Care Inspectorate Risk Policy

Table of Contents

POLICY REVIEW DATE : May/June 2019

1.0 Introduction

This Risk Management Policy forms part of the Care Inspectorate's internal control and corporate governance arrangements. Separate operational documentation exists for risks relating to the inspection process.

This policy sets out how and why the Care Inspectorate carries out risk management, explaining the underlying approach to risk management, documenting the roles and responsibilities of the Board, senior management and other key parties.

2.0 Corporate Statement on Risk

The Care Inspectorate is the official body responsible for inspecting standards of care in Scotland. That means we regulate and inspect care services to make sure they meet the right standards. We also carry out joint inspections with other regulators to check how well different organisations in local areas are working to support adults and children. We help ensure social work, including criminal justice social work, meets high standards. We provide independent assurance and protection for people who use services, their families and carers and the wider public. In addition, we play a significant role in supporting improvements in the quality of services for people in Scotland.

By undertaking risk management, we will better manage the successful delivery of our objectives by both preparing for and understanding the implications of adverse events. We will also be better able to provide assurance to our stakeholders that we are managing risks and appropriately maximising business and public value opportunities.

The Care Inspectorate has adopted the 3 Lines of Defence model for summarising its governance of risk - this is attached as an Annex to this policy.

The following principles outline the Care Inspectorate's approach to risk management and internal control

- The Board has responsibility for overseeing risk management.
- An open and receptive approach to solving risk problems and addressing risk implications is adopted by the Board.
- The Chief Executive and senior managers support, advise on and implement policies approved by the Board.
- The Board will be clear about its appetite for risk, maintaining a formal statement
- We make conservative and prudent recognition and disclosure of financial and non-financial implications of risks.
- Managers are responsible for encouraging good risk management practice within their functional areas.
- Key risk indicators will be identified and closely monitored on a regular basis with changes in assessed risk regularly reported to the Executive Group, Audit Committee or Board as appropriate.

3.0 Risk Levels

Four risk levels have been identified as follows:

- Strategic Risks
- Directorate Risks
- Team Risks
- Programme / Project Risks

4.0 Risk Escalation Procedures

Risks will be escalated in cases where:

- the controls are not effective in managing a risk to the tolerance level
- the controls are not reflecting the risk velocity

Escalation of Strategic Risks – these will be reviewed periodically by the Executive Group who will decide what to escalate to the Board.

Escalation of Directorate Risks – a Director should escalate risks to the Executive Group when it is of corporate significance or is outside his/her agreed tolerances. This can require an action plan to be developed to mitigate any identified risks. The Executive Group will consider any escalated risks for treatment as a Strategic risk under Executive Group scrutiny.

Escalation of Team Risks – any high team risks will be escalated to the Directorate Management Team. It is the Director's role to manage the risk, acknowledging his / her greater level of delegated authority, greater strategic perspective of risk tolerance and ability to flex resources under his/her control. Directors will determine the correct treatment for an escalated risk following discussion with the Directorate Management Team before empowering the Head of Service/Chief Inspector to take action or tolerate an increased level of risk that would not normally be within their discretion.

Escalation of Programme / Project Risks – Programme and Project Risks will be identified by the Programme / Project Manager who will present and review these as appropriate with the Executive Group. The Executive Group will keep under review the need to escalate any Programme / Project risks for review as a potential strategic risk.

5.0 Roles and Responsibilities

5.1 Role of the Board

The Board has a fundamental role to play in the management of risk. Its role is to set the tone and influence the culture of risk management within the Care Inspectorate. This includes:-

- Determining the appropriate risk appetite or level of exposure for the Care Inspectorate

- Setting the standards and expectations of staff with respect to conduct and probity
- Approving major decisions affecting the Care Inspectorate's risk profile or exposure
- Monitoring the management of significant risks to reduce their likelihood
- Satisfying itself that risk management is appropriately practiced and embedded throughout the Care Inspectorate
- Through the Audit Committee, ensuring strategic risk is effectively monitored and appropriate responses are made to changes in assessed levels of risk
- Through the Audit Committee, annually reviewing the Care Inspectorate's approach to risk management and approving changes or improvements to key elements of its processes and procedures

5.2 Role of the Chief Executive

The Chief Executive, as Accountable Officer, is required to ensure there are sound and effective arrangements for internal control and risk management.

5.3 Role of Senior Management

Key roles of the Care Inspectorate's senior managers (Executive Group) are to:

- Implement policies on risk management and internal control
- Identify, monitor and evaluate the strategic risks faced by the Care Inspectorate for consideration by the Board
- Provide adequate information in a timely manner to the Board and its Committees on the status of risks and controls
- Undertake an annual review of effectiveness of the system of internal control and provide a report to the Audit Committee and Board
- Ensure operational risks in their areas of responsibility are identified, monitored and controlled, taking appropriate action to mitigate risks and escalating issues as appropriate
- Carry out a quarterly review of the strategic risks

6.0 Risk Management as part of the system of internal control

The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the Care Inspectorate to respond to a variety of operational and financial risks. These elements include:

a) **Policies and Procedures**

Attached to significant risks are a series of policies that underpin the internal control procedures. The policies are set by the Board and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b) **Regular Reporting**

