An Roinn Leanaí, Comhionannais, Míchumais, Lánpháirtíochta agus Óige
Department of Children, Equality, Disability, Integration and Youth

Risk Management Policy of the Department of Children, Equality, Disability, Integration and Youth[1]

[1] To be read in conjunction with DPENDR's "Risk Management Guidance" (Feb 2016)

Contents

1. Introduction / Risk Policy 3
2. Risk Appetite Statement and Strategy 4
3. DPENDR Guidance 5
4. DCEDIY Risk Management Structures 5
   - **I. Unit and individual staff members** 5
   - **II. Risk Register - eRisk** 6
   - **III. Department's Risk Coordination Team** 6
   - **V. Risk Committee** 6
5. Risk Management Process 7
   - **5.1 Identifying Risk** 7
   - **5.2 Mitigating Risk** 8
   - **5.3 Assessing Risk** 9
   - **5.4 Additional Mitigations** 10
   - **5.5 Reviewing / Reporting of Risk** 10
6. Risk Incidents/Events 11

APPENDIX A – Assurance Framework 12

APPENDIX B – Risk Incident Report Template 13

1. Introduction / Risk Policy

Risk is a possible event or development that has the potential to interfere with the Department's ability to achieve its objectives. Having an effective Risk Management Framework and process in place allows for a better understanding of risk and should lead to better informed decision making.

The DCEDIY Risk Management Policy sets out how the Department is to identify, mitigate, assess, review and report on risks. The Policy is integrated with the Department's Statement of Strategy and its Annual Business Planning and Performance Management and Development System processes.

Risk Management is not a stand-alone activity. It is part of our normal day-to-day work. The following table should guide staff through the Risk Management process:

Identifying Risk Have you identified some factor/circumstance/development that could impact on the day to day business of your Unit, and/or on the Department as a corporate entity?
Mitigating Risk With the risk identified, the next logical step is for your Unit to consider and determine what measures currently exist to mitigate against that risk.
Assessing Risk When you have determined and agreed what mitigation measures are in place, you need to assess the likelihood and impact of the risk, should it occur with the existing mitigations in place. You must score this ' residual risk '.
Additional Mitigations You have scored the residual risk. Consider now what other actions could be put in place to further reduce the risk - these must be attainable and actionable and you should have a clear plan in place to action them.
Reviewing and Reporting of Risk You must have in place a standardised process to review risks, to interrogate the mitigations in place and to put identified additional mitigations into place. Monthly Unit meetings are one such example. You must ensure that any risk changes are reported within the Unit; captured on eRisk (and notified to the Risk Management Coordination team in DCEDIY. In the case of Corporate Risks, the Management Board in its role as the Risk Committee, review the Corporate Risks on a quarterly basis.

This Policy document outlines the manner in which Risk Management operates in DCEDIY.

2. Risk Appetite Statement and Strategy

The Department's Risk Management Committee actively monitors all corporate and high level risks. It also has in place a range of measures designed to reduce the likelihood of each risk occurring and its impact in the event that the risk materialises. It accepts that the likelihood of something occurring can be affected by factors within or outside its control.

The purpose of this Risk Appetite Statement is to set out the level and type of risk that the Department is willing to take in delivering on its responsibilities and strategic objectives. Risk Appetite is the amount of risk, at a broad level, that an organization is willing to accept. It reflects the risk management philosophy that the Management Board wants the organisation to adopt and, in turn, influences its risk culture, operating style and decision-making.

As a Department we acknowledge that there will always be a level of risk inherent in what we do. The nature of risk can be strategic, operational, reputational, financial or related to compliance.

Our approach is to minimise the exposure to strategic, operational, reputational, compliance and financial risk, whilst accepting and encouraging an acceptable level of risk in pursuit of our mission and objectives. The Department's acceptance of risk is subject always to ensuring that potential advantages and disadvantages are fully understood before developments are authorised, and that sensible measures to mitigate risk are established.

The Department is prepared to take controlled risks to capitalise on new opportunities so that it can meet its responsibilities and find innovative ways of furthering its objectives. It recognises that its appetite for risk varies according to the activity undertaken across the Department's broad range of functions.

