



**Seirbhís Thithe  
an Oireachtais  
Houses of the  
Oireachtas Service**

# RISK MANAGEMENT POLICY

December 2015

## Risk Management Policy

# Risk Management Policy

## Index

1.	OVERALL GOAL OF THE POLICY .....	4
2.	SPECIFIC RISK MANAGEMENT OBJECTIVES .....	4
3.	RISK AWARE CULTURE .....	4
4.	RISK MANAGEMENT ARCHITECTURE/ORGANISATION .....	6
5.	RISK MANAGEMENT ORGANISATION CHART .....	7
6.	ROLES AND RESPONSIBILITIES .....	8
7.	RISK PROTOCOLS .....	8
8.	RISK APPETITE/TOLERANCE .....	10
APPENDIX 1 – ROLES AND RESPONSIBILITIES .....		11

## Risk Management Policy

### 1. Overall Goal of the Policy

The overall goal of the Houses of the Oireachtas Service risk management policy is to ensure that

- all risk management activities contribute to the achievement of the Service's objectives.

and that the risk policy

- is aligned with the Service's business continuity plan
- articulates our approach and expectations in relation to the management of risk across the Service.

The Service encourages the taking of controlled risks, capitalising on new opportunities and using innovative approaches to further the interest of the Service and achieve the business objectives provided the resultant exposures do not infringe on the operating procedures or legal and regulatory requirements of the Service.

The best practice standard adopted is "ISO 31000:2009, Risk Management – Principles and Guidelines".

A risk is identified as anything which prevents the achievement of a section's objectives and results in actual quantifiable loss to the Service. The loss may be of a strategic, operational or reputational nature.

### 2. Specific Risk Management Objectives

The specific objectives of the risk management policy are:

- To create and protect value – in other words, to ensure that risk management contributes to the demonstrable achievement of objectives;
- To develop risk management strategies and risk management plans;
- To identify and prioritise potential risk events;
- To use established risk management methods, tools and techniques to assist in the analysis and reporting of identified risk events;
- To identify and evaluate risks;
- To achieve, measure and report results;
- To be dynamic, iterative and responsive to change;
- To integrate business continuity management within risk management; and
- To embed a risk management culture within the Service.

### 3. Risk Aware Culture

Embedding risk management involves -

- creating an environment that can demonstrate leadership from senior management,
- involvement of staff at all levels,
- a culture of learning from experience,
- appropriate accountability for actions (without developing an automatic blame culture), and
- good communication on risk issues.

## Risk Management Policy

The risk management process is managed from the top down but with an increased involvement from all staff. The Service maintains a single register but risk is managed at section level where possible and escalated as appropriate so that concentration at senior management and MAC is on the strategic and key operational levels.

