Risk Management Strategy

April 2019

Contents

1. Risk Management Strategy

1.1 Risk Management Strategy Overview

DAO (DFP) 10/12 issued by the former Department of Finance and Personnel in October 2012 confirmed the requirement for each Accounting Officer to prepare a Governance Statement in place of an Annual Statement on Internal Control from the financial year 2012/13 onwards. This Risk Management Strategy has been developed in order to support completion of this Governance Statement. The Strategy has been revised a number of times since its original development in 2012.

Libraries NI's risk management strategy is set out in a series of sections / documents.

- Risk Management Strategy
- The Assessment of Risk
- Risk Appetite
- Risk Management Group Terms of Reference
- Guide to Governance Statement
- Risk Management Terminology and Definitions
- Libraries NI Corporate Risk Register

These should be read in conjunction with:

- Risk Management Policy

1.2 Context for Risk Management

These documents require continuous review and are presented to the Audit and Risk Assurance Committee for endorsement and adoption after every material amendment.

The documents:

- Set out Libraries NI's attitude to risk
- Establish the definition of a 'Key Risk'
- Define the structures for the management and ownership of risk and the management of situations in which control failures may lead to material realisation of risks
- Specify the way in which risk issues are to be considered at each level of business planning ranging from the corporate process to the setting of individual staff's objectives
- Specify how new activities will be assessed for risk and incorporated into risk management structures
- Ensure common understanding of terminology used in relation to risk issues
- Define the structures for gaining assurance about the management of risk
- Define the criteria which will inform assessment of risk and the definition of specific risks as 'key'.

- Define the way in which risk register and risk evaluation criteria will be regularly reviewed.

1.3 Risk Management Context

The strategy is also developed with the understanding that risk management is not entirely internal to any organisation. In developing the risk management strategy, Libraries NI has to consider the attitude to risk and the risk priorities of stakeholders and external partners such as the Department for Communities; the Department of Finance; key suppliers of goods and services, the NIAO etc…

The development of this Risk Management Strategy has been based on the requirements and good practice guidelines contained in the following:

- DAO(DFP) 10/12 Requirement to Complete a Governance Statement
- Managing Public Monies NI Annex 3.1 The Governance Statement
- HM Treasury: The Orange Book: Management of Risk – Principles and Concepts October 2004
- HM Treasury: Risk Management Assessment Framework July 2009
- HM Treasury: Thinking About Risk – Managing Your Risk Appetite: A Practitioner's Guide November 2006
- HM Treasury: Thinking About Risk – Managing Your Risk Appetite: Good Practice Examples November 2006
- National Audit Office Fact Sheet – February 2013
- DAO(DFP) 06/13 Corporate Governance in Central Government Departments: Code of Good Practice – April 2013
- NIAO Good Practice in Risk Management - June 2011

2. Assessment of Risk

2.1 Core Strategic Objectives

In order to determine where resources should be concentrated to provide effective management of risk, it is necessary to identify Libraries NI's key objectives, i.e. those objectives the achievement of which is regarded as essential for the success of the organisation.

The Libraries NI Corporate Plan identifies Libraries NI's Core Objectives which are translated into annual business plans. The identification of these objectives is advised by policy documents such as 'Delivering Tomorrow's Libraries' and by other policy directives from the Minister and the Department for Communities.

Input is also being sought from other Libraries NI Stakeholders particularly, Customers, Staff and Board Members. Libraries NI also takes into account professional standards and performance targets which have been established.

2.2 Core Operational Objectives

Each directorate and project within Libraries NI has also established its own Risk Register. These are kept under continuous review. These registers are a record of the risks to the achievement of the operational objectives of each directorate or project and the controls in place or required to manage these risks.

2.3 Key Risk

A risk to a corporate objective where the inherent risk is considered to have a very high likelihood of occurring and a major impact on the achievement of the objective should it occur.

2.4 Horizon Scanning

Increasingly both in the public and private sectors the importance of looking over the horizon and managing upcoming risk is now recognised.

In particular, laws and regulations can have an effect on the risk environment. It is important for an organisation to identify the ways in which laws and regulations will make demands on it, either by requiring the organisation to do certain things or by constraining the actions which the organisation is permitted to take.

