mentalwelfare commission for scotland

Policy Title: Risk Management Policy	Policy Number: 67
Issue Number: 001	Date of First Issue: June 2019
Date of Last Review:	Date of Next Review: June 2022
Lead Person: Head of Corporate Services	Approved by: AR&IG Committee

Contents

Risk Management Policy

1. Introduction

1.1 This document sets out the Mental Welfare Commission's policy on the management of risk.

1.2 A risk is a circumstance, event or factor that may have a negative impact on the operation of the Commission or on its ability to achieve its corporate objectives. Risks can be the result of internal conditions, or external factors that may be evident in the wider business environment.

1.3 Risk management is the process that seeks to eliminate or minimise the level of risk associated with a business operation. Essentially, the process should identify the situations that could result in damage or ineffectiveness of any of the Commission's resources (including Staff and Board Members), identify the steps to remove, reduce or mitigate the effects of those situations and then take those steps.

2. Objectives

2.1 The Commission's objectives for risk management are:

- To identify, control, eliminate or reduce to an acceptable level all risk which may adversely affect:

    the health, safety and welfare of service users, participants to NCF and employees;
    the quality of our services;
    the ability of the Commission to provide services; or
    the ability of the Commission to meet its statutory requirements;
    the Commission's reputation

- To maximise the resources available to protect people with mental illness, learning disability or related conditions.
- To ensure the effective, efficient and equitable use of resources.
- To understand the risks the Commission faces, their causes, and control and the cost of risk to the Commission.
- To learn from experience and develop a learning, supportive and open culture.

3. Policy Principles and Approach

Principles

3.1 The Commission will embed risk management in its corporate decision-making ensuring that the impact of policy decisions on risk is considered each time a strategic decision is taken or a policy is approved.

3.2 The Commission will ensure that all processes and procedures are designed to minimise risk and the impact of risk.

3.3 The Commission will foster a culture that embeds risk management into all aspects of its business.

3.4 The Commission will ensure that risk management is embedded in strategic, financial and business planning, as well as its project management approach.

3.5 The Commission will maintain strategic and operational risk registers that are updated regularly.

3.6 In order to manage and mitigate risk, the Commission will promote a culture of risk management and put in place arrangements for ongoing review of risks and an action plan for risk management.

3.7 The Commission will ensure through the risk management arrangements that risks to the quality and delivery of our services are minimised and that the services, reputation and finances of the Commission are protected.

3.8 The Commission will take appropriate action to control or eliminate risks identified. The management of risk will be integral to the corporate governance of the Commission.

3.9 All Board members, National Confidential Forum members and staff have a responsibility to maintain a general risk awareness, participate in risk management training and comply with policies and procedures.

3.10 To reflect the operational arrangements and associated risks, the Commission has developed:

- Commission strategic risk register
- Commission operational risk registers for each individual business area: visits, investigations, engagement and participation, monitoring, and corporate services.
- Action plans for improvement for the strategic and operational registers
- NCF risk universe and action plan

Risk scoring

3.11 Risks will be scored on likelihood and impact.

3.12 A table in **appendix 1** sets out the scoring matrix.

Risk appetite

3.13 The Commission's risk appetite is usually low. This means that we would seek to minimise of reduce risk as far as possible and direct resources to making our operating environment as low-risk as practicable, balancing the costs of mitigating or removing risk with the impact and likelihood of it.

3.14 However, in certain areas the Audit, Risk and Information Governance Committee and Board may set a higher appetite where this is deemed necessary to meet a justifiable need in the effective and efficient delivery of our functions. More detail is provided in Appendix 2.

Ownership of risk

3.15 The overall strategic risk register is owned by the Board and Chief Executive.

3.16 Operational risk is owned by the Operational Management Group and each risk will have a named responsible manager from within that group. The OMG will ensure that all staff participate in the management of risk whether through direct ownership or through application of policies and procedures.