It will have no tolerance for risks that (I) affect the protection, safety and welfare of children (ii) impact on the application of sound financial controls or (iii) compromise the delivery of legislative or regulatory requirements. It has a high risk appetite for areas of our work involving (i) the development and implementation of new services and (ii) the management of emergency or crisis events.

The following table presents the framework of Risk Appetite under which this response is controlled.

Framework of Risk Appetite

Low Risk Appetite	Avoidance of risk and uncertainty is a key organisational objective.
Moderate/Low Risk Appetite	Preference is for ultra-safe business delivery options that have a low degree of inherent risk and may only have a potential for limited reward.
Moderate Risk Appetite	Preference for reasonably safe delivery options that have a low degree of residual risk and may only have limited potential for reward.
High Risk Appetite	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.).
Very High Risk Appetite	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

This Risk Appetite Statement was agreed by the Risk Committee of the Department on 19 March, 2024 and will fall for review in 12 months' time.

DCEDIY's Risk Strategy is to have proactive management-led behaviours and processes that help it to achieve its strategic and operational objectives. The DCEDIY Governance Framework outlines the overall approach to Risk Management as part of the system of internal controls and business management. ***Appendix A*** shows Risk Management as part of the wider system of Audit, Assurance and Compliance Arrangements in a Government Department.

3. DPENDR Guidance

Risk Management in DCEDIY has due regard to the Department of Public Expenditure NDP Delivery and Reform's document - *Risk Management Guidance for Government Departments and Offices (2016).* DPENDR's guidance aims to provide Departments with good practice, to support them with embedding risk management within the culture of the organisation and to reaffirm the benefits from effective risk management including accountability, assurance and enhanced decision-making. It identifies four Risk Management principles - *Governance, Structures, Management and Reporting* - and DCEDIY works within these principles.

DPENDR Guidance specifies that:-

- *Each Department should have clearly defined Risk Management structures and responsibilities, and*
- *The Risk Management process should be kept as simple and straightforward as possible and existing structures should be used as far as possible*

4. DCEDIY Risk Management Structures

Risk Management in the Department is structured as follows:-

I. Unit and individual staff members

While the Secretary General in his role as Accounting Officer of the Department has ultimate responsibility for risk management, most risks will be managed and reviewed at Unit level with individual staff members and Heads of Unit. Each Management Board member is responsible for risks in their area.

Each Unit, led by a Principal Officer or equivalent, should own the Risk Management process for its area. POs are the risk owners for the risks in their own business Units. The Business Plan, Risk Assessments and Goal Setting in each Unit are integrated and mutually supporting and reinforcing. The business objectives for which each Unit is responsible, should inform the Annual Business Plans. All Business Plan actions should be risk assessed and where associated risk(s) are identified, they should be captured on eRisk. Each risk will have an assigned owner on eRisk.

The contribution of staff to the delivery/management of Unit business actions and associated risks should be incorporated in to the PMDS annual Goal Setting exercise. Individual staff members, Heads of Unit and each Management Board member will be responsible for the ongoing management of risks within their area. The Risk Committee or the Internal Audit Unit may from time to time sample a selection of risks to confirm the processes in place for management and review.

II. Risk Register - eRisk

The Department maintains a centralised register of its risks, entitled eRisk. The Register is a primary tool for risk tracking. It contains the most up to date risk data for the Department including amongst others the risk status, its score, its associated mitigations as well as identifying the owner of the risk.

- The relevant Head of Unit must approve all risks which come under their remit;
- The relevant Management Board member must approve high-level risks, which come under their remit. These must be submitted to the Management Board member by the Head of Unit.

The Department will also maintain a corporate risk register, which will contain the principal corporate risks, which the Department faces.

III. Department's Risk Coordination Team

The Risk Coordination team is the Department's central contact point for all Units on matters relating to risk. The team monitors the Department's Risk Register on eRisk, ensuring a consistent approach is adopted across the Department in line with this policy and actively engages with Units on any issues identified. The team also supports the Department's Risk Committee in a secretariat role.