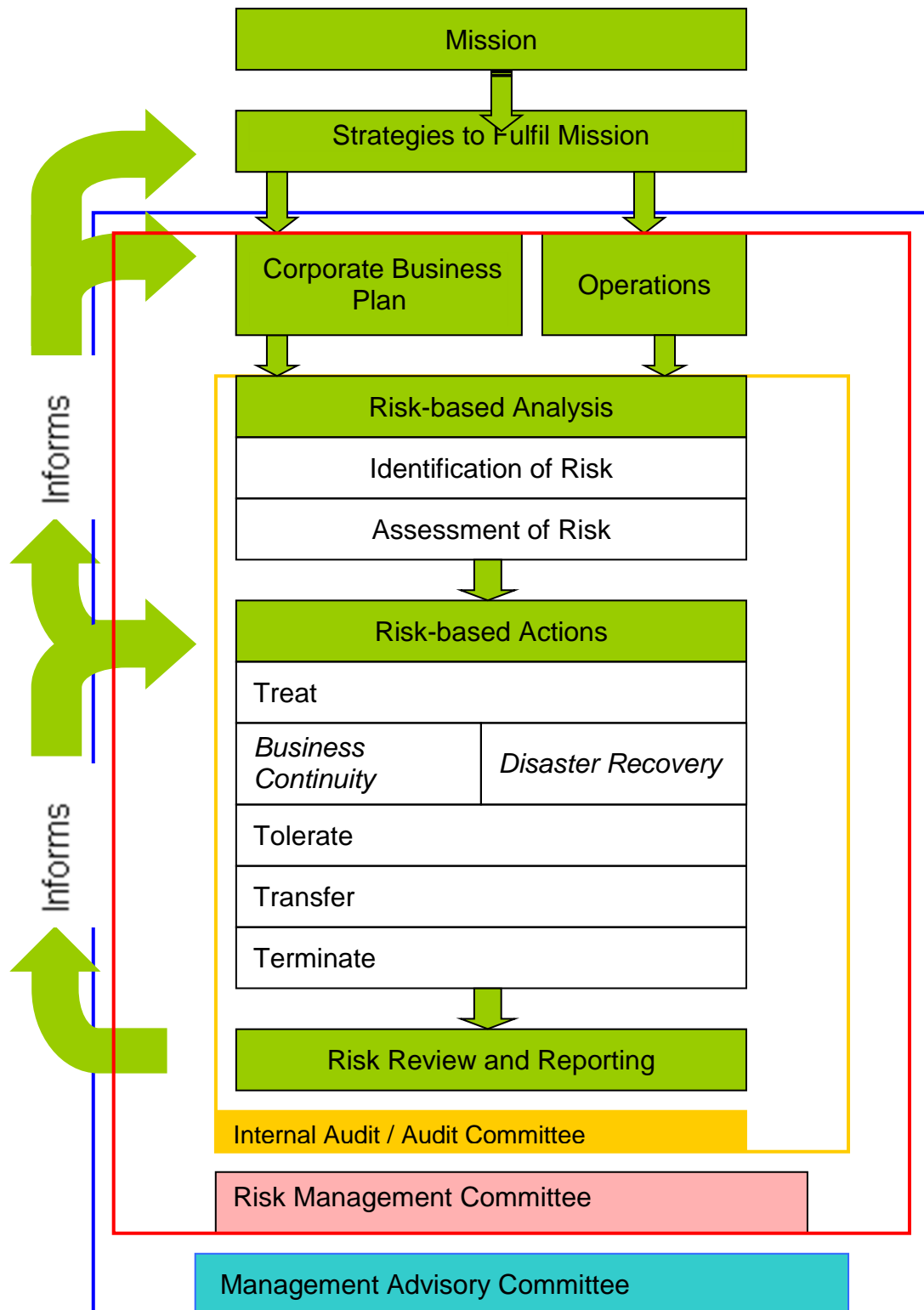
Monitoring activities provide assurance that there are appropriate controls in place and that the procedures are understood and followed.