4. Reporting and Assurance

4.1 Risk is ultimately owned by the Board. The Board receives assurance that risk is being monitored and managed appropriately from:

- The Audit, Risk and Information Governance Committee
- The Chief Executive
- The Operational Management Team
- Internal and External Auditors (regular audits and ad hoc, specific audits)

4.2 The sources of assurance are:

- Audit, Risk and Information Governance Committee reporting
- Risk Register
- Management reporting
- Key Performance Indicators
- Feedback from staff and other stakeholders

4.3 For each strategic risk the following will be reported:

- Definition and details of risk
- Gross (inherent) risk
- Current/ongoing mitigations
- Net (residual) risk
- Target risk
- Planned or further mitigations to assist in meeting the target risk.

Structures and Responsibilities for Managing Risk

4.4 Risk is proactively managed through monitoring and review of activity associated with or impacting on risk and its management. Review is managed through:

Audit, Risk and Information Governance Committee

4.5 The Audit, Risk and Information Governance Committee has delegated responsibility for the overall risk management strategy and to ensure it is incorporated into the business plans of the Commission and NCF and is monitored and reviewed regularly.

4.6 The Audit, Risk and Information Governance Committee will monitor and review risk through the monitoring of the strategic risk register and outputs of internal and external auditors. The Audit, Risk and Information Governance Committee will also have access to operational risk registers should they require them.

4.7 Where necessary, the Audit, Risk and Information Governance Committee will direct the Chief Executive and the Operational Management Group to take appropriate action, or refer issues to the Board for discussion and policy decisions, particularly in relation to operational risks directly in relation to the Board.

4.8 The Audit, Risk and Information Governance Committee will report annually to the Board to give assurance that risk is being appropriately managed.

Risk Management Group

4.9 The Commission has a Risk Management Group whose function is to develop the risk universe and to identify the consequence and likelihood for each risk identified. The group will review the strategic risk register and operational risk registers once a year and report to Operational Management Group.

4.10 Members of the group will be Head of Corporate Services, 3 members of the corporate services team, 2 practitioners and one casework administrator.

4.11 The group will meet at least annually. Extra meetings may be held during the year if major changes to the risks facing the Commission become apparent.

4.12 The group also meets once per year to review the Business Continuity Plan.

Operational Management Group

4.13 Each member of the Operational Management Group will be responsible for maintaining the operational risk register for their area of responsibility. Each operational risk register will be reviewed by the Operational Management Group annually. There will be separate risk registers for: visits, investigations, monitoring, engagement and participation, and corporate services.

4.14 An action plan for risk management will be developed and monitored by the Operational Management Group three times a year. This will be based on the strategic and operational risk registers. The Operational Management Group will report to the Audit, Risk and Information Governance Committee three times a year.

4.15 The Operational Management Group will also be responsible for the development and monitoring of the business continuity strategy and action plan.

4.16 The Operational Management Group will report to the Chief Executive and Audit, Risk and Information Governance Committee and provide assurance through reporting on action taken and its effectiveness.

Chief Executive

4.17 The Chief Executive will report to the Audit, Risk and Information Governance Committee through review of the strategic risk register and in bringing ad hoc issues to the attention of the Audit, Risk and Information Governance Committee outwith the regular reporting cycle.

4.18 The Chief Executive is responsible for ensuring the strategic risk register is reviewed and updated regularly as part of the assurance to the Audit, Risk and Information Governance Committee and Board.

4.19 The Chief Executive is responsible for monitoring and managing the operational risk registers through his role on the Operational Management Group.

National Confidential Forum

4.20 The Forum, supported by the NCF Project Manager, will develop a risk universe and to identify the consequence and likelihood for each risk identified. An action plan will be developed from the risk universe and reported to each Forum meeting and to the Audit, Risk and Information Governance Committee three times a year.

Internal and External Audit

4.21 Auditors will bring to the attention of the Management Team, Chief Executive and Audit, Risk and Information Governance Committee any areas of risk and report on the effectiveness of the Commission's risk management. Auditors will also provide advice and guidance in relation to risk management and specific areas of risk.

Risk Register

4.22 The 'risk register' is a generic name for a series of documents that collectively enable a proactive approach to identification and management of risk. It consists of:

4.23 **Strategic risk register – detailed information sheets** – a detailed set of information sheets, one for each individual risk, setting out the information required under this policy.

