An Roinn Coimirce Sóisialaí
Department of Social Protection

5 January 2024

Risk Management Policy

Contents

1. Purpose

Effective risk management supports the Department of Social Protection to prepare for uncertainty and respond to changes in its operating environment. Consequently, risk management contributes to the overall business resilience of the Department and supports the Department to achieve its strategic objectives.

The objectives of this Risk Management Policy are to ensure the Department of Social Protection has a systematic approach to risk management and to assist business areas in identifying, assessing, mitigating, monitoring and reporting on the risks to which the Department may be exposed.

In this context, a risk is considered as a possible loss or other adverse consequence that has the potential to interfere with the Department's ability to fulfil its mission.

2. Background

This policy is informed by Risk Management Guidelines published by the Department of Public Expenditure, National Development Plan Delivery and Reform. The guidelines require that:

- Each Department should include risk management as an integral and ongoing part of its management process.
- Departments should repeat the process of risk identification at least once a year.
- Departments should assess identified risks at least once a year.
- Departments should determine an appropriate method for addressing identified risks.
- Departments' risk management systems should provide for monitoring and reporting at various levels of management.

The Department's Risk Management Policy and practice complies with this guidance.

3. Risk Governance: Three Lines of Defence

The Department has adopted the "Three Lines of Defence" governance structure for the management of risk. This model is illustrated in Figure 1 and is a recommended approach for the effective management of risk. The three lines refer to the multiple internal risk monitoring and assurance functions within the Department, which provide assurance to senior management, governance committees and external stakeholders that risk is being effectively considered and managed. The following sections illustrate how the model is applied in the Department. It is based on a more comprehensive mapping of the Department's activities against the model, conducted by the Department's Internal Audit[1].

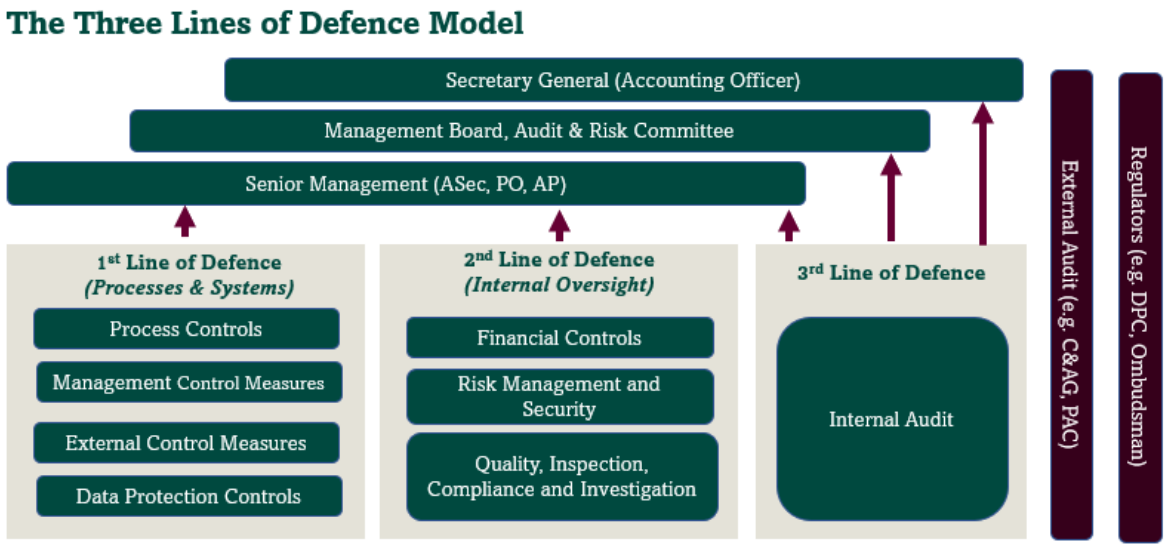


Figure 1: Three Lines of Defence Risk Governance Model (adapted from IIA, 2015)

[1] A more detailed mapping of the Department's activities against the model is available on the Governance page of the Internal Audit Unit site on Stór.

