breaches of regulations and poor management of resources.

There are a number of different risk categories related to our organisation's operations and structure. These are listed below with accompanying examples of the types of risks within these categories (these are not exhaustive):

Contracts	• Failure of partner or partners to deliver • Termination of contracts • Failure to adhere to monitoring arrangements
Management	• Loss of key staff • Recruitment and retention issues • Failure to deliver strategic or business plans
Assets	• Mis-use or loss of our assets • Damage, loss, impact on our Property – building and equipment, either owned or leased by the organisation • Information – security, retention, timeliness, accuracy, intellectual property rights
Political	• Change in government priorities which lead to adverse impact on clients or sponsors of the organisation
Financial	• Loss of/reduction in funding • Fraud or other criminal financial loss • Ineffective or inefficient controls in place
Governance	• Lack or failure of decision making
Regulatory	• Failure to meet the annual regulatory criteria as a not-for-profit organisation • Failure to meeting Funders' requirement
Reputation	• Negative publicity, either locally or nationally, about the organisation or one of its staff members or consultants • Damage to credibility through failure to deliver services to the satisfaction of clients
Socio/economic environment	• Limitation on delivery of services due to circumstances beyond the organisation's control, for example, Covid 19 or other phenomenon or disruption

Escalation of risk

The escalation of risk within an organisation is a key mechanism for ensuring that risk is managed at the appropriate level by the appropriate individuals. Relating this to organisation's risk governance framework, the escalation channels are illustrated below:



Escalation of the risk should occur in the following circumstances:

- If the risk is exceeding the risk appetite set by the Board for that type of risk and there are no further actions available to reduce it
- If the current risk owner does not have the delegated authority to manage the risk
- If the risk is shared with other programme/project/service delivery teams, or with external organisations, and agreement is not being reached on how to manage it effectively

Risks are escalated to the next accountable level i.e. a risk deemed to be too great for the risk owner at a programme/project/service delivery level will then be escalated and considered for inclusion at the next level, or, ultimately in the Strategic & Escalated Risk Register.

3. How to escalate risk

It is important to note that risk does not just increase or materialise once a quarter. It is key that the organisation's procedures are flexible and responsive to emerging risks in order to manage them effectively.

Discussion about emergent risks or potential risks should freely occur in planning, in 1:1 meetings, in team or programme meetings and senior management meetings. Where timely, these should be captured and documented as a matter of record so that they can be accessed at all times, and when recorded properly, the description of the risk should be easy to understand by any person who has access to the record.

A regular review of these risk records should be undertaken by a designated person or team in the organisation. Where this is not possible, the situation must be escalation and discussed with the respective Director.

In the case of any potential new or increased risk which needs to be escalated to the organisation's Strategic and Escalated Risk Register, the Director designated responsible for this should be informed as soon as practically possible so this can be recorded appropriately.

4. Reviewing and reporting risk within the organisation

Risks are rated at three different levels; red, amber, green (RAG), depending on their likelihood and impact – these are on a scale of 1 to 5 for each category which when multiplied together provide a RAG rating score - and the management attention and resource committed to mitigating each of these categories of risk should also be allocated proportionately.

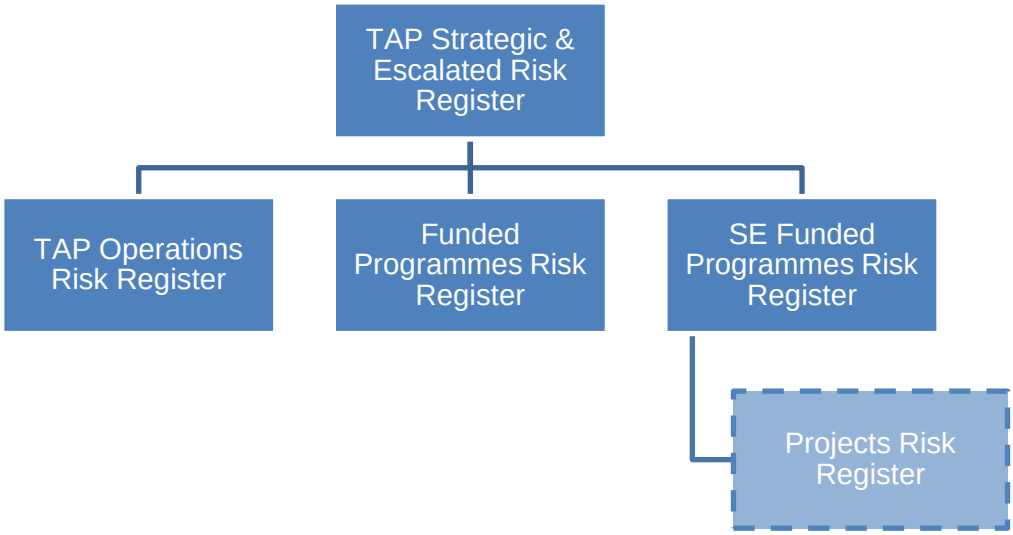
The table below outlines an approach for this for the Operational/Funding Registers:

Residual Risk Level and Score	**Frequency of Risk Reviews**
Red 12+	These are significant risks which may have a serious impact on the achievement of objectives if not managed. Immediate management actions need to be taken to reduce the level of residual risk. All red residual risks, at strategic and operational/funding level, should be reported the Board. **As a minimum review* <u>monthly</u> by the Directors and quarterly by the Board, until the risk is reduced. This review should include the cumulative/progressing impact of the mitigating actions.** **Decisions will need to be taken on whether these risks and mitigating actions should also be reported to any associated funding organisation.** ** The review period will be set by the Directors, but as a minimum it will be monthly, depending on the severity of the risk.*

Amber 6–10	These risks may require some additional mitigation to reduce the likelihood of their occurrence, if this can be done cost effectively. Reassess to ensure conditions remain the same and existing actions are operating effectively. **As a minimum review <u>quarterly</u> at Director level.**
Green 1-5	These risks are being effectively managed and any further action to reduce the risk would be inefficient in terms of time and resources. Ensure conditions remain the same and existing actions are operating effectively. **As a minimum review <u>6-monthly or a reasonable period for the programme</u>. Risks may reduce further and fall from the respective Risk Register.**

At a project/service delivery level, Directors may also wish to replicate this process for reviewing risks within their own areas, then using the escalation process when necessary (as stipulated).

5. How the organisation's Risk Registers fit together



Sitting underneath the Strategic and Escalated Risk Register are a number of different risk registers. These are owned by different teams or operational areas - ie, Operations/ Funded Programmes/ SE Funded Programmes, and where appropriate, specific Projects by scale or importance. On a monthly by month basis, the owner of each risk register is prompted to report any necessary escalations to the main Strategic and Escalated Risk Register. These are then reviewed by following the criteria in the table in section 4.

All mitigating actions are recorded in the appropriate risk register

Any mitigating actions that are agreed to lessen or counteract the identified risk, are recorded in the appropriate risk register. This will be done in such a way that anyone who is reviewing the risk register is able to clearly understand the actions taken and their resultant outcomes.

6. Using a Lessons Learnt Review process to manage risk

As a tool for managing ongoing risk and mitigating future materialisation of risk, the organisation operates a *Lesson's Learnt Review (LLR) process,* part of which records and logs learnings and corrective actions from the occurrence of a 'high impact' classified risk, which is deemed an 'incident' by the Board. This enables the organisation to utilise learnings in the planning of future activities, and, prevent these types of incidents from reoccurring or progressing further.

Any incident that is reported or referred to an external client, funding body or associated regulator (eg, regulator for GDPR), must be taken through a LLR process.