4.24 **Strategic risk register – risk summary** – a numbered summary of the identified risks, their likelihood of occurrence, their impact and which operational risks contribute to the factors. The aim is to keep this at a strategic level, linked to the corporate strategic objectives. It is the overarching document into which other registers feed. The strategic risk register is owned by the Board and Chief Executive and monitored and reviewed by the Audit, Risk and Information Governance Committee.

4.25 **Operational risk registers** – will be produced for each operational area of work. These consist of a numbered summary of operational risks that collectively feed into the strategic risk register. These should be reviewed at least quarterly by the Executive lead responsible for the operational area.

5. Summary of Roles and Responsibilities

5.1 Roles and responsibilities are summarised as:

Party	Responsibility	Role	Frequency of reporting
Board	Ownership of Commission risk and risk policy	• Approve risk management policy • Assurance that policy is applied and strategic risk is managed effectively	As required to external and internal stakeholders
Audit, Risk and Information Governance Committee	• Monitoring of risk management activity • Providing assurance to the Board	• Oversee and monitor the risk policy and risk management activity. • Review the strategic risk register (and on request, the operational risk register) • Direct the Chief Executive and Management Team as appropriate • Provide support and advice to the Chief Executive and Management team as appropriate	• Annually to the Board
Chief Executive	• Shared ownership of risk • Management of risk • Providing assurance to AC	• Ensure that risk registers are updated and reviewed regularly • Own and manage the operational risk register • Report and provide assurance to Audit, Risk and Information Governance Committee • Ensure risk is managed in line with the risk registers and other direction from Audit, Risk and Information Governance Committee and/or the Board • Ensure that staff and managers are appropriately briefed and trained to manage risk	• Three times a year to Audit, Risk and Information Governance Committee • Annually to Board
Operational Management Group	• Shared ownership of risk • Management of risk • Providing assurance to Audit, Risk and Information Governance Committee and Chief Executive • Ownership of Operational Risk Registers	• Ongoing updating of the operational risk register for owned risks • Reporting and review of the risk register and action plan to Chief Executive, Operational Management Group Team and Audit, Risk and Information Governance Committee three times a year. • Ensure staff are aware of risk that it is embedded in processes and performance management and that staff are appropriately trained to deal with risk.	• Three times a year to Audit, Risk and Information Governance Committee on strategic risk register • Annually to Chief Executive on Operational risk registers • As required to Chief Executive
Internal and External Audit	• Report and advise on risk to Audit, Risk and Information Governance Committee and Chief Executive • Provide assurance to Audit, Risk and Information Governance Committee	• Carry out and report on audits to the programme agreed with the Commission • Give appropriate advice to the Commission at all levels in relation to risk management • Bring concerns about risk to the attention of the Chief Executive and Audit, Risk and Information Governance Committee	• As agreed through audit programme

All staff	• Operational management of risk through application of policies and procedures	• Contribute to the management of risk through applying policies and procedures appropriately and consistently • Raise concerns or identified risk with line management, Chief Executive, Operational Management Group or Board as appropriate.	• As required by line management

Appendix 1 – Scoring Template

SIMPLE RISK QUANTIFICATION

AS/NZS 4360:1999 Risk management defines risk as “The chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood.”

Risk = Consequences x likelihood

A simple approach to quantifying risk is to define qualitative measures of consequences and likelihood such as the exemplars given below. This allows construction of a risk matrix that can be used as the basis of identifying acceptable and unacceptable risk.

QUALITATIVE MEASURES OF CONSEQUENCE

LEVEL	DESCRIPTOR	DESCRIPTION
1	Negligible	No impact on Commission objective. Low financial loss.
2	Minor	Limited impact on Commission activities. Moderate financial loss.
3	Serious	Commission fails to meet key part of its objective. Moderate environmental implications. High financial loss. Moderate loss of reputation. Moderate business interruption.
4	Major	Commission will not achieve objectives. High environmental implications. Major financial loss. Major loss of reputation. Major business interruption.