3.1 First Line of Defence

The first line of defence refers to the functions that own and manage risk. Within the Department of Social Protection each business area is required to manage the risks within their area through both management controls and internal control measures. In practice, this is primarily achieved through *process controls*, such as scheme take-on controls, sign-off requirements, etc, and *access controls*, e.g. system access controls, the use of "roles" in BOMi. This is supported by monitoring and accountability mechanisms such as regular reports, periodic reviews and checks such as quality controls.

3.2 Second Line of Defence

The second line of defence refers to the dedicated teams and functions, which have a specific role to play in risk management. For example, within the Department, the Accounts Branch team support financial oversight, Corporate Planning Unit provide oversight of risk management processes while the Cybersecurity and Data Protection Units actively work to reduce the risk of a data breach.

In addition, there are numerous compliance roles across the Department to mitigate against the risk of a failure to meet statutory requirements.

As one of the largest payment institutions in the State, the Department has a significant number of individuals working in control and investigation functions dedicated to managing the risk of fraud or abuse of public funds. These include Social Welfare Inspectors, Special Investigations Unit and Control unit.

3.3 Third Line of Defence

The Third Line of Defence is the provision of objective and independent assurance regarding the integrity of risk management. This is primarily delivered through the

Internal Audit function of the Department. Key to the integrity of the Internal Audit function is that it is independent of the Executive. Internal Audit assurance is reported to Senior Management, Management Board and the Audit and Risk Committee.

3.4 External Audit & Regulators

The Department's risk management is also subject to scrutiny by external audit and regulatory functions. These include Comptroller and Auditor General audits, the Data Protection Commissioner and the Ombudsman's Office. In addition, the Social Welfare Appeals Office, by offering an appeal mechanism to customers, allows the Department to review first-instance decision-making in relation to claims.

3.5 Secretary General, Management Board, Audit & Risk Committee and Senior Management

As Accounting Officer for the Department, the Secretary General has ultimate responsibility for risk management in the Department. In this role they are supported by the Management Board, the Audit and Risk Committee and senior management. More information on specific roles and responsibilities is provided in Section 5.

4. Risk Management Processes

Since 2011, a fully integrated Business Planning and Risk Management (BPRM) process has been used in the Department. The BPRM process is aligned to the Department's Statement of Strategy[2] and considers both risks to the delivery of activities within business areas and General Corporate Risks (GCRs). Management and reporting on business activities, associated risks and General Corporate Risks is supported by a custom-built SharePoint BPRM application.