### **How is this done in the Oireachtas?**

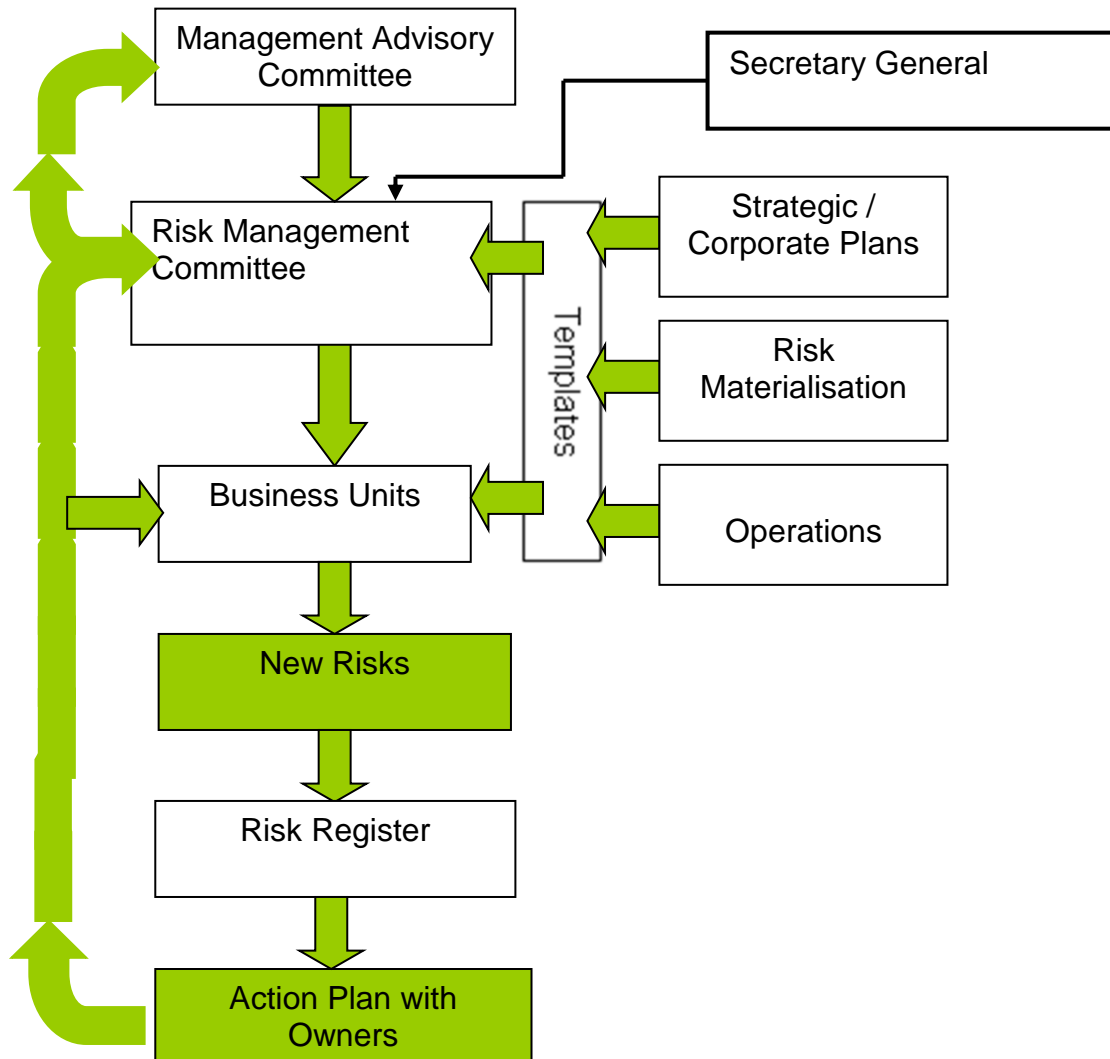
- The approach is to be management led and top down.
- All operations, strategic and business plans should be risk assessed against a set of templates in order to ensure that all foreseeable risks are identified and considered.
- Section heads and risk co-ordinators within sections have responsibility for identifying risks in their own areas, with the help of a customised template they should only escalate risks where the seriousness of the risk occurring requires that.
- Senior Managers have responsibility to bring forward strategies to mitigate serious risks to the Service.
- The entire risk management process is monitored and controlled by the Risk Management Committee which ensures that all required activities are being carried out on time and effectively. This involves reporting on a monthly basis to the Management Advisory Committees, with the risk report including details of all materialised risks, near misses and emerging risks.
- Risk assurance continues to be provided through the Audit Committee.
- A full annual risk register review by each Section. Target to reduce risks by analysing action plans for residual risk. Removing any steady state processes, i.e., terminating risks that are managed day to day. These terminated risks are retained in the Risk Database in case they need to be reactivated at a later date. Completion of the risk review should be reported on by Senior Managers to Assistant Secretaries and MAC under the standing risk item on the MAC agenda.