Regular reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the Executive Group (and also the Board if appropriate).

c) **Corporate Planning and Budgeting**

The planning and budgeting process is used to set objectives, agree action plans and allocate resources. Progress towards meeting objectives is monitored regularly.

d) **Strategic Risk Review (significant risks only)**

A formal annual strategic risk review helps to facilitate the identification, assessment and ongoing monitoring of risks that are of strategic significance to the Care Inspectorate. The risk register is formally appraised annually but emerging risks are assessed and added as required. Risk indicators are monitored regularly to detect changes to risk profile. Improvement actions or risk mitigation actions are taken as appropriate. A similar approach is carried out for operational risks at a Directorate level.

e) **Audit Committee**

The Audit Committee is required to report to the Board on internal controls and alert the Board members to any emerging issues. In addition, the Committee oversees internal audit, external audit and management as required in its review of internal controls. The Committee is therefore well placed to provide advice to the Board on the effectiveness of the internal control system, including the Care Inspectorate’s system for managing risk.

f) **Internal Audit Programme**

Internal audit is an important element of the internal control process. Apart from its normal programme of work, which is regularly aligned to the strategic risks, internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the Care Inspectorate.

g) **External Audit**

External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the external audit as well as reviewing corporate governance and best value arrangements.

h) **Third Party Reports**

From time to time, the use of external consultants will be necessary in areas such as health & safety and human resources. The use of independent third parties for consulting and reporting can augment the reliability of the internal control system.

7.0 Risk Appetite

Why do we need to determine our risk appetite?

If managers are running the organisation with insufficient guidance on the levels of risk that are legitimate for them to take or are not seizing opportunities due to a perception that taking on additional risk is discouraged then organisational performance will not be maximised and business opportunities will not be taken. At the other end of the scale, an organisation constantly erring on the side of caution, or one that has a risk averse culture, is one that will stifle creativity, not necessarily encourage innovation or exploit opportunities.

Organisations that have not made a formal statement on risk appetite therefore have a control problem. Without such a statement, managers have insufficient guidance on the levels of risk they are permitted to take.

The Board has prepared a Risk Appetite Statement and this will be kept under annual review as a minimum. The Executive Group is responsible for developing Risk Tolerance Statements for individual risks in support of the overall Risk Appetite Statement.

8.0 Types of Risk and Response

8.1 Types of Risk

There are four broad classifications of risk as follows:

a) Internal Risk – these are risks over which the organisation has some control i.e. risks that can be managed through internal controls and mitigating actions. Examples include fraud, health & safety, capacity and capability and data security.

b) External Risk – this category focussed on big external events and then considers how to make the organisation more resilient. Risks in this category have a very low likelihood but overall, the chance of one out of the many occurring is not low. Examples include cyber attacks, extreme weather, building fire or flood. A tried and tested approach to such risks is through developing a resilience framework or business continuity plan.

c) Strategic Risk – this category focusses on the organisation's raison d'etre and key objectives (as set out in the corporate plan) identifying the principal risks to the achievement of those objectives within a set timeframe. Examples include immediate impact risks such as a sudden loss of case service data as well as slower burning risks that grow and eventually prevent delivery of objectives such as staff turnover or loss of leadership capability.

d) Major Projects – this category focusses on the major projects that need to be considered at Board level in their own right. There is no standard reporting format for this category. Risks could involve shifting requirements, failure to deliver or slippage in delivery timeframes of a major digital project.

8.2 Types of Response

There are 4 types of responses to risks:

a) tolerate – for unavoidable risks, or those so mild or remote as to make avoidance action disproportionate or unattractive

b) treat – for risks that can be reduced or eliminated by prevention or other control action

c) transfer – where another party can take on some or all of the risk more economically or more effectively e.g. sharing risk with a contractor

d) terminate – for intolerable risks, but only where it is possible for the organisation to exit

9.0 Risk Management Processes

9.1 Identification of New Risks

New Risks can be identified by the Executive Group or the Board and will be documented using the established pro-forma that captures risk data including : risk owner, link to Corporate Plan, risk description and consequences, scoring of raw risk, risk velocity, control measures, scoring of residual risk, risk indicators and further action required.

For a new risk, it is the Raw Risk score that determines how significant a risk is and whether it requires to be included on the Board Strategic Risk Register.

9.2 Review of Risks and Planning and Implementing Actions

The Board, through the Audit Committee, is responsible for reviewing the effectiveness of internal control of the Care Inspectorate, based on information provided by senior management. Risk is a standing item on all Committee agendas as well as being a standing item on the Board agenda.

The Audit Committee hosts a Board Development event annually to review the Strategic Risk Register. This includes examination of the Care Inspectorate’s track record on risk management and internal control. In addition, the Board considers the internal and external risk profile for the coming year and considers if current internal control arrangements are likely to be effective.

During the year, the Executive Group will consider and update in-year changes to the residual risk scores and update the Audit Committee accordingly. An additional form has been developed to support this process showing changes in **residual** risk.