2.5 The Assessment of Risk

2.5.1 RISK REGISTER: Risk Levels

Impact Levels

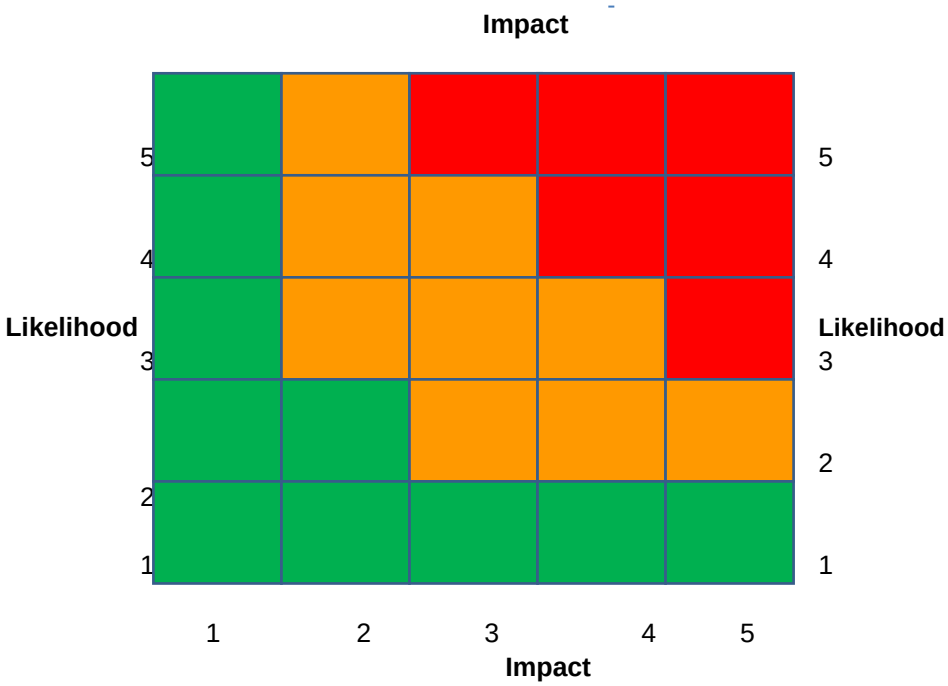
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Catastrophic

Likelihood

1	Rare
2	Unlikely
3	Moderate
4	Likely
5	Almost Certain

Risk Appetite

0 - 2	Averse
3 - 4	Minimalist
5 - 8	Cautious
9 - 12	Open
13 - 25	Hungry



The assessment of risk is performed by evaluating both the likelihood of the risk being realised, and of the impact if the risk is realised. A categorisation of high / medium / low in respect of each is often considered sufficient. However, it has been decided that a more detailed analytical scale should be used within Libraries NI as it is felt that clear quantitative evaluation can be applied to the identified risks - A “5x5” matrix is used to assess risk. This operates with impact on a scale of “insignificant / minor / moderate/ major/ catastrophic” and likelihood on a scale of “rare / unlikely / possible / likely / almost certain”. Colour (“Traffic Lights”) are used to further clarify the significance of risks.

The assessment of risk is carried out at three levels:

2.5.2 Inherent Risk: Risk is defined as the uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks (the “inherent risks”) and then responding to them i.e. risks that could occur if no internal control framework was in place.

2.5.3 **Residual Risk:** The response, which is initiated within the organisation, to risk is called “internal control” and may involve one or more of the following:

- tolerating the risk
- treating the risk in an appropriate way to constrain the risk to an acceptable level or actively taking advantage, regarding the uncertainty as an opportunity to gain a benefit
- transferring the risk
- terminating the activity giving rise to the risk.

In any of these cases the issue of opportunity arising from the uncertainty should be considered.

2.5.4 **Treated Risk:** The level of risk remaining after internal control has been exercised (the “residual risk”) is the exposure in respect of that risk, and should be acceptable and justifiable – it should be within the risk appetite. Where treated risk exceeds the risk appetite, consideration should be given to providing additional resources to supplement the internal controls (treating), insuring against the risk (transferring) or discontinuing the risky activity (terminating).

Most controls are designed to reduce the likelihood of a risk materialising however, controls are also required to mitigate the impact and extent of a risk should it occur. Managers should draw up contingency plans for the management of situations in which control failure leads to materialisation of risks.

The plans should be communicated to those who are involved in it and critical to its success. Testing of the plans to ensure that they will work when required is also essential.

2.6 **Risk Management Reporting and Structures**

The following arrangements have been established within Libraries NI:

- A Risk Management Group (RMG) exists which consists of the Chief Executive, the Director of Business Support and the Director of Library Services. The Head of Internal Audit also attends all meetings of this group. Other Board officers as required will advise the group;
- The RMG will identify key risks to Core Objectives identified in the Libraries NI Corporate Strategy and Operational Business Plans. They will review and update the Corporate Risk Register and will draw the attention of the Audit and Risk Assurance Committee to any relevant matters. The Risk Management Group Terms of Reference is included as Section 4 of this document.