#### 4. Risk Management Architecture/Organisation

The following chart demonstrates the Risk Management process that is be in place:



## 5. Risk Management Organisation Chart



## 6. Roles and Responsibilities

The Risk Management Committee is primary champion of risk management at strategic and operational level in the organisation and is responsible for developing and maintaining the policy and strategic approach to risk in the Service. The Risk administrator is a member of the Risk Management Committee and has responsibility for managing the risk policy and coordinates all risk activities within the Service. The Internal Auditor attends the Risk Management Committee in an advisory capacity only.

The Management Advisory Committee (MAC) approves the policy and strategy for risk management and the Risk Management Committee reports to the MAC on a monthly basis.

The Audit Committee has an important role to play in reviewing management and the Internal Auditor's reports on the effectiveness of the risk management systems in the Oireachtas. Risk is a standing item on the agenda of the Audit Committee and the Risk Management Committee must report quarterly.

Each individual in the organisation has a role to play in implementing and enforcing effective risk management systems in their day to day activities. All roles and responsibilities are outlined in detail in Appendix 1.

## 7. Risk Protocols

### 7.1 Risk Identification

All new projects are risk assessed and activities to mitigate any resulting risks to be put in place to be detailed as part of the project management process.

### 7.2 Risk Classification

Risks are classified in the following ways:

1. *Strategic*: Failure to achieve the strategic and business objectives of the organisation.
2. *Environmental*: The risk that human health or the environment could suffer harm as the result of the presence of environmental hazards.
3. *Operational*: Risks that could lead to losses resulting from inadequate or failed internal processes, people and systems or from external events.
4. *Financial*: Risks that could result in a failure to maintain effective financial management and accountability arrangements in all the Houses activities.
5. *Reputational*: Risks that could impact negatively upon the confidence and trust which stakeholders have in the Houses of the Oireachtas.
6. *Procedural – Core Business*: The risk that procedural mistakes, omissions and errors could cause serious impact on the smooth running of the Houses of the Oireachtas.

## Risk Management Policy

7. *Security*: The risk of an event or person(s) being a threat to the secure operation of the Houses of the Oireachtas.

8. *Legislative*: The effects of new legislation, compliance with existing legislation.

9. *Emerging*: This is a risk which has escalated in likelihood or impact or a new risk likely to have serious and imminent impact on the running of the Houses of the Oireachtas.

### 7.3 Risk Estimation

A five tier system is used to rate risks. The five tiers are high, medium high, medium, medium low and low.

### 7.4 Risk Treatment

The risk treatment plan is the immediate output of the risk assessment. It defines how, based on the criteria established by senior management, each risk is to be handled. The options are to:

- 1) Knowingly accept the risk as it falls within the Service's "risk appetite"; in other words, management deems the risk acceptable, compared to the cost of improving controls to mitigate it. **(Tolerate)**
- 2) Implement a suitable control or combination of controls to reduce (mitigate) the risk to a more acceptable level. **(Treat)**
- 3) Avoid the risk i.e. do not undertake the associated business activity. **(Terminate)**
- 4) Transfer the risk to another organisation (e.g. through insurance or by contractual arrangements with a business partner). **(Transfer)**

## 8. Risk Appetite/Tolerance

**8.1.** Risk Appetite refers to the amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time.

The organisation must accept a certain element of risk across all its activities. As a public sector organisation, the Service will seek to mitigate risk as far as possible.

The Service encourages the taking of controlled risks, capitalising on new opportunities and using innovative approaches to further the interest of the Service and achieve the business objectives provided the resultant exposures do not infringe on the operating procedures or legal and regulatory requirements of the Service.

	Assessment	Risk Appetite Guiding Statement
Strategic Environmental Operational / Procedural Financial Reputational Emerging	Low Risk Appetite	The risk appetite in relation to risks in these categories is generally low. However in circumstances where the need for a progressive change or advancement is deemed appropriate the Service will avail of such opportunities.
Security Compliance	Zero Risk Appetite	The Service will endeavour to achieve full compliance, and will avoid any risk or uncertainty in this area.