IV. Unit Risk Coordinators

Unit Risk coordinators, should assist the Unit PO in their role as champion of risk management for their Unit. They have an important role in helping keep the risk management process live, dynamic and effective for their Unit on an ongoing basis. In doing so, they should ensure that risk is a standing agenda item at their Unit's team meeting and that an active discussion around risk takes place at each meeting and that each meeting is also minuted.

As well as being the central contact person for both the Unit head and the Department's Risk Coordination team, regarding both the risk management process and eRisk for their Unit, Risk Coordinators are also responsible for monitoring and overseeing eRisk for their Unit. They should be included in any notifications of new, closed or updated risks, which have been identified by members of their Unit, and captured on the eRisk system.

V. Risk Committee

In DCEDIY, the Management Board also sits as the Department's Risk Committee. The Secretary General, as Accounting Officer, has ultimate responsibility for Risk Management as part of the system of internal controls. The Risk Committee meets quarterly (or as required) for the purpose of:-

a. Overseeing the system of Risk Management in the Department, and embedding Risk Management effectively;
b. Considering Corporate Risks and reviewing their ongoing management;
c. Reviewing reports detailing high scoring risks across MB areas, and considering whether mitigation and management measures are appropriate and adequate;
d. Considering whether a high scoring risk needs to be reflected in the Corporate Risks.

Dates for Risk Committee meetings are set at the beginning of each year, and as far as possible are scheduled to precede the pre-arranged meetings of the Audit Committee. This ensures that when the Audit Committee considers risk, it has the latest information at its disposal.

VI. Management Board

The Management Board meets on a bi-monthly basis. Many of the updates brought to a meeting by Management Board members have constituent Unit or Corporate Risk elements, which are discussed. Management Board members consider whether changes to the Risk Register are warranted as a result. All such changes should be notified to the relevant Unit Risk Coordinator who will update the eRisk system for their Unit. The Management Board may also finalise Corporate Risks considered at the previous Risk Committee meeting.

VII. Internal Audit

Internal Audit is responsible for providing an independent assurance opinion to the Accounting Officer and the Audit Committee on the Risk Management framework, policy and processes. Internal Audit should review Risk Management to ensure that it is fit for purpose.

VIII. The Audit Committee

The Audit Committee has an independent role in providing advice and guidance to the Accounting Officer regarding the systems of Risk Management and Internal Control, as set out in the Audit Committee Charter. It should have a standing item on risk at its meetings.

The Committee reviews the Corporate Risk register periodically at its meetings and makes suggestions from time to time on the risks. These suggestions are conveyed to the Risk Committee via the DCEDIY Risk Coordination team, members of which may attend an Audit Committee meeting by invitation and act as a conduit between the Risk Committee and Audit Committee on risks and the risk management process.

5. Risk Management Process

There are four key areas of risk management - identifying, mitigating, assessing and reviewing/reporting- as follows:

5.1 Identifying Risk

Risk is a possible event or development that has the potential to interfere with an organisation's ability to achieve its objectives. It is integral to many activities and monitoring and management of risk is a continuous process.

- **Corporate Risks**
  The corporate risks are risks, which have an impact on the Department as a corporate entity. These are defined and managed by the Risk Committee, and recorded on a distinct Corporate Risk sheet, which forms part of the Risk Register.

- **Unit-level Risks**
  Unit level risks are risks, which could undermine key aspects of the Department's performance. The Annual Business Planning process provides a mechanism to identify core Unit objectives. All objectives should be risk assessed and those considered to have associated risks should be recorded on eRisk. Unit risks should be reviewed regularly and updated or closed as required. The monthly unit team meeting, which should have risk as a standing agenda item provides an opportunity for such reviews to take place. All updates should be minuted and eRisk updated as necessary.

  Risks which derive from a possibility that staff members will not effectively discharge their normal duties should not be included, except insofar as there may be a risk that can be mitigated - e.g. by training, mentoring, support and supervision, procedures or policies.