- Line managers (Assistant Directors, Heads of Department, Service Development Managers etc…) will identify operational risks. Each Directorate has developed its own risk register based on their core operational objectives. These are used to inform the development of the Corporate Risk Register.
- The identification, assessment and management of key risks is an ongoing process, however a formal review of risk is conducted in each Directorate twice a year. The identification of controls required will require the implementation of an action plan, individual actions should be incorporated into the business planning process and individual staff objectives during annual appraisal.
- The RMG will meet formally four times a year in advance of each scheduled ordinary meeting of the Audit and Risk Assurance Committee. A report on risk management issues within Libraries NI will be developed by the Group and issued to the Committee. (See RMG Terms of Reference).
- Independent review of the effectiveness of the Risk Management Framework is essential. Risk Management has been identified as a Strategic Area and will be subject to ongoing review by Internal Audit. Assurance on the independence and effectiveness of this review has been strengthened. In October 2016 an External Quality Assessment was completed on the Internal Audit Section of Libraries NI. This assessment concluded that in all areas examined Internal Audit met the standard required and was therefore in compliance with Public Sector Internal Audit Standards.

2.7 Risk Register

The Libraries NI Corporate Risk Register has been designed to record all key risks to core objectives in a structured way. There is a record of dependencies between risks, identifying the risks together that may impact on each key objective. It identifies the inherent risk rating (both impact and likelihood) and identifies the risk owner.

This risk owner has been delegated responsibility for keeping the risks to the objective under review, identifying what factors may contribute to the realization of the risks, ensuring a control framework is in place to reduce the likelihood of the risk occurring or to reduce the impact of the risk should it occur.

An assessment of residual risk (with controls in place) is then completed. If the residual risk rating is still greater than is acceptable as defined by the Risk Appetite, additional controls and an action plan to put them in place are required.

The ‘risk owner’ must have the authority to assign resources to ensure appropriate management of the risk.

3. Risk Appetite

3.1 Risk Appetite: Definition

Risk appetite is the amount of risk to which the organisation is prepared to be exposed before it judges action to be necessary. The fact that the resources available to control risks are likely to be limited means that value for money decisions have to be made – what resource cost is it appropriate to incur to achieve a certain level of control in respect of the risk? Apart from the most extreme circumstances it is unusual for good value for money to be obtained from any particular risk being completely obviated with total certainty.

Risk appetite may be very specific in relation to a particular risk, or it may be more generic in the sense that the total number of risks, which an organisation is prepared to accept at any one time will have a limit.

The successful application of risk appetite is about taking well thought through risks where the long-term rewards are expected to be greater than any short-term losses.

When considering threats, the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance.

3.2 Identification of Risk Appetite

In consequence every organisation has to identify its risk appetite. Decisions about response to risk have to be taken in conjunction with an identification of the amount of risk that can be tolerated. Any particular organisation is unlikely to have a single risk appetite. The tolerable extent of risk will vary according to the perceived importance of particular risks. For example, tolerable financial loss may vary in accordance with a range of features including the size of the relevant budget, the source of the loss, or associated other risks such as adverse publicity. The control responses therefore have to be considered in detail to identify the appropriate balance of potential realisation of risk against the costs of limiting that risk.

The most significant issue is that it is unlikely, except for most extreme risks that any particular risk will need to be completely and absolutely obviated. Identification of risk appetite is a subjective (rather than an objective or scientific) issue.

3.3 Risk Tolerance

An awareness and understanding of the current risk tolerances of various stakeholders is a key ingredient in establishing the corporate risk profile. The environmental scan will identify stakeholders affected

by an organisation's decisions and actions, and their degree of comfort with various levels of risk. Understanding the current state of risk tolerance of citizens, parliamentarians, interest groups, suppliers, as well as other government departments will assist in developing a risk profile and making decisions on what risks must be managed, how, and to what extent.

In the public service, citizens' needs and expectations are paramount. For example, most citizens would likely have a low risk tolerance for public health and safety issues (injuries, fatalities). Other risk tolerances for issues such as project delays and slower service delivery may be less obvious and may require more consultation.

In general, there is a lower risk tolerance for the unknown, where impacts are new, unobservable or delayed. There are higher risk tolerances where people feel more in control (for example, there is usually a higher risk tolerance for automobile travel than for air travel).

Risk tolerances may change over time as new information and outcomes become available, as societal expectations evolve and as a result of stakeholder engagement on trade-offs.