QUALITIVE MEASURES OF LIKELIHOOD

LEVEL	DESCRIPTOR	DESCRIPTION
1	Rare	The event may occur only in exceptional circumstances.
2	Unlikely	The event may occur at some time.
3	Moderate	The event probably will occur at some time.
4	Likely	The event is expected to occur in most circumstances.
5	Certain	The event will occur.

	Rare 1	Unlikely 2	Moderate 3	Likely 4	Certain 5
Major 4	4	8	12	16	20
Serious 3	3	6	9	12	15
Minor 2	2	4	6	8	10
Negligible 1	1	2	3	4	5

Appendix 2 – Risk Appetite Definitions

	Avoid	Minimal	Caution	Open	Seek	Mature
	Avoidance of risk and uncertainty is a key organisational objective	*(as little as reasonably possible) Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.*	*Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward.*	*Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.)*	*Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.*	*Confident in setting high levels of risk appetite because controls, forward scanning and responsive systems are robust*
1. Finance and best value	Avoidance of financial loss is a key objective. We are only willing to accept the low cost option as best value is our primary concern	Only prepared to accept the possibility of very limited financial loss if essential. Best value is the primary concern.	Prepared to accept possibility of some limited financial loss. Best value still primary concern, but willing to consider other benefits or constraints. Resource generally restricted to existing commitments	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable lever. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise opportunities	Investing in the best possible return and accept the possibility of financial loss (with controls in place). Resources allocated without firm guarantee to return – 'investment capital' type approach	Consistently focussed on the best possible return of stakeholders. Resources allocated in 'social capital' with confidence that the process is a return in itself
2. Political and policy	Play safe, avoid any confrontation of challenge of status quo	Play safe, avoid any confrontation of challenge of status quo unless on minor technical or legal changes	Play safe, broader changes considered but only changes likely to have support / or no opposition from all stakeholders	Risk / benefit analysis; changes considered positive for the Commission will be considered even if some likely opposition	Risk / benefit analysis; changes will always be pursued where positive for the Commission, even if some / significant likely opposition	Seeking leadership role in political and policy thinking through radical commentary on potential for change..
3. Quality and operational delivery	Avoidance of anything that could compromise quality	Only prepared to accept the possibility of very limited negative impact on performance against quality standards. Fairness is the primary concern	Prepared to accept possibility of some limited deterioration in performance against quality standards. Willing to consider other benefits linked to adverse performance where fairness is not compromised.	Prepared to consider metrics and performance and the benefits and constraints of meeting targets whilst managing associated risks to a tolerable level. Fairness to be considered first to ensure any decisions do not compromise.	Prepared to take a degree of risk when pursuing a new of innovative course of action to help improve performance and willing to accept the possibility of performance deterioration (with controls and checks in place for fairness)	Consistently focussed on pursuing new or innovative courses of action to deliver best in class performance. Willing to take risks to do so. Willing to accept performance deterioration as new approaches are tested (within controls and check in place for fairness)
4. Legal and regulatory compliance	Play safe, avoid anything which could be challenge, even unsuccessfully	Want to be very sire we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we could win.	Challenging would be problematic, but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better and more proportionate regulation

5. People	Defensive approach to people management – aim to maintain within headcount allocations and maintain current roles rather than create of innovate	Workforce innovations avoided unless essential or proven track record elsewhere	Tendency to stick to status quo in terms of workforce planning, innovations and new approaches avoided unless really necessary and linked to leadership management	Innovation supported, with demonstration of improvements in workforce output	Innovation and alternative approach pursued in order to challenge and change current practices and achieve improvements in workforce output and engagement.	Innovation and alternative approached pursued as a priority in order to challenge and change current practice and achieve improvements in workforce output and engagement.
6. Opportunity and innovation	Defensive approach to objectives – aim to maintain or protect, rather than create or innovate. Priority for tight management controls and oversight with limited devolved decision authority	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management.	Innovation supported,. With demonstration of commensurate improvements in management control. Responsibility for non-critical decision may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Devolved authority – management by trust rather than tight control is standard practice.
Appetite : **Acceptable level of residual risk**	**NONE**	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**