The following are 'Descriptions of Risk Types', and are used to indicate the nature of the impact of particular risks:-

- **Strategic:-** Risks deriving from factors outside of the Department, such as the economic climate, interest rates, exchange rates, and inflation,

- **Operational: -** Risks which relate to or derive from the Department's activities or discharging of its functions, from its procedures or technologies.

- **Financial: -** Risks which could give rise to a financial loss or exposure.

- **Reputational: -** Risks to the public reputation of the Department.

- **Legal and Regulatory:-** Risks arising from failure to comply with laws and regulations, damages or compensation claims, judicial review, drafting of legislation which gives rise to unintended outcomes, or failure to legislate.

Some risks may have more than one risk type (e.g. they could have a 'Financial' and 'Reputational' impact). In such cases the principal risk type - having the perceived higher risk impact - should be recorded in eRisk. Where it is not possible to determine the principal risk type for a risk there is an option available on eRisk to select more than one risk type.

Risks versus issues

It is important to highlight the difference between risks and issues to avoid a situation where the risk register contains issues as well as risks. The table below outlines the main differences between the two:

Issues	Risks
Focused on the present	Future focused
Always negative	Can be positive or negative
Should be recorded in an "issues" register	Should be recorded in a "risk" register
An issue is dealt with through a "work-around"	A risk is managed where possible through the implementation of mitigations

New Business Activities

Particular attention should be paid to new policy and business activities, which can arise at any time, be political or strategic in nature, and which may have specific time-bound implications. It is incumbent upon management/staff to risk assess new policies/activities. They should also re-evaluate the risk attaching to other Unit business items to see how they are impacted upon in the light of the new additions and the priority that may attach to same.

5.2 Mitigating Risk

Mitigation measures are controls currently in place to ensure that the Unit can achieve its business objectives without running the risk of interruptions to those objectives. It should be clear to staff of the Unit that these controls are known, assigned and implemented.

Mitigations can include legislation, regulation, resource allocation, ICT solutions, management focus, Ministerial prioritisation, financial policies and procedures, documented processes, external (expert) assistance and periodic review. Business Continuity management is an essential element towards mitigating the effects of risks on key Departmental activities.

Mitigation tasks involve staff at all levels across the Department. It is important that Units include in their Business Plans the various arrangements in place to ensure that business runs smoothly, commitments are met and objectives are achieved. Individuals should be able to see the link from the Business Plan to their PMDS Goal Setting.

5.3 Assessing Risk

The degree of risk should be determined by factoring ' Likelihood ' and 'Consequence/Impact' criteria. The following table sets out a simple scoring system to be used:-

Likelihood	**Almost unavoidable/Already Occurring**	**Very Likely**	**Likely**	**Possible**	**Rare**
Score	5	4	3	2	1
Consequence / Impact	**Substantial**	**Significant**	**Moderate**	**Minor**	**Negligible**
Score	5	4	3	2	1

The impact on the Department if the risk actually happens is estimated using a scale of 1 to 5, where 1 is equivalent to having "no significant impact" and 5 is equivalent to having an "extremely detrimental impact".

In order to provide assistance to staff in the scoring of risks, the Corporate Governance Unit has included the following examples of risks that would most likely have a consequence/impact of 5[2]:

- The risk of a cyber-attack compromising the Department's operating systems;
- The risk of the Department failing to achieve one of its strategic objectives as set out in its Statement of Strategy;
- The risk of the Department failing to advance or implement one or more of its key policies or legislative initiatives, including those commitments contained in the Programme of Government;
- The risk of the Department failing to provide or enable the provision of one or more of its core services to its customers.

Scores for the criteria are multiplied together to give an overall risk score for each risk. For example, *a risk with substantial consequence (5), and an almost unavoidable likelihood (5), would score 25 (5 x5).*

The risk likelihood and consequence are scored <u>after</u> the effectiveness of existing mitigation/control measures is considered. This approach will result in all risks being rated on the basis of ***residual risk,*** since the effectiveness of existing mitigation measures are factored into the assessment.

[2] The examples provided are illustrative and not exhaustive.