It should be noted that some risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example organisations have to accept that there is a risk arising from the possibility of a flu pandemic which they cannot control. In these cases, the organisation needs to make contingency plans which will help to reduce the impact should the risk be realised.

3.4 Risk Appetite

- Averse – Avoidance of risk and uncertainty is a key objective (Residual Risk Rating 0 – 2)
- Minimalist – Preference for ultra-safe options that have a very low degree of residual risk and only have potential for limited reward (RRR 3 – 4)
- Cautious – Preference for safe options that have a low to moderate degree of residual risk and may have limited potential for reward (RRR 5 – 8)
- Open – Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward… Will have a moderate degree of residual risk (RRR 9 – 12)
- Hungry – Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risk). Will have a high degree of residual risk. (RRR 13 – 25)

With the risk factors defined, individual risks can be assessed against the risk appetite descriptors to determine whether the optimum level of residual risk has been reached.

3.5 Risk Appetite within Libraries NI

Libraries NI's risk appetite is conditioned by many issues. Among the more important of these are government statute and guidelines. Much of Libraries NI's attitude to risk is driven by the attitude of the host department, the Department for Communities.

The Risk Management Group have identified eight key issues where risks to each need to be identified. A description of the context of each issue is included. The assessment of corporate risk appetite has been taken by the Risk Management Group and has been presented to the Audit and Risk Assurance Committee for their consideration.

Participation and Relevance: The risk appetite for this objective has been determined as being **Open**. Managers are willing to consider all options and choose the one that is most likely to result in successful delivery.

Stakeholder Engagement: The risk appetite for this objective has been determined as being **Open**. Managers are willing to consider all options and choose the one that is most likely to result in successful delivery.

Staff: The risk appetite for this objective has been determined as being **Cautious**. It is considered that for the effective operation of Libraries NI only safe options with a low to moderate degree of residual risk should be considered.

Corporate Governance: The risk appetite for this objective has been determined as being **Averse**. It is a priority objective that the service should achieve its main governance objectives. Avoidance of risk in this area is a key objective.

Resources: The risk appetite for this objective has been determined as being **Cautious**. It is considered that for the effective operation of Libraries NI only safe options with a low to moderate degree of residual risk should be considered.

Planning: The risk appetite for this objective has been determined as being **Open**. Managers are willing to consider all options and choose the one that is most likely to result in successful delivery.

Information Security: The risk appetite for this objective has been determined as being **Averse.** It is a priority objective that the service should achieve its main governance objectives. Avoidance of risk in this area is a key objective.

Business Continuity: The risk appetite for this objective has been determined as being **Minimalist**. There is a preference for ultra-safe options that have a very low degree of residual risk even if there is only potential for limited reward.

4. Risk Management Group – Terms of Reference

4.1 Constitution

Libraries NI has established a Risk Management Group (RMG) as an officers' working group with responsibilities for issues of risk, control and governance. Its remit is to ensure that the Corporate Risk Register is kept up to date and is an accurate reflection of the risks facing the organisation. The Group is also tasked with ensuring that the controls in place are adequate to mitigate key risks and where that is not the case, additional resources are employed to develop an action plan whereby additional controls can be implemented.

4.2 Membership

The members of the RMG are:

- The Director of Business Support (Chair)
- The Chief Executive
- The Director of Library Services

The Head of Internal Audit will also attend meetings of the Group to offer consultancy advice and guidance.

The RMG will be provided with a secretariat function on a rotational basis by a manager of appropriate seniority.

4.3 Reporting

The RMG will formally report in writing to the Accounting Officer and to the Audit and Risk Assurance Committee after each meeting.

4.4 Responsibilities

The objectives of the Risk Management Group are as follows:

- Take steps to raise the level of awareness of risk throughout the organisation
- Co-ordinate the identification of those risks and exposures, which have or may give rise to loss producing events
- Assess the impact of potential loss producing events
- Co-ordinate the taking of reasonable physical or financial steps to avoid or reduce the impact and or likelihood of potential losses
- To 'Scan the Horizon' to identify external risks that may in the future have an impact on the ability of Libraries NI to meet its core objectives

4.5 Rights

The RMG may:

- co-opt additional members to provide specialist skills, knowledge and experience
- procure specialist ad-hoc advice at the expense of Libraries NI, subject to agreed budgets

4.6 Meetings

- The RMG will meet at least four times a year in advance of each routine meeting of the Audit and Risk Assurance Committee. Additional meetings may be convened as deemed necessary
- An appropriate manager (selected on a rotational basis) will act as secretary ensuring that an agenda is set for and minutes and action plans result from each meeting of the Group. He / She will also ensure that a report is issued to the Chief Executive and to the Audit and Risk Assurance Committee
- The RMG may ask other officials of Libraries NI to attend to assist it with its discussions on any particular matter.

