RISK MANAGEMENT GUIDANCE

for Government Departments and Offices

An Roinn Caiteachais Phoiblí
agus Athchóirithe
Department of Public
Expenditure and Reform

February 2016

Preface

Good governance in Government Departments and Offices is about delivering priorities, achieving objectives, behaving with integrity and acting in the public interest, and in ways that are consistent with legal, regulatory and Government policy obligations.

Effective risk management supports good governance as it assists in determining priorities and setting objectives, in analysing uncertainties within decision-making arrangements, in clarifying accountabilities and in demonstrating how the public interest is best served.

Risk Management Guidance for Government Departments and Offices (2004) was published by the Department of Finance on foot of a recommendation in the *Report of the Working Group on the Accountability of Secretaries General and Accounting Officers* (2002) to introduce formal risk management in Government Departments and Offices. *A summary of the 2004 Department of Finance Guidelines is provided at Appendix 1.*

Risk Management Guidance for Government Departments and Offices (2016) is a further development to enhance governance arrangements across Government Departments and Offices. This document complements the recently published *Corporate Governance Standard for the Civil Service (2015)* and supports the development of governance frameworks in Government Departments and Offices. The guidelines take account of developments in risk management including the International Standards Organisation (ISO) 31000, *Risk Management – Principles and Guidelines.*

Scope

The scope of this guidance is Government Departments and Offices (Departments and Central Government Offices in the Civil Service[1], hereafter referred to as Department(s)).

This document is intended to be a living document which will evolve in line with best practice. For the most recent version please check the website http://govacc.per.gov.ie.

Government Accounting Unit
Department of Public Expenditure and Reform
February 2016

[1] The Civil Service comprises all Departments as defined by the Public Service Management Act 1997, all Offices or branches of the Public Service specified in Part I or in Part II of the Schedule to that Act and 'Vote Holding' bodies under the aegis of those Departments and Offices.

Risk Management Guidance

Table of Contents Page

Appendices Page

Purposes and Principles

Purpose of this guidance

An integrated and holistic approach to risk management is one of the keystones to achieving effective corporate governance. Departments must be able to respond appropriately to significant business, strategic, operational, finance, compliance and other risks that threaten the successful achievement of their strategic and operational objectives.

Organisations face internal and external factors and influences that make it uncertain whether and when the extent to which they will achieve or exceed their objectives. The effect that this uncertainty has on the organisations objectives is “risk”.

Uncertainty can be as a consequence of cultural and behavioural factors, variability and changes over time within the operating environment, revisions of mandates and obligations, differing expectations within and across stakeholder groups as well as inaccurate or incomplete information.

As there is almost always some uncertainty associated with decisions and decision-making, there is almost always risk. Those with responsibility for achieving and delivering on objectives, and involved in making or altering decisions need to appreciate that risk is an unavoidable part of organisational activity. Risk associated with decisions should be understood at the time the decision is made. Having an effective risk management framework and process in place allows for better understanding and more informed decision-making.

The purpose of this guidance is to update Departments with current 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.

This document identifies four principles – *Governance, Structures, Management and Reporting* – and the associated guidelines for the operation of risk management as an integral part of the governance and management culture of Departments.

Risk involves uncertainty. It raises issues of *probability* and *potential impact*:

- The *probability* (likelihood) of the occurrence of events, circumstances or developments; and
- The *potential impact* (consequence) of these events, circumstances or developments to interfere in or affect a Department's ability to achieve its goals and objectives.

Risk and uncertainty are part of the internal and external environment in which Departments operate. The risk management framework sets out the overall architecture within the organisation for the management and mitigation of risk. The purpose of the framework is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. A comprehensive risk management process facilitates Departments in achieving their business objectives and positions risk within the overall governance structures of the organisation.

The implementation of risk management within Departments involves strong management commitment. Management should ensure that risk management within their organisation encompasses the principles identified in this document.

The associated guidelines are for guidance purposes and can be adapted to suit the requirements of individual Departments.

This guidance has been developed by Government Accounting Unit, Department of Public Expenditure and Reform. For further information, please contact:

Government Accounting Unit
Department of Public Expenditure and Reform
Upper Merrion Street
D02 R583
Email: govacc@per.gov.ie

4 Risk Management Principles

Governance

Each Department is required to have a pro-active management-led Risk Management Strategy as part of their governance framework.

Structures

Managing risk requires a systematic, timely and structured approach with clearly defined risk management structures, processes and responsibilities.

Management

The risk management framework and process should be appropriate to the scale, nature range of activities and risk appetite of the Department and should be subject to continuous improvement.

Reporting

Departments’ risk management systems should provide for monitoring and reporting at various levels of management.

Risk Management Guidelines

Guideline 1 - Governance

As part of its governance framework, each Department must have a risk management strategy which informs and facilitates risk management as an integral and on-going part of its management process.

1.1 Governance

1.2 Risk Management

1.3 Leadership

1.4 Environmental Factors

1.1 Governance

"Good governance requires that the notion of risk be embedded into an entity's culture, with governing body members, together with managers at all levels, recognising that risk management is integral to all of their activities and must be regarded as a continuous process. It is about being risk aware rather than risk averse."[2]

The Accounting Officer of a Department has ultimate responsibility for risk management. Each Department is required to have a pro-active management-led risk management policy as part of their governance framework.

The Accounting Officer and Heads of Offices should define the Management Boards' role in regard to risk and ensure that there are adequate systems in place for identification and management of risk. The role of the managers and relevant officials with responsibility for policy and financial risk should be clearly defined in each Department's framework of assignments under the Public Service Management Act 1997 and in the Statement of Internal Financial Control.

[2] Taken from the International Framework: Good Governance in the Public Sector (July 2014)

The Management Board should ensure that the risk management policy is an integral part of the business planning, decision making and management process, with appropriate Structures (*Guideline 2*), Management (*Guideline 3*) and Reporting (*Guideline 4*).

The risk management policy should:

- add value to business activity and contribute to the economic, effective and efficient delivery of business objectives, at both strategic and operational level;
- reflect organisational culture and values; and
- take account of the environment, both internal and external, in which the Department operates.

1.2 Risk Management

"Risk management and internal control are important and integral parts of a performance management system and crucial to the achievement of outcomes."[3]

Risk management can be defined as a set of co-ordinated activities to direct and control the management of risk within a Department.

In the context of developing a risk management strategy, risk can be defined as events or actions which affect the Department's ability to meet its business objectives. The ISO defines risk as *"the effect of uncertainty on objectives".*

Whilst Departments have traditionally incorporated risk assessment, implicitly or explicitly, as part of its strategic and operational decision-making process, the development and implementation of the risk management policy commits the organisation to identifying, assessing and mitigating risk and to ensuring the ongoing review and improvement of risk management approaches in a changing operational environment. Typically the risk management strategy sets out the context for risk management within the Department setting, the risk management objectives, the risk management framework and process, roles and responsibilities and assurance arrangements.

[3] Taken from the International Framework: Good Governance in the Public Sector (July 2014)

In summary the risk management strategy helps an organisation achieve its strategic and operational objectives by managing and mitigating the risks which have the potential to affect the achievement of those objectives.

The risk management process should:

- address any uncertainty around the delivery of objectives;
- be based on the best available information;
- facilitate continual improvement;
- be part of decision making;
- be integral to strategic planning;
- be structured, systematic and tailored to organisational needs; and
- be dynamic, transparent and responsive to change.

The objectives of a risk management policy should include:

- how to address certain risks;
- protecting the reputation of the Department;
- improving the overall risk management framework;
- providing a level of assurance that the key legal, regulatory and governance obligations of the Department are being met; and
- ensuring that the Department is meeting the requirements of any control/governance procedures which it has in place.

These objectives can be reprioritised as part of the risk management review process should the risk profile change (for example, as a result of new services). The objectives may also be re-emphasised based on risk assessment results or other considerations.

Potential sources of risk and uncertainty include:

- economic and financial changes;
- business relationships and obligations;
- legal expectations and liabilities;
- technological developments;
- political changes and trends;
- natural events;
- human resource issues;
- leadership and management change; and
- system weaknesses.

1.3 Leadership

The Management Board of a Department provides leadership in promoting risk management, addressing key risks in the context of the Department's Statement of Strategy and determining the Department's risk appetite (deciding what risks the Department is prepared to accept or retain in the pursuit of its core priority objectives).

The focus of the Management Board should be on key business risks/principal risks and uncertainties as outlined in the corporate risk register. Other risks should be monitored and reported on at other levels within the organisation. However, the Management Board should satisfy itself that appropriate risk management systems are in place for the management of these risks, throughout the organisation.

The Management Board ensures that:

- a clearly articulated risk appetite statement is in place;
- a clear strategy for risk management is in place;
- the Department's key business processes explicitly incorporate effective risk management;
- direction on risk management policy and practices is communicated, understood and applied throughout the Department;
- risk ownership is assigned and people are equipped and supported to manage risk;
- the distinction between internal and external risks, expenditure and policy risks and the risk factors under the direct control of managers and external factors should be clear;
- the extent of responsibility for risk delegated to managers, the extent of the discretion available to them for dealing with risk and the means for bringing policy and external risks beyond their control to the attention of those with responsibility for that risk should be made clear;
- risk management is a regular agenda item at management and divisional meetings;
- accompanying control measures are identified and put in place;
- there is regular and appropriate reporting to management; and
- where appropriate, risk management responsibilities be included on PMDS forms.

A Sample Risk Appetite is provided at Appendix 2

On-going review and improvement of risk management is essential to:

(i) provide assurance that risk management processes are effective;
(ii) identify where further action is necessary in order to mitigate risks; and
(iii) assess whether the risk profile of the Department is changing.

It is essential that good communication, on-going learning and the active sharing of good practice is integral to the risk management process. Everyone in the Department needs to understand, as appropriate to their role:

- the risk appetite, risk management framework and process;
- risk priorities - at Organisational, Divisional and Unit level;
- associated controls and the importance of these to be operating effectively; and
- how their particular responsibilities contribute to the achievement of Departmental and Divisional risk management objectives.

1.4 Environmental factors

The external and internal environment in which the Department operates should be taken into account when considering the risk management policy.

External environmental factors which affect the achievement of objectives include:

- legal, regulatory, audit and compliance obligations;
- changing financial/economic environment;
- cultural, social, political considerations;
- key business drivers and priorities; and
- needs and expectations of external stakeholders.

The internal environment factors which affect the achievement of objectives include:

- governance, roles and accountabilities;
- objectives and associated strategy;
- resources - capital and human resources and knowledge;
- information systems and decision-making processes;
- standards and guidelines ;
- contractual obligations; and
- administrative and management systems.

Guideline 2 - Structures

Each Department should have clearly defined risk management structures and responsibilities.

2.1 Risk Management Structures

Effective risk management is operated on the basis of clearly-defined structures and responsibilities, including roles for management assurance functions and internal audit.

In large Departments, there may be a need for dedicated structures to co-ordinate management of risk while, in smaller Departments, it may be possible to combine roles within existing management structures.

The management of risk, at operational and strategic level, is achieved by having a risk management structure which provides for clear lines of responsibility and a coordinated set of activities designed to identify, assess, mitigate and report on risks at all levels. The risk management structure is integral to management structures within a Department.

2.2 Management Structures

There are a number of important structures in place in Departments for directing, overseeing and implementing good risk management practices:-

Management Board

The Accounting Officer shall define the role of the Management Board and its role and responsibility in:

- establishing and maintaining a sound system of internal control that supports the achievement of policies, aims and objectives;
- approving the risk management policy;
- setting the risk appetite statement; and
- reviewing the corporate risk register at least on an annual basis.

The system of internal control is designed to respond to and manage the whole range of risks that the organisation faces. The system of internal control is based on an ongoing process designed to identify the principal risks, to evaluate the nature and extent of those risks, and to manage them effectively. The Management Board should consider key strategic risks and should also receive reports on the operation of the risk management system and take action, as necessary.

Heads of Division

Heads of Division with their senior managers should be responsible for:

- implementing the Department's risk management process in their Division;
- identifying, evaluating and signing off on risks at Divisional level;
- owning and managing the risks within the Division's organisational or functional remit on a day to day basis;
- ensuring that clear roles and responsibilities for risk identification, management and reporting are defined within their areas using PMDS and business planning;
- ensuring compliance with the formal risk reporting requirements on an on-going basis; and
- ensuring risk management awareness throughout the Division.

Risk Co-Ordinator

The risk co-ordinator is responsible for:

- co-ordinating the collection of risk assessments;
- co-ordinating the scoring of risks;
- ensuring that risks are scored in a consistent manner;
- collating reports to be provided to the Management Board with regard to risk management; and
- ensuring that sufficient training has been made available to management and staff.

Staff

Individual members of staff have a key part to play in managing risk by:

- being aware of the nature of risks in their day-to-day work;
- monitoring the effectiveness of management procedures created to mitigate those risks identified;
- being responsive to the changing nature of the risks faced by the organisation; and
- proactively identifying risk issues and bringing these to the attention of management.

A common responsibility of all of the above structures is communicating to everyone at all levels in the Department, the importance of knowledge, awareness and commitment to identifying, responding to and addressing individual risk areas.

Each level of supervision and management in the Department - up to and including the Management Board - should actively seek and receive appropriate and regular assurance about the management of risk within their areas of responsibility/business units/divisions. This must provide sufficient information to allow the planning of actions in respect of risks that, notwithstanding the internal controls in place, are not acceptable as well as providing assurances about risks which are deemed to be acceptably under control or will be tolerated.

2.3 Audit Structures

(i) Audit Committee

The Audit Committee has an independent role in the provision of assurance to the Accounting Officer of a Department. This includes consideration of the adequacy and effectiveness of the Department's internal control systems, control environment and control procedures, overseeing the work of Internal Audit Unit, providing advice and professional guidance in relation to the development of the Unit, and the provision of advice and guidance regarding the systems of risk management and internal control within the organisation.

Audit Committees should advise on the systems of control underlying the risk management framework and processes, including:

- engagement with and receiving assurances from management in relation to risk management systems;

- engagement with and receiving assurance from the risk committee lead/chief risk officer/risk and control functions;
- review of corporate level and divisional level risk registers;
- receiving feedback from the Head of Internal Audit and the organisation's management on the effectiveness of the risk management process; and
- taking such feedback into account for input into the priorities of the Internal Audit Unit work programme.

Further information on the role of audit committees operating in the Central Government sector is available in Guidance for Audit Committees.

(ii) Internal Audit Unit

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. Its mission is *"to enhance and protect organisational value by providing stakeholders with risk-based, objective and reliable assurance, advice and insight".*

The Internal Audit function should as part of their work programme:

- regularly review risk management arrangements and risk policy implementation;
- assess the extent to which Internal Audit can add value to the process of risk management; and
- adopt a risk-based approach to the development of its audit plan.

The work of internal audit may bring to light new or altered risks or weaknesses to controls being relied upon to manage risks.

2.4 Dedicated Risk Structures

(i) Risk Register

Departments will need to maintain centralised records about their key risks in a risk database or corporate risk register. The register will be a primary tool for risk tracking, containing the overall system of risks and the status of any risk mitigation actions. The corporate risk register will inform the principal risks and uncertainties which the Department faces.

(ii) Risk Committee

The **Risk Committee** is responsible for advising the Management Board on risk management strategy and the development of appropriate policies, procedures and systems including the preparation of a Risk Register on a Department-wide basis.

Risk committees are representative of different functional areas (technical, specialist as well as policy) and have the responsibility of coordinating the efforts of the Management Board and Line Divisions. A risk committee would also report to the Management Board on the lessons learned from risk occurrences.

Typical responsibilities of an existing committee of management assigned the risk function or a dedicated Risk Committee would be to:

- oversee the implementation of the Department's risk management framework;
- actively promote awareness in the Department in relation to embedding risk management effectively; and
- monitor the management of risk throughout the Department and report on a regular basis to the Department's MAC and Audit Committee.

Where appropriate, the role of the Risk Committee could be assigned to a Governance Committee within a Department.

(iii) Risk Management Team

In some cases, particularly with larger Departments, there may be a need for a dedicated risk management team.

A typical role for such a team would involve:

- assisting the Risk Committee with the development of risk management policy and the supporting framework;
- assisting and providing guidance to divisions of the Department on the management of risk;
- coordinating the management of risk for business processes that may cross the boundaries of business areas, divisions and locations (*"cross cutting"* issues);
- providing an analysis of risk findings on a regular basis for the Risk Management Committee; and
- maintaining the risk management reporting system

Ongoing monitoring and review arrangements by the risk committee or risk management team provides assurance that risk management performance is as expected, whether it can be improved or whether change to the framework or the process is required.

Guideline 3 - Management

Each Department should have clearly defined risk management processes and responsibilities.

3.1 Managing Risk

3.2 Risk Appetite Statement

3.3 Risk Identification

3.4 Risk Assessment

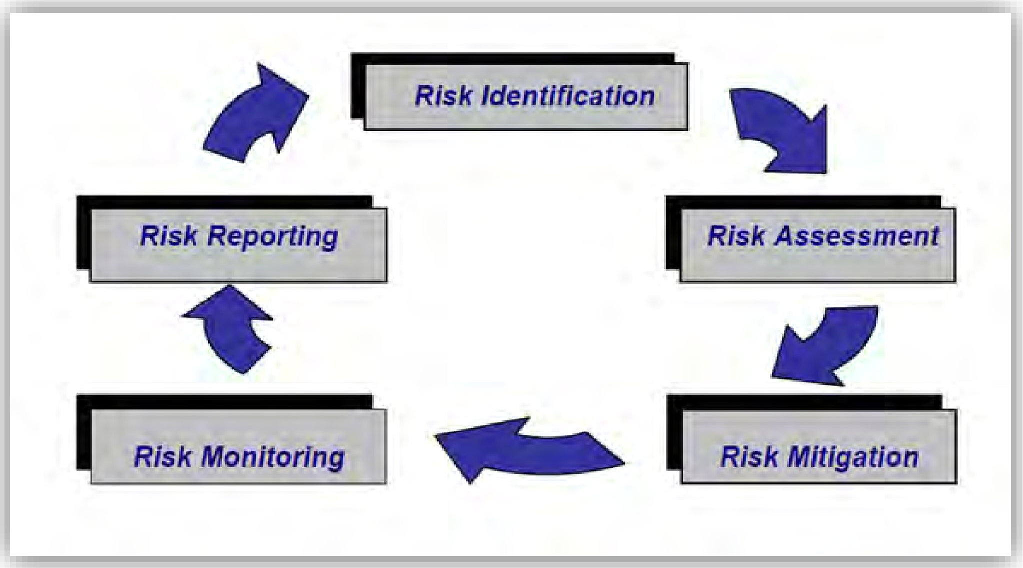
3.5 Risk Treatment and Mitigation

3.6 Risk Incidents/Events

3.1 Managing Risk

The processes for the management of risk involves establishing the risk appetite of the organisation; risk identification; risk assessment, risk treatment and mitigation, risk monitoring and reporting. The process of risk management commences with identifying risks, assessing their potential consequences and determining the most appropriate response to treating these risks. The cycle, see Figure 1 overleaf, is completed by a system of regular monitoring and reporting.

Figure 1 – The Risk Management Cycle



3.2 Risk Appetite Statement

A risk appetite statement should be drafted and approved by the Management Board for each Department. This statement should clearly articulate the degree to which the organisation is willing to accept risk. Organisations are usually willing to accept different levels of risk depending on the risk type. For example, an organisation may have zero risk tolerance with regard to compliance risk but may be willing to accept a level of risk with regard to financial risk. The risk appetite statement, once approved by the Management Board, should be clearly communicated to management. The importance of the risk appetite statement is that this will be the basis of articulating what is accepted in terms of appropriate levels of risk to be taken throughout the organisation.

3.3 Risk Identification

Categories: Risks will typically form natural groupings. While a number of approaches can be adopted, an initial approach can be adopted which classifies risks into four areas as follows:

- *Strategic risks* (risks that may be external to the organisation such as the economic climate, including factors such as interest rates, exchange rates and inflation).
- *Operational risks* (relating to the procedures/technologies etc. employed to achieve particular objectives).

- *Financial risks* (relating to the procedures/systems/accounting records in place to ensure that the organisation is not exposed to avoidable financial risks, including risks to assets).
- *Reputation and compliance risks* (involving risks to the public reputation of the organisation and their effects).

A summary of common types of risk with examples of the nature, source and effect issues, is provided at Appendix 3

***Periodic Identification**:* The process of identifying risk exposures is key to the success of a risk management process as all other elements of the process flow from this initial step. It is crucial that a comprehensive process of risk identification is completed on a regular basis. It will be a matter for each Department to identify the risks it faces as an organisation. It is also important for Departments to identify risks which could arise from not pursuing opportunities.

Identification Process: Risk identification attempts to identify a Department's exposure to uncertainty. This requires a detailed knowledge of the Department's operations and a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives. The process of drawing up statements of strategy should ensure that these elements are in place. Departments need to ask what can happen, why, and assess the consequences. They then need to establish the probability of each identified risk happening and the procedures which need to be put in place to mitigate the consequences of the risk or reduce the probability of it occurring.

Techniques: As regards how to identify risks, examples of risk identification techniques include:

- Listing the risks to continuity of service;
- Brainstorming (when, where, why and how are risks likely to arise);
- Questionnaires (e.g. to heads of divisions);
- Workshops (perhaps facilitated jointly by management and internal audit);
- Incident investigations;
- Results of audits and inspections; and
- Analysis, e.g. Cost-benefit, SWOT, Sensitivity, Cash flow.

3.4 Risk Assessment

Risk assessment is an integral part of risk management which provides a structured process for Departments to identify how its objectives may be affected. It provides management with an improved understanding of risks that could affect achievement of objectives, and of the adequacy and effectiveness of controls already in place. When the important risks facing a Department have been identified, the next step is to assess them.

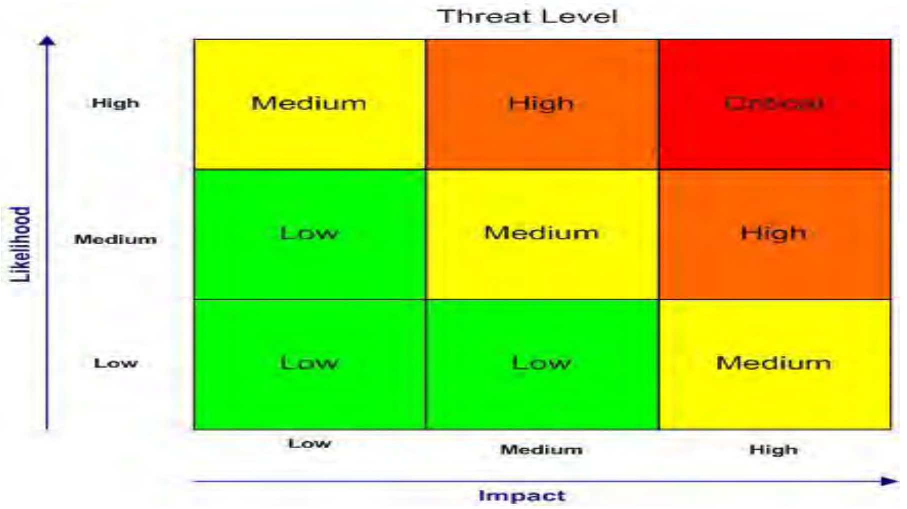
Two approaches to risk analysis are outlined below to assist Departments in structuring their own approach to risk assessment. These approaches are only examples and Departments may find that other approaches or variants of those illustrated may be more appropriate to their circumstances.

Risk mapping is a simple and useful method for assessing risks identified. It involves plotting risks on a matrix or map against relevant criteria. The assessment is usually carried out on the basis of two criteria; impact and likelihood. Having identified risks, they are recorded in the appropriate quadrant of the map. Risks located in the upper right hand side of the map i.e. those of both high impact and likelihood will require the close attention of management.

Risk criteria are the parameters established by the organisation to allow it to describe risk and make decisions about the significance of risk that take account of the organisation's attitude to risk. These decisions enable risk to be assessed and treatment to be selected.

An important consideration in the development and updating of the risk map/matrix is the extent to which the organisation proposes to rank risk inherently (on gross basis with no consideration of mitigations or controls) or residually (on net basis taking into account the effectiveness or otherwise of mitigations and controls) or to rank risks both inherently and residually. Good practice is that risks are first reviewed from an inherent perspective and then from a residual perspective in order to establish the importance of the associated controls. This can be missed if residual risk only is scored, ranked and reviewed.

The following pages outline various approaches that could be used.



Threat Level

Likelihood

High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium
	Low	Medium	High

Impact

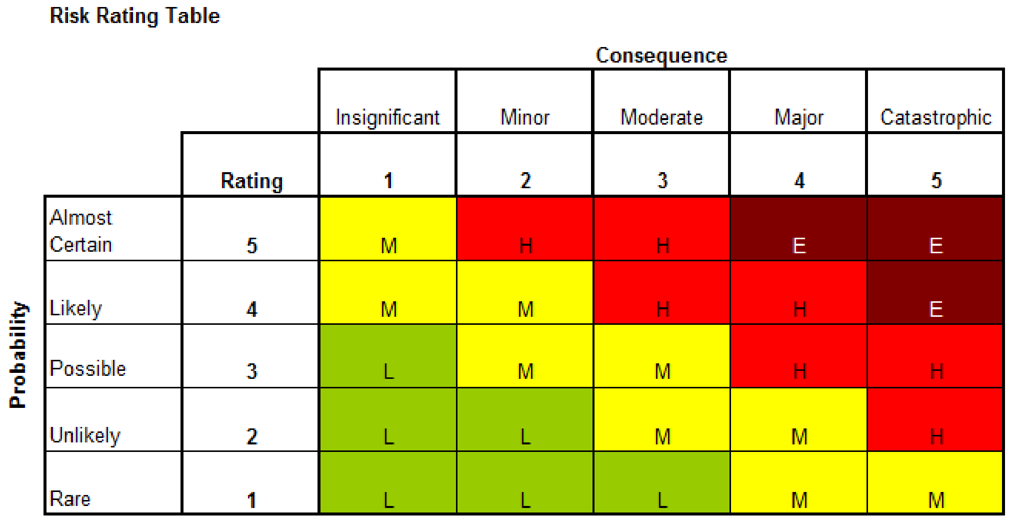
Red: Critical - Issues that require immediate attention of senior management.

Amber: High - Issues that need constant monitoring by senior management.

Yellow: Medium - Issues for frequent review

Green: Low - Issues that need to be reviewed from time to time.

Below is a more detailed version as set out in the Department of Public Expenditure and Reform *"Risk Management Handbook"* which is consistent with "*International Standards Organisation (ISO) 31000 Risk Management - Principles and Guidelines"* in rating risks on a 5x5 matrix reflecting consequence and probability. In rating risk, risk criteria should be used so as to ensure consistency in scoring. For example for any of the categories mentioned above i.e. reputational or operational, what does a rating of 5 mean? In terms of probability, what



Risk Rating Table

Probability

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Rating	**1**	**2**	**3**	**4**	**5**
Almost Certain	**5**	M	H	H	E	E
Likely	**4**	M	M	H	H	E
Possible	**3**	L	M	M	H	H
Unlikely	**2**	L	L	M	M	H
Rare	**1**	L	L	L	M	M

Where: **L** = Low Risk, **M** = Medium Risk, **H** = High Risk, **E** = Extreme Risk does a rating of 3 mean? The scoring should reflect the context within the Department and the nature and extent of risk mitigations and controls in place.

Likelihood Scoring

Likelihood scoring is based on the expertise, knowledge and experience of the individuals scoring the likelihood. In assessing likelihood, it is important to consider the nature of the risk. Risks are assessed on:

- the probability of future occurrence;
- how likely is the risk to occur; and
- how frequently has this occurred?

The likelihood of a particular risk materialising depends upon the effectiveness of existing controls. In assessing the likelihood, consideration should be given to the robustness of existing controls in place.

The assessment of likelihood of a risk occurring is assigned a number from 1-5, with 1 indicating that there is a remote possibility of it occurring and 5 indicating that it is almost certain to occur.

Impact Scoring

To determine the impact each risk area should be assigned descriptors over 5 levels ranging from negligible or insignificant to substantial or catastrophic. In scoring impact, the anticipated outcome of the risk is graded from 1-5, with 5 indicating a more serious impact.

Another method of assessment is to include an assessment of how effective existing controls are in relation to each risk. This added element is rated 1 to 3 and used as an extra multiplier in rating risk as part of the assessment process. The example overleaf demonstrates how risk could be assessed on the basis of three criteria; Impact, Likelihood and Effectiveness of Existing Controls.

Impact on the Department: 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”.

Likelihood of occurrence: The likelihood of occurrence is estimated again on a scale of 1 to 5 where 1 is "rarely, if ever" and 5 is "almost unavoidable/already happening".

Effectiveness of existing controls: The effectiveness of existing controls is estimated using a scale of 1 to 3 where 1 is "highly effective" and 3 is "no controls/controls ineffective".
A risk 'score' is then determined by multiplying the three numbers together to determine the risk reporting level. Under this method, the risk scores are defined as follows:

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 Effect	5 = Almost unavoidable/ already occurring	

Possible Risk Reporting Level:

0 – 12 = Green	13 – 24 = Amber	25+ = Red

Sample Risk Registers are provided in Appendices 4, 5 & 6

Risk management is an organisational-wide activity and staff should be aware that it is an important part of their work and robust and effective procedures for escalating important risk issues which suddenly develop or emerge must be in place.

Accountable ownership of each risk is an important element of the strategy. It is essential that the owner of the risk has sufficient information to correctly assess its place on the register and is empowered to implement changes/controls to manage the risk.

3.5 Risk Treatment and Mitigation

Whatever method is used for risk assessment, for each type of risk identified, a Department can treat risks in the following manner:

- treat it according to the activities defined for it;
- tolerate unavoidable risks depending on the risk tolerances/appetite of various key stakeholders;
- transfer the risk elsewhere;
- terminate the activity causing it; and
- introduce additional mitigating activities in order to reduce the impact or the likelihood of the risk.

When risks have been identified and analysed, Departments should determine an appropriate method for addressing them.

Before considering which method is most appropriate to a particular risk, Departments will firstly need to consider the adequacy and appropriateness of any existing controls.

Departments should ensure that the costs of controls to mitigate risk are not disproportionate to the potential impact of a risk being managed.

Departments should also bear in mind that business continuity management is an essential element towards mitigating the effects of risks on the key activities of a Department.

It might be helpful for users of these Guidelines to be aware that the Business Continuity Institute produce *"Good Practice Guidelines"* (2013), which users may find useful.

In summary, the risk register will normally include:

- a description of the risk;
- the category or type or risk;
- the current mitigations and actions in place to address the risk;
- an assessment of the likelihood that it will occur and the possible consequences if it does occur ranked in accordance with the agreed rating scale;
- an outline of additional proposed mitigation actions, where appropriate; and
- who is accountable and responsible for managing that risk.

Each Division will maintain their own risk register as a basis for implementing and monitoring risk management activities at that level.

A corporate level risk register will outline the principal risks and uncertainties facing the Department.

3.6 Risk Incidents/Events

Each Department should have an incident management policy in place. This should include ensuring that the following occurs:

- the incident is reviewed to assess the impact of the incident using the agreed impact criteria;
- the impact is compared to the risk appetite statement to determine its seriousness;
- this is used as the basis for escalation of the incident to the responsible individual/ group;
- a mitigation plan for reducing the impact of this event is determined, agreed and actioned;
- consideration is taken with regard to other similar risks/potential incidents which may occur; and
- the risk register is updated accordingly.

In addition to this, “near misses” should be treated in line with the above. Staff should be aware of the requirement to report “near misses” and should take into account the potential impact should an event have taken place and should escalate as appropriate.

Guideline 4 – Monitoring and Reporting

Departments' risk management systems should provide for monitoring and reporting at various levels of management.

4.1 Risk Monitoring and Reporting

4.2 Records

4.3 Risk Review

4.1 Risk Monitoring and Reporting

Management Board

The risk assessment process will identify the risks with the greatest potential for negative impact and high likelihood. This will inform the basis of the monitoring and reporting of risk at Management Board level. There should be regular and structured engagement at Management Board level and consideration of current priorities, the principal risks and uncertainties and the overall risk profile and risk trends as evidenced in the risk register.

The Management Board, and in particular the Accounting Officer, should:

- be assured that the risk management processes are working effectively;
- ensure periodic updates on risk management and findings are provided to the Management Board;
- ensure at least annual review of entire risk register;
- ensure periodic review of effectiveness and associated internal controls;
- ensure periodic review of effectiveness of the risk management framework; and
- know how the Department will manage a crisis. This will require regular testing of contingency plans to deal with risks identified.

Divisions should:

- be aware of the significant risks that come within their area of responsibility; the possible impacts those risks could have on other areas of their Department and the consequences other Divisions' risks might have on them; and
- report systematically and promptly to senior management about risk management, in particular about perceived new risks or failures of existing controls.

Staff should:

- understand their accountability for risks and report systematically and promptly to senior management on any perceived new risks or failures of existing controls.

4.2 Records

The retention of records is an important element of a good risk management system. Records document the fact that risks have been identified and remedies considered. Management may be reluctant to release such records for sensitivity reasons and because they would highlight weaknesses detrimental to the effective management of the organisation.

Departments should ensure that they achieve a consistent approach to FOI requests relating to risk management records and should have regard to any guidance in this area issued by the FOI Central Policy Unit, Department of Public Expenditure and Reform.

4.3 Risk Review

Reviewing risk is crucial to ensuring that significant risk areas are included in the monitoring and reporting system (and removed, if appropriate) and that measures are identified to address those risks. The review process can be applied at a strategic, structural, management, control or individual risk level.

In this context, particular attention should be paid to the compilation of a schedule of key strategic risks drawn from the annual Business Plan at the beginning of the year and the subsequent review process throughout the year. This involves:

- identifying key risk areas;
- evaluating their likelihood and possible impact; and
- developing options for minimising/mitigating risks.

One key measure of effectiveness of the risk management process is the nature and extent to which it forms part of the dialogue within Divisions and at Management Board level through the sharing of insights and experience and also, through fostering a culture of constructive challenge as part of the process.

The key objective of this exercise is to restrict threats to key Departmental priorities and administrative processes to acceptable levels and to ensure appropriate reporting to the Management Board.

Appendix 1 – Risk Management Guidance for Government Departments and Offices (2004)

	Guideline
Integrated to management process	Each department is to initiate risk management as an integral and on-going part of its management process. The Management Board should put in place effectiveness mechanisms to carry out risk management accordingly.
Simple and straightforward	The risk management process should be kept as simple and straightforward as possible, and existing management structures should be used, as far as possible.
Risk ownership	Each department should have clearly defined risk management structures and responsibilities.
Risk identification	Departments should repeat the process of risk identification at least once a year.
Risk assessment	Departments should assess identified risks at least once a year.
Risk mitigation	When risks have been identified and assessed, Departments should determine an appropriate method for addressing them.
Risk monitoring	Departments risk management systems should provide for monitoring and reporting at various levels of management.

Appendix 2 – Risk Appetite Sample

Category	Item	Green (Appetite)	Amber (Tolerance)	Red (Limit)	Internal Monitoring and Reporting	External Monitoring and Reporting
Financial	Monetary value of financial impact of identified risk, after mitigation.	2.5% of budget or ≤€XXK	Between 2.5% and 5% budget or Between XK and €250K	>5% of budget or >€XXK	Relevant Committee: >€XXk or 4% of budget Management Board: >€XXk or 10% of budget	If deemed appropriate by the Management Board
Strategic	Strategic impact on organisation measured against set KPIs	No appetite – KPI targets are met	Minor KPI target(s) are not met	Will not meet key strategic objective(s) as per Legislation	Relevant Committee: Minor KPI target not met Management Board: Will not meet a strategic objective	If deemed appropriate by the Management Board
Operational	Lack of quality in response to stakeholder requirements	0 complaints from individual stakeholder	< 2 complaints from individual stakeholder	>2 complaints from individual stakeholder	Committee: If >2working days or >2 complaints for from individual stakeholder Management Board: If deemed appropriate by Committee	If deemed appropriate by the Management Board
	Unavailability and/or system(s) failure	1 working day	< 2 working days	>2 working days		
	Unable to provide core service(s)	1 working day	< 2 working days	>2 working days		
Reputational	Adverse media coverage and/or public attitude	No media coverage	Critical article in press and/or public criticism from regulatory body	Ministerial concern or comparable political repercussions.	Committee: Critical article in press or criticism from regulatory body or < 2 concurrent complaints. Management Board: Anything involving political repercussion or >2 complaints from individual stakeholder	If deemed appropriate by the Management Board
	Loss of stakeholder confidence	0 complaints from individual stakeholder	< 2 complaints from individual stakeholder	>2 complaints from individual stakeholder		
Compliance	Confirmed and quantified breaches of compliance and/or regulatory requirements.	Compliance with all standards internal and external	Minor non-compliance with internal standards or protocols	Non-compliance with regulatory and/or legislative and/or other compliance requirements	Management Board: If deemed material by Committee	If deemed appropriate by the Management Board

Appendix 3 – Risk Categories

The table below offers a summary of the most common categories of risk with examples of the nature of the source and effect issues.

Category of Risk	
External	
1. Infrastructure	Relating to infrastructures such as transport systems for staff, power supply systems, suppliers, business relationships with partners and dependency on internet and e-mail.
2. Economic	Relating to economic factors such as interest rates, exchange rates, inflation.
3. Legal & Regulatory	Relating to the laws and regulations which if complied with should reduce hazards (E.g. – Health and Safety at Work Act).
4. Environmental	Relating to issues such as fuel consumption, pollution.
5. Political	Relating to possible constraints such as change of Government.
6. Market	Relating to issues such as competition and supply of goods.
7. "Act of God"	Relating to issues such as fire, flood, and earthquake.
Financial	
8. Budgetary/Financial	Relating to the availability of resources or the allocation of resources.
9. Fraud or theft	Relating to the unproductive loss of resources.
10. Insurable	Relating to the potential areas of loss which can be insured against.
11. Capital investment	Relating to the making of appropriate investment decisions.
12. Liability	Relating to the right to sue or to be sued in certain circumstances.
Activity	
13. Policy	Relating to the appropriateness and quality of policy decisions.
14. Operational	Relating to the procedures employed to achieve particular objectives.
15. Information	Relating to the adequacy of information which is used for decision making
16. Reputational	Relating to the public reputation of the organisation and consequent effects.
17. Transferable	Relating to risks which may be transferred or to transfer of risks at inappropriate cost.
18. Technological	Relating to the use of technology to achieve objectives.
19. Project	Relating to project planning and management procedures.
20. Innovation	Relating to the exploitation of opportunities to make gains.
Human Resources	
21. Personnel	Relating to the availability and retention of suitable staff.
22. Health and Safety	Relating to the well-being of people.
OTHER 23 Inter-agency 24 Intra-agency	Relating to work and activities of external bodies Relating to internal activities and support services

(Source: HM Treasury modified)

Appendix 4 – Sample Risk Register

RISK NO.	DESCRIPTION	DIVISION	STRATEGY STATEMENT OBJECTIVE NO.	LIKELIHOOD	IMPACT	CONTROL EFFECTIVENESS	RATING	CONSEQUENCES	MEASURES TO ADDRESS	ADDITIONAL ACTION	OWNER
2/04	Impact of an increase in BSE cases in ROI	Beef Division	4.1. 2004	3	5	2	🟥 30 RED	-Fall in public confidence in beef. -Financial consequences for livestock industry -	-Develop communications strategy ………	Review efficacy of control measures	Head of Beef Division
3/04	…..						🟩				
4/04	……						🟨				

Appendix 5 – Sample Risk Register

A N OTHER ORGANISATION

Principal Risks*	Mitigations / Controls / Management Actions	Risk ranking						Suggestions on Additional Actions / Controls / Mitigations	Account / Owner
		(a) Impact			(b) Likelihood				
		Low (1)	Medium (3)	High (5)	Low(1)	Medium (3)	High(5)		

Appendix 6 – Sample Risk Register

Objective ____________________

Activity: ____________________

Likelihood	Consequence
1 Rare	1 Negligible
2 Low	2 Minor
3 Medium	3 Moderate
4 High	4 Significant
5 Very High	5 Substantial

Risks Category	Principal Risks	Mitigations / Controls / Management Actions	Risk Ranking		Suggestions on Additional Actions / Controls / Mitigations	Responsibility Ownership
			Likelihood	Consequence		

Bibliography

- Business Continuity Institute (BCI) *Good Practice Guidelines* (2013)
- Department of Public Expenditure and Reform, *Corporate Governance Standard for the Civil Service* (November 2015)
- CIPFA and IFAC, *International Framework: Good Governance in the Public Sector* (July 2014)
- International Standards Organisation (ISO*) 31000 Risk Management - Principles and Guidelines* (November 2009)
- *Report of the Working Group on the Accountability of Secretaries General and Accounting Officers* (July 2002)
- Department of Finance, *Risk Management for Government Departments and Offices* (March 2004)

Tithe an Rialtais,
Sráid Mhuirfean Uacht,
Baile Átha Cliath 2,
Éire.

Government Buildings,
Upper Merrion Street,
Dublin 2,
Ireland.

T: 353 1 676 7571
E: govacc@per.gov.ie