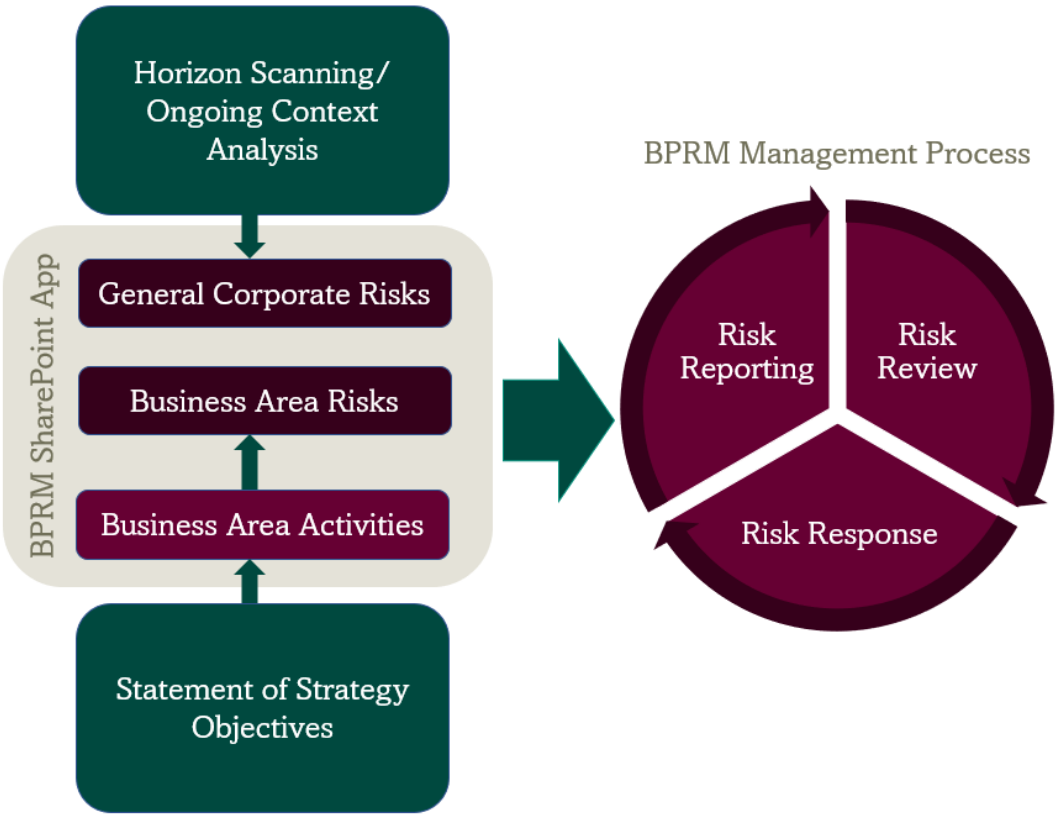


Figure 2: Department of Social Protection Business Planning & Risk Management (BPRM) Approach

The Department's BPRM approach is illustrated in Figure 2 and can be described as

[2] For more information on the relationship between the Statement of Strategy and BPRM see the Department's Corporate Governance Framework

follows:

- On an annual basis, all business areas identify activities for the following year aligned to an objective of the Statement of Strategy.
- For each activity, risks to the achievement of the activity are identified, as are actions to mitigate the risk.
- Each risk is scored (based on the likelihood of the risk occurring, the scale of its impact were it to occur and the controls in place to manage the risk) and a red/amber/green rating assigned based on the score.
- On an ongoing basis Management Board identify General Corporate Risks to the Department. These risks are scored and risk mitigation actions identified.
- The General Corporate Risks, Business Area Activities and Business Area Risks are all housed on a custom-built SharePoint application, which is fully accessible to Management Board and risk owners.
- All activities, risks and the General Corporate Risks are reported on quarterly via the SharePoint app.
- Updates on key business area risks, high risks and General Corporate Risks are reviewed and discussed four times a year at Management Board meetings. During these discussions risks may be revised, and additional risk-mitigating actions agreed.

5. Roles and Responsibilities

As **Accounting Officer** for the Department, the **Secretary General** has ultimate responsibility for risk management in the Department. However, in line with best practice for risk management[3], the responsibility and accountability for risks have been assigned at the appropriate level across the Department as follows:

Collectively, the **Management Board** is responsible for:

- Overall management of risk in the Department,
- Providing leadership in promoting risk management,
- Determining the Department's risk appetite,
- Approval and review of the Department's risk management policy and process,
- Monitoring the assessment and management of risk throughout the Department,
- Identification and management of General Corporate Risks, and
- Monitoring and reviewing the KPA and GCR quarterly progress reports.

Individually, each **Assistant Secretary** is responsible for:

- Ensuring accurate identification and reporting of risks within their business areas, and
- Ensuring effective control and mitigation measures are identified and put in place for risks within their business areas.
- Identification and oversight of General Corporate Risks relevant to their business areas.

[3] ISO 31000 Risk Management

In addition, the **Assistant Secretary with responsibility for Finance, Legislation and Corporate Services** is the Department's **Risk Officer**, with the additional responsibility for:

- Overseeing the risk coordination and reporting function provided by Corporate Planning Unit,
- Contributing to the National Risk Assessment, and
- Ensuring the Risk Policy is updated as needed.

Heads of Business Areas (Principal Officers) are responsible for:-

- Identifying, evaluating and managing risks as part of the overall business management process,
- Ensuring compliance with the integrated business planning and risk reporting requirements,
- Monitoring and reviewing the BPRM quarterly progress reports for their business area, and
- Promoting and ensuring risk management awareness throughout their business area.

GCR Updates Coordinators (usually Principal Officer level) are responsible for:-

- Providing quarterly updates on the status and rating of allocated General Corporate Risks,
- Compliance with GCR reporting guidelines and timeframes, and
- Updating the responsible Assistant Secretary of any significant changes to allocated GCRs.

Corporate Planning Unit is responsible for:-

- Supporting the Management Board with the development and maintenance of a risk management policy and process,
- Assisting and providing advice and guidance on business planning and risk management,

- Maintaining the integrated business planning and risk management (BPRM) application system, and
- Coordinating the production of quarterly and other progress reports on business activity and risks for the Management Board.

All Staff are responsible for:

- Notifying their manager of any new risks or significant changes to risk ratings.
- Where nominated by their manager, providing quarterly updates on business activities and associated risks in line with guidelines and requested timeframes.

The Audit & Risk Committee is responsible for:

- Considering and reviewing the Department's risk management arrangements and, as appropriate, advising the Accounting Officer on such arrangements.
- Communicating with the Secretary General and senior management in relation to any significant shortfalls in the business control and/or risk management environments that come to the attention of, and are of concern to, the Committee.
- Meeting with senior management of the Corporate Planning Unit, or the Department's Risk Officer if applicable, at least on an annual basis.
- Receiving quarterly reports on and considering the Department's General Corporate Risks.

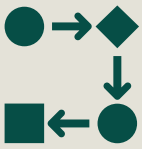
As an integral part of the Department's overall business control, risk management and governance environment, **the Internal Audit Unit** is responsible for providing independent oversight, assurance and advice on the integrity of the risk management process.

6. Risk Classification

In line with Department of Public Expenditure, National Development Plan Delivery and Reform guidelines, business plan risks are generally classified into four types of risks as follows:

Financial Risks: Risks with a financial implication, including risks related to fraud, mismanagement of funds or loss of assets. This also includes risks relating to the procedures, systems or accounting records in place to ensure that the organisation is not exposed to avoidable financial risks.

Strategic Risks: Risks that affect the achievement of the Department's mission. These may be external to the organisation such as the economic climate, including factors such as economic shocks, mass unemployment and inflation.



Operational Risks: Risks relating to the delivery of the Department's operations. This includes risks associated with supporting information systems and cybersecurity.

Reputational and Compliance Risks: Risks to the public reputation of the organisation which leads to lack of trust in its ability to fulfil its mission.

To delineate and support their effective management, General Corporate Risks are categorised separately to allow for an increased Management Board focus.

7. Risk Appetite

The Department recognises that risks cannot be eliminated entirely, and a degree of risk must be tolerated to effectively fulfil the Department's mission. The Department is committed to taking effective action to mitigate risks where feasible. The following risk appetite statement reflects the Department's risk tolerance for different classification of risks. The Department will invest as required in control measures and mitigating actions to ensure that risks remain within the specified risk appetite.

The following classification of Risk Appetite has been used for Risk Classification:

Classification	Description
Low	Preference for safe delivery options that have a low degree of risk.
Medium	Willing to consider all potential delivery options, including innovative approaches and choose the one that is most likely to result in successful delivery while also providing an acceptable level of value for money.
High	Eager to be innovative and to choose options with potentially higher inherent risk in the interests of delivering public goods.

Table 1: Risk Appetite Classification

The Risk Appetite Classification has been applied to each category of risk to provide a risk appetite statement for the Department.

Department of Social Protection Risk Appetite Statement

Risk Category	Risk Appetite
Financial Risk	**Low** risk appetite for loss of public funds. The Department of Social Protection has established extensive monitoring and control measures to identify and respond to attempts to defraud the DSP. Where incidents of fraud are identified, the DSP responds, as necessary, to retrieve funds. Most people supported by the Department claim and receive payments to which they are entitled. However, to protect the integrity of the system and target resources at those most in need, we continue to take all steps to combat social welfare fraud and error. Activities in dealing with financial risk are outlined here: DSP Compliance and Anti-Fraud Strategy 2019-2023 The Department has also developed a robust budgeting process to ensure that expenditure is monitored on a monthly basis throughout the year, comparing expenditure against profile and reporting variances to the Management Board, Minister and the Department of Public Expenditure, National Development Plan Delivery and Reform.
Strategic risks	**Medium** risk appetite for strategic risks. The DSP maintains a comprehensive oversight of strategic risks and proactively takes action to mitigate their impact on the delivery of the Department's mission.

Operational risks - Payment Failure	**Low** risk appetite for the **failure of DSP payment operations.** The DSP has an extremely low appetite for a loss or delay of payments to customers. The Department has established a comprehensive business continuity programme to support the continuance of operations in the event of external disruptions. This includes comprehensive measures to protect the Department's operations in the event of a cyberattack. Strong working relationships are maintained with financial institutions for payment delays outside the Department's control.
Operational Risks – Technological Innovation and Business Modernisation	**Medium** risk appetite for risks associated with technological innovation. As technology continues to move forward at an enormous speed, the Department needs to be ready to avail of potential new technologies and developments where possible. The Department has a moderate risk appetite for technological innovation to embrace 'digital by desire' service for customers, and ultimately, support the delivery of robust public services.
Operational risks – Data Protection	**Low** risk appetite for Data Protection breaches. The Department's operations require the use of significant personal and sensitive information. In addition, the Department has overall responsibility for the Public Service

	Identity dataset, including the Personal Public Service Number (PPSN). The Department has a very low tolerance for data protection risks and has extensive control measures in place to protect against data breaches due to internal errors, or external actors.
Operational risks – Customer and Staff Safety	**Low** risk appetite for risks to customer and staff safety. The DSP has a very low appetite for risk to the safety of our staff and customers.
Reputation and compliance risks	**Low** risk appetite for reputational and compliance risks. The Department will avoid any situation or any action originating in the DSP, which results in a negative impact on our reputation for integrity. The Department has a strong customer focus and expects full adherence to the Civil Service Code of Standards, the Corporate Governance Framework, and best practice generally regarding corporate governance.
Crisis Response	**High** risk appetite during crisis response. The Department recognises the critical role it plays in delivering the right income supports to the right people at the right time. Hence, in the event of a national crisis, the Department will adopt a strong risk appetite to maintain and deliver necessary services.

8. Risk Scoring

To assess the relative seriousness of the risks all risks are scored in terms of the expected impact, likelihood and quality of controls.

A five-point scoring is used for impact and likelihood while a three-point system is used for scoring of controls. A description of each score is described in the Table 2.

Impact	Likelihood	Control Effectiveness
1 = No significant impact	1 = Rarely, if ever	1 = Controls highly effective
2 = Minor impact	2 = Possible	2 = Controls could be improved
3 = Significant but containable impact	3 = Likely	3 = No controls/controls are ineffective
4 = High Impact	4 = Very likely	
5 = Extremely detrimental	5 = Almost unavoidable/ already occurring	

Table 2: Scoring for Impact, Likelihood and Controls

For each a risk score by is calculated by multiplying the rating for the impact, likelihood and control. The risk score is then converted to a Red/Amber/Green risk indicator system for monitoring and reporting as illustrated in Figure 3.

		No significant impact	Minor impact	Significant but containable impact	High Impact	Extremely detrimental
	Rating	**1**	**2**	**3**	**4**	**5**
Almost unavoidable	**5**	L	M	H	H	H
Very likely	**4**	L	M	M	H	H
Likely	**3**	L	L	M	M	H
Possible	**2**	L	L	L	M	M
Rarely, if ever	**1**	L	L	L	L	L

L = Low Risk (0-12)	M = Medium Risk (13-24)	H = High Risk (25+)

Figure 3: Risk Scoring (assuming Controls Score= 2)