5.4 Additional Mitigations

The Risk Register provides for the consideration of ***Additional Mitigations,*** which are actions not in place but which constitute viable options to reduce the likelihood or impact of a risk. These mitigations should be part of an ongoing strategy to further allay the risk and should be realistic, manageable and achievable. These should be identified in the Business Planning and PMDS Goal Setting processes.

5.5 Reviewing / Reporting of Risk

(i) Unit Risks

Ownership of Unit risks is at Unit level. Risk should be an agenda item at least once a month at regular meetings between Management Board Members and their PO teams, and at monthly team meetings conducted by POs for their Units. Changes resulting from review of risks require approval of the relevant Head of Unit. This could include, for example, movement between the 'Additional Mitigations' and ' Mitigations' columns. Over time, the aim is to implement identified 'Additional Mitigations' and move them to the ' Mitigations' column.

Each Head of Unit is also responsible for approving the inclusion on the Risk Register of relevant risks for their areas. Where additional risks arise or where risk circumstances change, these should be communicated to the Risk Coordination team by the Unit using eRisk. The Risk Coordination team is responsible for the preparation of reports for the Risk Committee's quarterly meetings.

A report on high-scoring risks, is supplied to the Risk Committee, which includes:

- All risks rated as having a score of 15 and above.

The Risk Committee will decide on the cut-off point in terms of residual risk above which these risks will continue to be considered by the Committee. It is important to note that all risks continue to be managed at Unit level. Given that the scoring of risks and the development of new risks may change over time and according to circumstance, risks may move in and out of the high-scoring risks report.

(ii) Corporate Risks

Ownership of Corporate Risks is at Management Board level. Risk Committee meetings ensure that Corporate Risks are regularly monitored and mitigation measures agreed. Any revisions to the Corporate Risks arising from a Risk Committee decision may be finalised in a written procedure post-meeting.

While the Department's Corporate Risks are determined by the Risk Committee and constitute high-level risks affecting the organisation as a corporate entity, it is important that all staff are familiar with these risks, as there may be some instances where the materialisation of, or the elevation of the status of a Unit-level risk could have a DCEDIY corporate implication. Management Board members need to be mindful of this whenever formal or informal discussions on risks take place. The relevant Management Board member will need to consider whether the matter needs to be raised at the next Management Board meeting.

6. Risk Incidents/Events

Risk incidents may include the materialisation of a risk, or a "near miss".

Most incidents can be, and are managed at Unit level. Some will require to be escalated to the Management Board member to be addressed at Divisional level. It is a matter for the Management Board member to decide if a particular incident should be escalated to the Management Board.

Where it is deemed at any stage that a Unit-level or a Corporate Risk needs to be brought to the attention of the Management Board, the matter should be reported by the responsible Management Board member at the next available Management Board meeting. The Management Board may direct any necessary corrective action.