## 8.2 Acceptable Risks

Management should be willing and able to take calculated risks to achieve the Service's business objectives. The associated controls, proposed actions and decisions should be properly identified, evaluated and managed to ensure that the exposures are acceptable.

Within the Service, particular care is needed in taking any action which could:

- Impact on Service Delivery
- Result in financial loss
- Result in censure / fine by legal or regulatory bodies
- Impact on reputation
- Impact on performance
- Undermine the independent and objective review of activities.

Any threat or opportunity which has a sizeable impact on any of the above should be examined, its exposure defined and it should be discussed with the appropriate line manager. Where there is a significant potential impact and high likelihood of occurrence, it should be referred to the Assistant Secretaries/ MAC as a possible strategic risk.

## **Appendix 1 – Roles and Responsibilities**

The Risk Management Committee is primary champion of risk management at strategic and operational level and is responsible for -

- recommending policy and strategy for risk management
- building a risk aware culture within the organisation including appropriate education
- establishing internal risk policy and structures for business units
- designing and reviewing processes for risk management
- co-ordinating the various functional activities which advise on risk management issues within the organisation
- developing risk response processes, including contingency and business continuity programmes
- preparing reports on risk management progress for the MAC
- facilitating risk identification/assessment and educating line staff in risk management and internal control.
- Preparing an overarching BCM strategy for the Service and co-ordinating the development of contingency and BCMs for the entire Service

The MAC –

- approves policy and strategy for risk management
- reviews performance for the risk management system
- approves the costs and benefits of the risk and control activity undertaken
- approves the effectiveness of the risk management process
- considers the risk implications of Commission decisions
- identifies strategic risks
- has risk as a standing item on its agenda
- reviews risk materialisations where relevant
- receives reports from the Risk Management Committee as appropriate.

The Risk Administrator has responsibility for -

- managing the risk management policy and keeping it up to date
- documenting the internal risk policies and structures
- co-ordinating the risk management activities, compiling risk information and preparing reports for the Risk Management Committee and other management as appropriate
- reporting on risk management performance annually to the Risk Management Committee and other management as appropriate
- reporting on risk management performance monthly to MAC
- keeping up to date with best risk management practice

Audit Committee

- Review management and the Internal Auditor's reports on the effectiveness of the risk management systems
- Review the statement in the organisation's annual report and accounts on internal controls and risk management framework.
- Assess the scope and effectiveness of the systems established by management to identify, assess, manage and monitor financial and non-financial risks and advise the Accounting Officer accordingly, and provide assurances that the risks management strategy is working within the organisation.

## Risk Management Policy

Senior Managers have overall responsibility for –

- the risk management process for each of their sections
- identifying strategic risks for consideration at MAC
- completing a full annual risk register review by each Section. Target to reduce risks by analysing action plans for residual risk. Removing any steady state processes, i.e. removing risks that are managed day to day.
- appointing risk coordinators
- reporting to Assistant Secretaries and MAC on risk issues within their areas
- embedding risk awareness within their areas.

### Sections

The section head is responsible for:

- managing risk on a day-to-day basis
- embedding risk awareness within their operations and introducing risk management objectives into their business
- building a risk aware culture within the Section
- ensuring risk management is a regular management-meeting item to allow consideration of exposures and to reprioritise work in the light of effective risk analysis
- ensuring that risk management is incorporated at the conceptual stage of projects as well as throughout a project.

The Risk Coordinator, who is appointed by the Section head is responsible for:

- maintaining the sectional risk management registers
- identifying and reporting changed circumstances/risks.

All other individuals in a section should: -

- understand, accept and implement Risk Management processes
- report inefficient, unnecessary or unworkable controls
- report loss events and near miss incidents
- co-operate with management on incident investigations
- embed risk culture in the organisation.

### Internal Audit -

- advises on the appropriateness, efficiency and effectiveness of the Service's procedures relating to risk management
- operates an internal audit programme in line with the Institute of Internal Auditors ( IIA) Internal Audit Standards
- audits the risk processes across the organisation
- receives and provides assurance on the management of risk.