5. Requirement to Complete a Governance Statement

5.1 Introduction

Annex 3.1 of Managing Public Monies Northern Ireland (MPMNI) issued by the former Department of Finance and Personnel in October 2012 contains guidance on the completion of the Governance Statement. It is fundamental to each accounting officer's responsibilities to manage and control the resources used in his or her organisation. The governance statement, a key feature of the organisation's annual report and accounts, manifests how these duties have been carried out in the course of the year. It should encompass discussion of both corporate governance and risk management matters.

There is no set template for the governance statement however the following listing summarises subjects that should always be covered.

- the governance framework of the organisation, including information about the Board's committee structure, its attendance records, and the coverage of its work
- the Board's performance, including its assessment of its own effectiveness
- highlights of Board / Committee reports, notably by the Audit and Risk Assurance Committee
- an account of corporate governance, including the Board's assessment of its compliance with the *Corporate Governance Code*, with explanations of any departures
- information about the quality of the data used by the Board, and why the Board finds it acceptable
- a record of any ministerial directions given, subject to a public interest test
- a risk assessment, including the organisation's risk profile, and how it is managed, including, subject to a public interest test:
    - any newly identified risk
    - a summary of any significant lapses of protective security (e.g. data losses).

5.2 Internal Control Divergences

In putting together the governance statement, the Accounting Officer needs to take a view on the extent to which items are significant enough to the welfare of the organisation as a whole to be worth recording. Where potential internal control divergences have been identified the following factors should be taken into account;

- might the issue prejudice achievement of the business plan? – or other priorities?
- could the issue undermine the integrity or reputation of the organisation?
- what view does the Board's Audit and Risk Assurance Committee take on the point?
- what advice or opinions have internal audit and/or external audit given?
- could delivery of the standards expected of the AO (Box 3.1) be at risk?
- might the issue make it harder to resist fraud or other misuse of resources?
- does the issue put a significant programme or project at risk?
- could the issue divert resources from another significant aspect of the business?
- could the issue have a material impact on the accounts?
- might national security or data integrity be put at risk?

5.3 Completion of Governance Statement

The Governance Statement provides assurance as to the effectiveness of the risk, control and governance framework within Libraries NI. It requires ongoing and continuous consideration of whether appropriate risk management, control and review processes are in place within all levels of the organisation to support its completion.

6. Risk Management – Terminology and Definitions

6.1 Introduction

Risk management is part of the broader management processes of organisations. Where terms related to risk management are used in a policy or procedure, it is imperative that their intended meanings within that context are not misinterpreted or misunderstood. Accordingly, this Guide provides definitions for the various meanings that each term is likely to have.

6.2 Terminology and Definitions

6.2.1 Risk

Combination of the likelihood of an event and its impact

6.2.2 Key Risk

A risk to a corporate objective where the inherent risk is considered to have a very high likelihood of occurring and a major impact on the achievement of the objective should it occur.

6.2.3 Assessment of Risk

Overall process of risk analysis and risk evaluation

6.2.4 Risk analysis

Systematic use of information to identify sources and to estimate the risk

6.2.5 Risk identification

Process to find, list and characterise elements of risk

6.2.6 Inherent Risk

The combination of the likelihood of an event and its impact assessed before the implementation of a control framework

6.2.7 Impact

The effect that the material realisation of a risk will have on the achievement of an objective. The material realisation of a risk can have impact on more than one identified objective.

6.2.8 Likelihood

The frequency of or extent to which an event is likely to occur

6.2.9 Event

Occurrence of a particular set of circumstances

6.2.10 Contributing Factors

Issues which may precipitate or facilitate the realisation of an event.

6.2.11 Risk criteria
Terms of reference by which the significance of risk is assessed

6.2.12 Risk management
Co-ordinated activities to direct and control an organisation with regard to risk

6.2.13 Residual risk
Assessment of risk remaining after the implementation of existing controls.

6.2.14 Stakeholder
Any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by, a risk

6.2.15 Risk optimisation
Process, related to a risk, to minimise the negative and to maximise the positive consequences and their respective probabilities

6.2.16 Risk reduction
Actions taken to lessen the probability, negative consequences or both, associated with a risk

6.2.17 Mitigation
Limitation of any negative consequence of a particular event

6.2.18 Risk Appetite
The amount of risk to which an organisation is prepared to be exposed.

6.2.19 Treated Risk
The assessed risk level remaining after all planned actions and controls have been implemented.

7. Libraries NI - Corporate Risk Register

See attached document