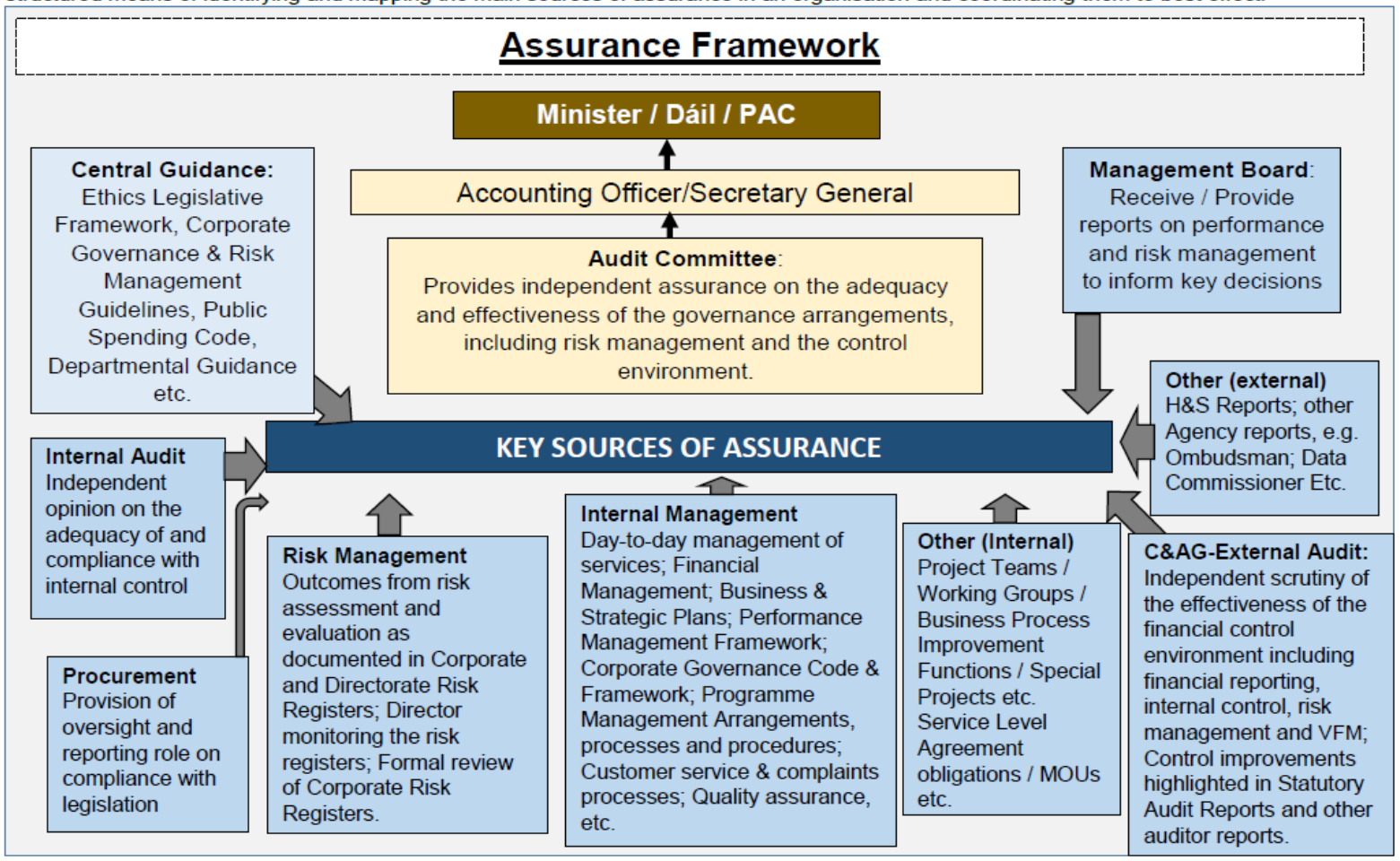
In all cases of a materialised risk, regardless of the level of escalation, the Principal Officer of the Unit will be required to complete an Incident Report ***(Appendix B)*** and send it to the Risk Coordination team.

The Risk Coordination team will compile an update for the Risk Committee on all Incident Reports completed in the period between Risk Committee meetings. The Audit Committee will also be informed of any incidents by the Risk Coordination team.

APPENDIX A – Assurance Framework

Audit, Assurance & Compliance Arrangements

In mapping audit and assurance arrangements, Departments may have regard to the following Assurance Framework which provides a structured means of identifying and mapping the main sources of assurance in an organisation and coordinating them to best effect.



APPENDIX B – Risk Incident Report Template

TO BE COMPLETED BY UNIT PRINCIPAL OFFICER

This form is to be completed following the materialisation of a unit-level risk as outlined in Section 6 of the DCEDIY Risk Management Policy (19 March 2024).

Description of materialised risk: *Insert description here*

QUESTION	**Y/N**	EXPLANATION
Has the incident been escalated to (i) PO level? (ii) Head of Division? (iii) Management Board?		
Has the cause been identified?		
Has corrective action been taken?		
Has the risk on eRisk been reviewed/ revised?		
Has the risk been updated on the eRisk system?		
Has the matter been discussed at your Unit meeting?		
Has the incident required a change to the Unit Business Plan and/or staff Goal Setting/PMDS?		

Signed:

Unit:

Date: