N I A O

Northern Ireland Audit Office

Good practice in risk management

REPORT BY THE COMPTROLLER AND AUDITOR GENERAL
8 June 2011

Northern Ireland Audit Office

Report by the Comptroller and Auditor General for Northern Ireland

Good practice in risk management

BELFAST: The Stationery Office £5.00

This report has been prepared under Article 8 of the Audit (Northern Ireland) Order 1987 for presentation to the Northern Ireland Assembly in accordance with Article 11 of that Order.

K J Donnelly
Comptroller and Auditor General

Northern Ireland Audit Office
8 June 2011

The Comptroller and Auditor General is the head of the Northern Ireland Audit Office employing some 145 staff. He and the Northern Ireland Audit Office are totally independent of Government. He certifies the accounts of all Government Departments and a wide range of other public sector bodies; and he has statutory authority to report to the Assembly on the economy, efficiency and effectiveness with which departments and other bodies have used their resources.

For further information about the Northern Ireland Audit Office please contact:

Northern Ireland Audit Office
106 University Street
BELFAST
BT7 1EU

Tel: 028 9025 1100
email: info@niauditoffice.gov.uk
website: **www.niauditoffice.gov.uk**

Contents

Part one	Introduction	1
Part two	Risk management framework	5
Part three	Risk management process	13
Part four	Accountability	29
Appendices		35
Appendix 1	Risk management checklist	36
Appendix 2	Participants	41
Appendix 3	HM Treasury – Key questions for an audit committee to ask	42
Appendix 4	Extract from DHSSPS communications plan	43
Appendix 5	Categories of risk	45
Appendix 6	Department for Regional Development - Risk checklist	47
Appendix 7	Department of Education - Assessment categories for impact and likelihood	49
Appendix 8	Model of risk appetite	56
Appendix 9	Strategic Investment Board – Fraud risk assessment	58
Appendix 10	OFMDFM stewardship statements pro forma	59

Glossary

Horizon scanning	the technique used to identify risks by a systematic examination of potential threats, opportunities and likely future developments, including (but not restricted to) those at the margins of current thinking and planning
Inherent risk	the exposure arising from a specific risk before any action is taken to manage it
Residual Risk	the exposure arising from a specific risk after action has been taken to manage it and assuming that the action taken has been effective
Risk appetite	the extent of exposure to risk that has been assessed as tolerable for an organisation or business activity
Risk Register	captures, maintains and monitors information on the risk to realisation of a specific objective and the associated control actions that have been put in place to mitigate that risk

Abbreviations

ALB	Arms Length Body
BAFO	Best and Final Offer
CE	Chief Executive
CGAC	Corporate Governance Audit Committee
DARD	Department of Agriculture and Rural Development
DE	Department of Education
DFP	Department of Finance and Personnel
ELB	Education and Library Board
EU	European Union
IT	Information Technology
MEMR	Monthly Expenditure and Monitoring Report
NAO	National Audit Office
NDPB	Non-departmental Public Body
NIAO	Northern Ireland Audit Office
NICS	Northern Ireland Civil Service
OFMDFM	Office of First Minister and Deputy First Minister
OGC	Office of Government Commerce
PDP	Personal Development Plan
PPA	Personal Performance Assessment
PSA	Public Service Agreement
RRG	Risk Review Group

Part One:
Intoduction

Part One: Introduction

1.1 Risk management is a highly topical issue for all government departments and their sponsored bodies and has a vital role to play in promoting and securing value for money in the use of public funds.

1.2 As a result of recent public spending cuts announced by Westminster, public bodies face greater challenges in managing risk. The cuts announced by the Chancellor of the Exchequer in the National Spending Review in October 2010 will result in a reduction of 8 per cent in the Northern Ireland Executive's delegated current expenditure limits by 2014-15. The delegated expenditure limit for capital investment available to the Northern Ireland Executive will reduce by 40.1 per cent in real terms by 2014-15. It is essential therefore, that public bodies adopt and embrace an innovative approach to managing risk to assist in the delivery of better, more cost effective public services.

1.3 There is currently a great deal of risk management guidance available, the essence of which is broadly similar. The purpose of this publication is to provide a best practice guide tailored to the experiences and needs of public sector bodies in Northern Ireland. The report reflects on local case study examples to illustrate how well risk is being handled in practice and to identify better and more innovative ways of managing risk.

1.4 In producing this report, we developed a risk management checklist (see Appendix 1), designed as a tool to enable public bodies to self assess their capability and capacity to manage risk. However, as a one-off exercise, we completed the checklist with all of the Northern Ireland Civil Service (NICS) departments and a number of Arm's Length Bodies, (see Appendix 2 for a full list). This exercise facilitated the identification of good practice in the application of risk management principles. This report examines good practice in the context of:

- the risk management framework (Part Two);
- the risk management process (Part Three); and
- accountability (Part Four).

1.5 Overall, we found that the departments had developed a strong awareness of risk and had made genuine efforts to develop and embed an effective risk management strategy. Traditionally public sector bodies display many of the characteristics associated with a highly risk averse culture, however, best practice guidance on risk management emphasises that the consequences of risk can be positive or negative. Well managed risk taking can produce benefits for the organisation in terms of opportunities, but equally can present threats that ultimately may impact on an organisation's ability to meet its strategic objectives. Risk management is an important aspect of good governance and is a useful tool in contributing to the achievement of outcomes and ensuring that public bodies meet their objectives as the following Case Study illustrates.

Case Study 1
Department of Education – Managing risk to achieve outcomes

Following substantial overspends in 2003-04 and 2004-05 by two Education and Library Boards (ELBs), the Department of Education (DE) introduced a series of measures to ensure tighter financial monitoring and control with the aim of preventing recurrence. This included the introduction of:

- a revised Monthly Expenditure and Monitoring Report (MEMR) to provide more relevant and detailed information;
- a signed assurance statement from the Chief Executive as to the accuracy of the information provided and a commitment to remain within budget;
- monthly meetings with each Chief Finance Officer to discuss in detail the information on the MEMR and reduce the risk of under/overspend at the year end;
- reconciliation and review of details provided in the MEMRs with details held in DE to reduce the risk of errors in figures being used by ELBs and DE; and
- keeping the DE Board informed to aid better decision making.

Following the implementation of these measures, the ELBs have remained within budget since 2004-05.

Source: Department of Education

Case Study 2
The Fermanagh Flooding – Managing risk to achieve outcomes

During the course of late October and November 2009, County Fermanagh experienced unprecedented levels of rainfall. The area was subject to widespread flooding, leading to significant disruption to life in the county at both individual and community level.
The Northern Ireland Executive decided, at its meeting on 3 December 2009, that a Flooding Taskforce should be established to investigate the causes of the flooding, identify lessons learned and consider measures required to mitigate the impact of any future flooding. This cross-departmental Taskforce gathered evidence from members of the public in the affected areas, business people, local representatives and stakeholder organisations. The Taskforce also took full account of the issues identified by a Review of the Flood Response conducted by the Rivers Agency, Department of Agriculture & Rural Development.

Part One:
Introduction

Following detailed examination of all the evidence the Taskforce presented a number of recommendations to the Northern Ireland Executive on 22 July 2010. These included:

- conducting an in-depth review of the Management of the Operating Regime for the Erne System;
- undertaking a programme of road improvement works;
- conducting a feasibility study to consider options for a flood alleviation scheme;
- undertaking a programme of work to improve the level of protection from flood risk;
- maintaining and further developing emergency planning arrangements and networks;
- ensuring that robust contingency arrangements are in place for the provision of essential services to the local community; and
- developing an education and public awareness programme to inform the local community about flooding in the Fermanagh area and how to deal with it.

The recommendations outlined above were approved by the Northern Ireland Executive on 22 July 2010 and Office of First Minister and Deputy First Minister advised us that considerable progress has since been made on their implementation.

Rainfall levels in County Fermanagh have not reached the unprecedented levels experienced in November 2009 since and the measures outlined above have not, therefore, been tested in a live environment. However, if these control measures prove to be effective, this case demonstrates the principles of effective risk management. As a result, any adverse impact on the community on the scale of that experienced in November 2009 should be averted.

Source: Department of Agriculture and Rural Development

Part Two:
Risk management framework

Part Two:
Risk management framework

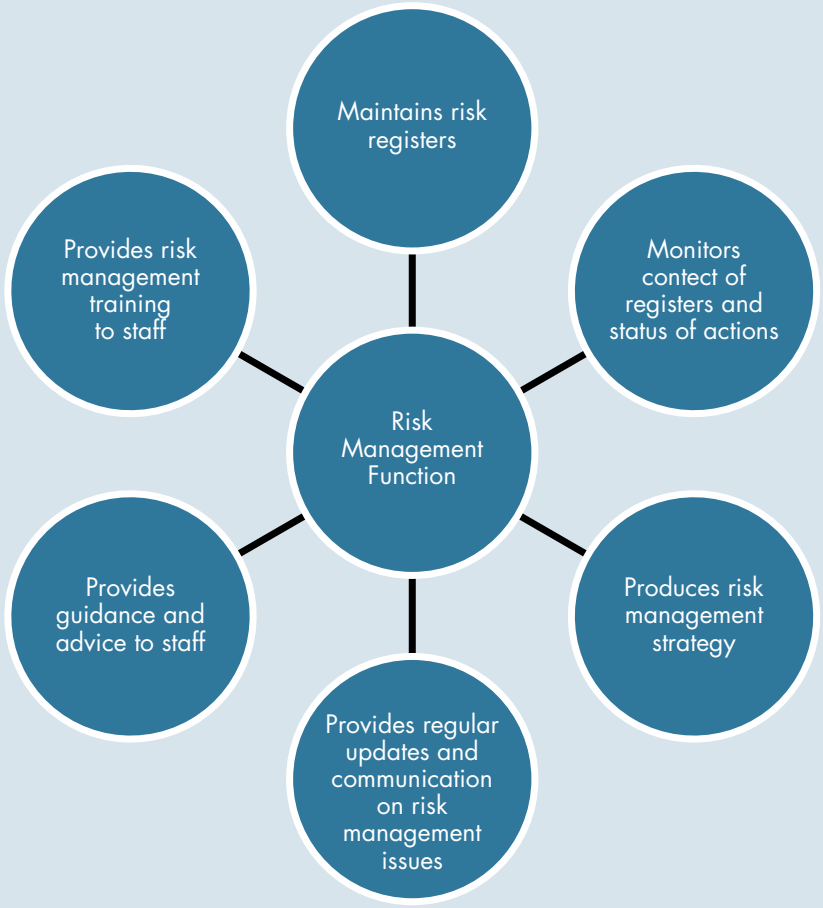
Risk management function

2.1 The structure of an organisation's risk management function will vary according to its size, nature and resource constraints. The risk management function may range from a single individual risk champion or manager to a whole risk management department. Figure 1 provides a summary of the roles and responsibilities that may be delegated to, and coordinated by, the risk management function.

Good Practice – Forums for exchanging knowledge and working practices

HM Treasury currently runs a risk improvement group that meets twice a year. This provides a good networking opportunity and enables attendees to meet experts in the field. Guest speakers are invited to attend the meetings and share experiences including case studies and guidance. The forum plays a useful role in spreading and embedding good practice.

Figure 1 – Risk management function: roles and responsibilities



Leadership

2.2 In public bodies the Accounting Officer has responsibility for maintaining a sound system of internal control that supports the achievement of policies, aims and objectives, whilst safeguarding the public funds and departmental assets. This involves putting a system in place to ensure that all business areas identify the key risks to the achievement of the organisation's objectives. The Accounting Officer must report annually on the organisation's system of internal control in the Statement on Internal Control. The statement should highlight any key internal control issues that have been encountered throughout that year.

2.3 Strong leadership and clear ownership at Accounting Officer level is essential in embedding an organisational risk management culture. An organisation's risk management strategy should outline clearly the roles and responsibilities for risk management, including that of the Accounting Officer.

2.4 In addition, the corporate governance framework of public sector bodies will include a Board, an Audit Committee and an internal audit service, all of which will assume some responsibility for seeking and providing assurance in relation to risk management. The management of risk however, always remains an executive responsibility.

2.5 According to HM Treasury guidance, "the Board should ensure that effective risk management arrangements are in place to provide assurance on risk management, governance and internal control".[1] Depending on an organisation's circumstances it may choose to establish a separate risk committee. However, frequently the role of the Audit Committee will be extended to include seeking assurances in relation to risk management. For this reason the Audit Committee is sometimes referred to as the Audit and Risk Committee. The Audit Committee will support the Board and the Accounting Officer by gathering assurance and providing advice to the Board on risk management, governance and control issues. HM Treasury guidance reflects that, "the Audit Committee is charged with ensuring that the Board and Accounting Officer of the organisation gain the assurance they need on risk management, governance and internal control".[2] The guidance provides a list of questions that an Audit Committee may wish to ask in seeking assurance on risk management issues (Appendix 3). It is essential, however, that audit committees maintain their independence and do not become operationally involved in risk management.

2.6 Internal Audit should adopt a risk based approach to planning its programme of work which will refer to organisational risk registers to identify topics for review. In addition to individual audit reports, Internal Audit provides an independent opinion on the overall adequacy and effectiveness of the framework of governance, risk management and internal control which should support and inform the Accounting Officer's Statement on Internal Control.

1 HM Treasury guidance - Corporate governance in central government departments: Code of Good Practice.
2 HM Treasury – Audit Committee Handbook.

Part Two:
Risk management framework

Figure 2 – Risk management in practice: roles and responsibilities

Accounting Officer	• Retains ultimate responsibility for the organisation's system of internal control and ensures that an effective risk management process is in place and is regularly reviewed • Provides clear direction to staff • Establishes, promotes and embeds an organisational risk culture • Reports to the Board and the Audit Committee
Board	• Establishes and oversees risk management procedures • Endorses the risk management strategy/policies • Ensures appropriate monitoring and management of significant risks by management • Challenges risk management to ensure that all key risks have been identified • Is aware of any instances where risks are realised
Audit (& Risk) Committee	• Reports to the Board on the effectiveness of the system of internal control and alerts the Board members to any emerging issues • Endorses the organisation's risk management strategy/policies • Takes responsibility for the oversight of the risk management process • Reviews risk registers to provide challenge and advice (not in an executive capacity)

Senior Management	• Acts on behalf of the Board and will:
	  • determine the organisation's approach to risk management
	  • implement policies on risk management and internal control
	  • discuss and approve issues that significantly affect the organistion's risk profile or exposure
	  • continually monitor the identification and management of significant risks and ensure that actions to remedy control weakness are implemented
	  • report changes in risk assessment to the Board on an exception basis
	  • annually review the organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures
	  • report to the Audit Committee and to the Board on risk management matters
	• Provides subsidiary management/internal control statements to the Accounting Officer

Risk Owner	• Identifies and assesses individual risks • Decides whether a risk is sufficiently serious to be escalated to the next level of the organisation • Ensures that actions to treat or control the risk are carried out and informs the risk manager of any consequent updates to the risk register • Reviews the risk rating and the necessity to keep the risk on the register

Risk Management Function e.g. risk champion/ manager/co-ordinator/ department	• Maintains the risk register under the direction of risk owners and updates or amends the risk register as necessary • Regularly reviews the content of risk registers with a view to ensuring that risk actions are being completed and that all details on the risk register are correct
Staff	• Carry out risk actions identified and delegated by the risk owners • Maintains awareness of the organisation's risk management strategy and the key risks faced by the organisation • Ensures that duties relating to controls are carried out
Internal Audit	• Provides independent opinion on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and internal control to the Accounting Officer (and Audit Committee)

Risk management strategy and policies

2.7 Public bodies should document formally their approach to risk management in a risk management strategy. This will assist the Accounting Officer, the Board and the senior management team in promoting and embedding risk management in the culture of the organisation. The risk management strategy will usually be published in a separate document but may be integrated with established policies for departmental business activities. Regardless of how organisations choose to present their risk management strategy, there are a number of key issues that should be addressed.

1. The strategy should outline the organisation's approach to risk management and should define its risk appetite.

2. The roles and responsibilities for the management and ownership of risk should be documented to ensure that all staff have a clear understanding of their remit.

3. The risk management process adopted by the organisation should be clearly outlined in the strategy.

4. The strategy should define how risks will be evaluated or ranked. This should assist in identifying key risks.

5. Risk registers should be regularly reviewed and this process should be identified in the strategy.

6. The process for monitoring and reviewing risk management procedures should be documented.

7. The process by which the Accounting Officer satisfies himself/herself that there is an adequate system of internal control in place should be outlined in the strategy.

Part Two:
Risk management framework

2.8 The risk management strategy is a key document which should underpin the organisation's risk management culture. It is essential, therefore, that it is endorsed by the Accounting Officer, the Board and the Audit Committee given their respective roles and responsibilities in relation to risk management.

Good Practice - Risk management guidance

In addition to its risk management strategy, the Department of Justice has produced 'a practical guide' to risk management which aims to assist staff in interpreting the guidance and addresses common issues. The Department informed us that this document is made available to all staff and supplements any training provided. The guide is user friendly and would be of particular benefit to those staff who may not have direct responsibility for risk management, but need to be aware of the key concepts.

Communicating the risk management strategy

2.9 Once the risk management strategy has been approved by the Board, (any subsequent updates should also be approved by the Board) it is essential that the document is publicised throughout the organisation and made available to all staff. This can involve holding training sessions tailored to the needs of different levels of staff throughout the organisation, sending out updates by email and publishing the document on the organisation's intranet. One of the key ways of gaining staff buy-in is for senior management to promote the importance of risk management. This might involve senior management facilitating staff meetings and delivering risk awareness sessions to staff.

Good Practice – Embedding risk management

Embedding effective risk management processes across the Department for Social Development and its sponsored bodies is a continuous process rather than a one-off annual exercise. It has involved looking below the surface of policies and procedures to identify what is actually happening on the ground. Taking on board the principle that this affects a wide range of people, the Department has adopted an all inclusive process driven by the Board and the Audit Committee. People are engaged continually through ongoing support and challenge by a dedicated team of staff. Recognising the benefits that a separate set of views can bring, a peer review process has been used to obtain an external perspective on risk management arrangements. To ensure continual refreshment of the process, managers from across the Department and its sponsored bodies have been brought together for a series of externally facilitated workshops to provide time for reflection, an opportunity to challenge each others' thinking and to assess the adequacy of current risk management arrangements in the context of identified good practice outside the NICS. The workshops provided a forum for sharing knowledge and experience and the output informed the ongoing review of the Department's risk management strategy. This included the involvement of staff in the development of definitions to help build

consistency in the risk assessment process which has helped to keep risk management at the forefront of decision-making.

Source: Department for Social Development

Contingency and business continuity plans

2.10 It is essential that public services can be maintained in the event of a disaster. Contingency planning is therefore vital in ensuring that the negative impact associated with risks occurring is managed and that there is minimal interruption to service delivery. Contingency plans should be put in place and regularly reviewed and tested to ensure that they provide adequate cover in the event of a disaster.

2.11 Due to the nature of the public sector, the services it provides, and the way in which it is funded, public bodies must manage reputational risk. Risk cannot however be eliminated entirely and there will always be a residual risk to the reputation of an organisation in the event of a risk maturing. In order to minimise the potential impact that this may have, public bodies should ensure that they are well equipped to deal with the event. This involves developing a communications strategy and providing training to relevant staff on its application.

2.12 We asked departments to comment on and provide a copy of their communications strategy. A significant number of the public bodies we reviewed referred us to their risk management strategy which did not, in our view, deal adequately with external communications. The Department of Health, Social Services and Public Safety has developed a communications plan as an annex to its business continuity plan which focuses on the external aspects of communication. The plan identifies a list of questions for consideration when devising a communications strategy in response to an event that may impact adversely on the organisation and a summary of the key steps that should be applied. An extract from the plan is provided at Appendix 4.

Arm's length bodies

2.13 Risk management is an important aspect in the governance of arm's length bodies (ALBs). HM Treasury guidance indicates that effective risk management needs to give full consideration to the context in which the department functions and to the risk priorities of partner organisations. For example, departments delegate aspects of service delivery to ALBs. If ALBs fail to manage these delegated risks appropriately this could impact on the department's achievement of objectives. In addition, any reputational risk faced by an ALB can also impact on the reputation of the sponsoring department. It is essential therefore, that departments seek assurances that their ALBs are managing risk at an acceptable level. Managing Public Money Northern Ireland states that 'the Accounting Officer of a department which sponsors an ALB should make arrangements to satisfy himself/herself

Part Two:
Risk management framework

that the Accounting Officer is carrying out his/her responsibilities'.

2.14 The approach adopted by departments will be influenced by the number of ALBs they provide funding to and the risk profile of those ALBs. Departments and ALBs need to work together to identify shared risks and develop appropriate efficient risk management approaches. Departments should regularly review the risk profile of their ALBs and ensure that appropriate and effective risk management processes are in place, including:

- structured processes for identifying and managing risks associated with departmental sponsorship responsibilities;
- regular review of processes for gaining assurances on ALBs' management of risks to ensure that appropriate and effective controls are in place; and
- regular and open discussion of risk issues between departments and their ALBs.

2.15 Departments have developed a number of techniques for gaining assurances on the governance and risk management of their ALBs.

Good Practice – managing risks in arm's length bodies

- The Accounting Officer of each ALB is required to complete an annual 'Subsidiary Statement on Internal Control' confirming that risks within their organisation have been identified, evaluated and managed appropriately. This statement is timed to support the departmental Statement on Internal Control which will reflect any significant control failures reported within ALBs.
- The head of Internal Audit in each ALB provides an annual opinion on the adequacy of the organisation's risk management, control and governance process. This report should be timed to support the Accounting Officer in each ALB prepare his/her Statement on Internal Control.
- Training is provided for Board members of ALBs on their roles and responsibilities.
- The Department attends in an observer capacity at the meetings of the ALB's Audit and Risk Committee to ensure alignment of risks, monitor the effectiveness of systems in place and maintain awareness of key risks.
- ALB representatives attend the departmental Audit and Risk Committee in an observer capacity on matters which impact on both, to offer reassurance that appropriate governance arrangements are in place and working.
- Procedures are documented and embedded to ensure that new risks identified in the ALBs are escalated to the Department on a timely basis.

Part Three:
Risk management process

Part Three:
Risk management process

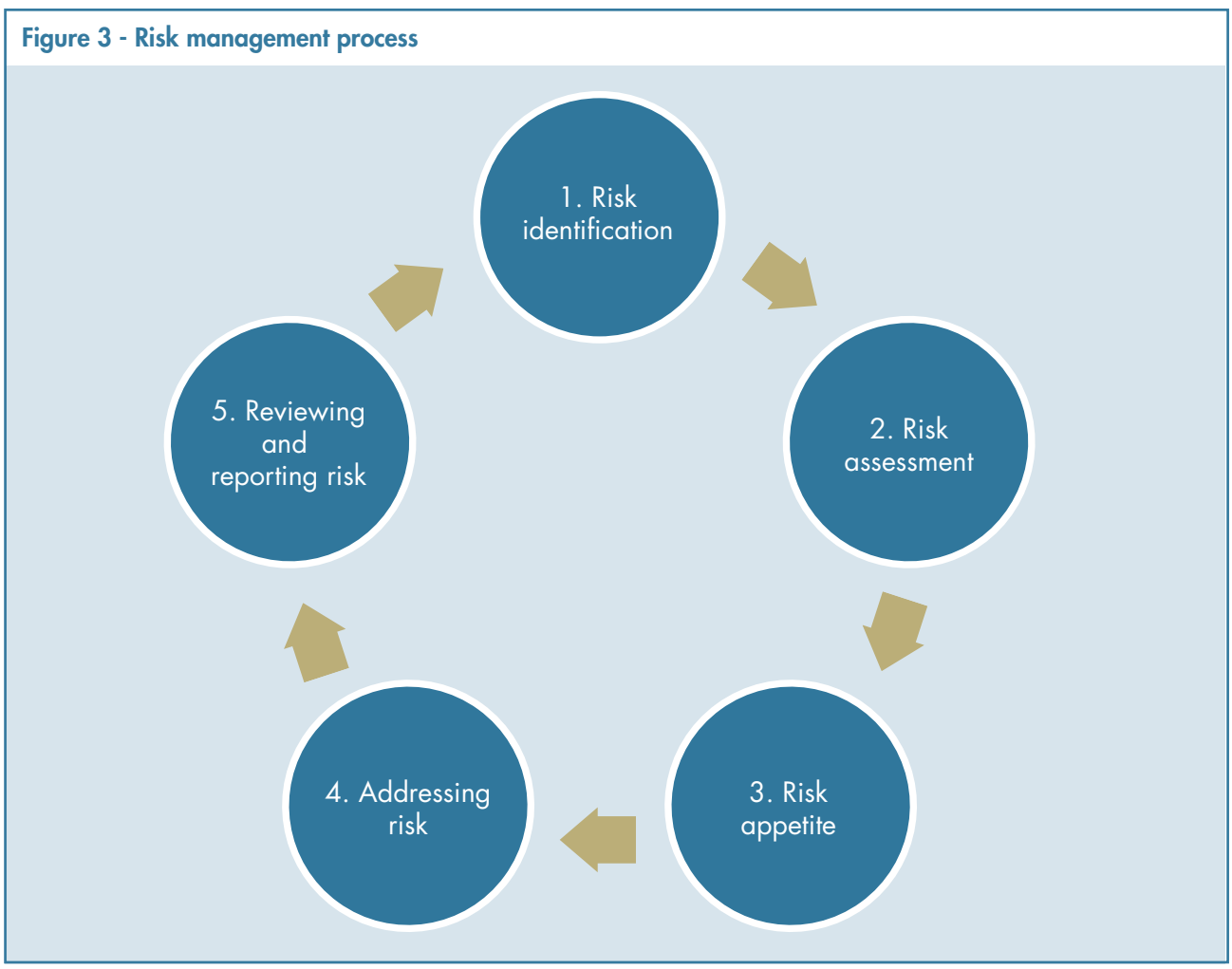
3.1 There is no one size fits all approach to the risk management process for public sector bodies. However, all risk management processes should incorporate five core stages and these should be outlined in the risk management strategy.

Step 1: Risk identification

3.2 Risk identification is the process of identifying risks which may impact on the organisation's ability to achieve its objectives. The aim is to identify what, when, where, why and how events could prevent, degrade, delay or enhance achievement of objectives. Appendix 5 provides a breakdown of the 3 main categories of risk which includes:

- external risks;
- operational risks; and
- change risks.

Figure 3 - Risk management process



3.3 Risk identification should be approached in a methodical way to ensure that all significant activities within the department have been identified and all risks flowing from these activities defined. Risk should always be related to objectives. Departments use a number of methods for identifying risks including facilitated workshops, brainstorming, using past experience, audit reports such as internal audit, NIAO and other audit institutions. As part of its risk management procedure manual the Department for Regional Development has compiled a risk checklist as a tool to facilitate the consideration of risk for any business activity. Although not exhaustive it provides a starting point for business areas to assess risk (see Appendix 6).

3.4 A number of departments also use a technique called "horizon scanning" which identifies risks that are likely to arise in the future. Horizon scanning is defined by the Government Office for Science as *'the systematic examination of potential threats, opportunities and likely future developments, including (but not restricted to) those at the margins of current thinking and planning.'*

3.5 The identification of risk can be separated into 2 stages:

Initial risk identification should be completed by those bodies which have not previously identified risks in a structured way, new organisations, or when an organisation undertakes a new project or activity.

Continuous risk identification is a process of review to identfy new risks as they arise, changes to existing risks, or eliminate risks which are no longer relevant.

3.6 In the current economic climate it is particularly important that public sector bodies are responsive to changes in their operating environment. Organisations must engage in the process of continuous risk identification to identify and manage threats to the business that may arise as a result of changes to the operating environment. The process should not only involve identifying new risks, but should incorporate a review of the documented risks which may no longer be valid or which may have been fully addressed. These risks should be removed from the risk register. Frequently, organisations add new risks to the register but fail to remove risks that have been addressed and that are no longer current. This can result in:

- the risk register providing an inaccurate profile of the organisation's corporate risks;
- the risk register becoming 'cluttered' with risks that are no longer current, making it difficult to identify the most significant strategic level risks faced by the organisation; and
- the risk register becoming burdensome to maintain and review.

3.7 Risk assessment and management should be a routine element of all policy development and implementation. Risks

Part Three:
Risk management process

considered should not only include those which threaten the achievement of objectives, but also those of failing to identify and exploit opportunities to do things differently or better (missed opportunities).

Risk ownership

3.8 Public bodies must establish appropriate accountability arrangements to provide assurances on risk management to the Board and the Audit Committee. This will involve assigning each of the risks identified to an owner who will be responsible for ensuring that the risk is managed and monitored over time. In order to promote accountability, risk owners should be named individuals and not groups, for example 'Finance Director' rather than 'Senior Management Team'.

3.9 Ownership of *key strategic risks* will usually be assigned at senior management/Board level. The ownership of *operational risks* will be allocated to head of division or head of branch level depending on the nature of the identified risk and the potential impact on business. These risks may not be included on the corporate risk register or reported to the Audit Committee. In promoting the need for accountability, organisations should link the ownership of risk to an individual's performance objectives.

3.10 It is essential that risk owners receive the support they require in order to manage those risks that have been assigned to them and that they have the authority to assign resources to manage key risks. They will be responsible for ensuring the risk framework is applied at all levels throughout their business area.

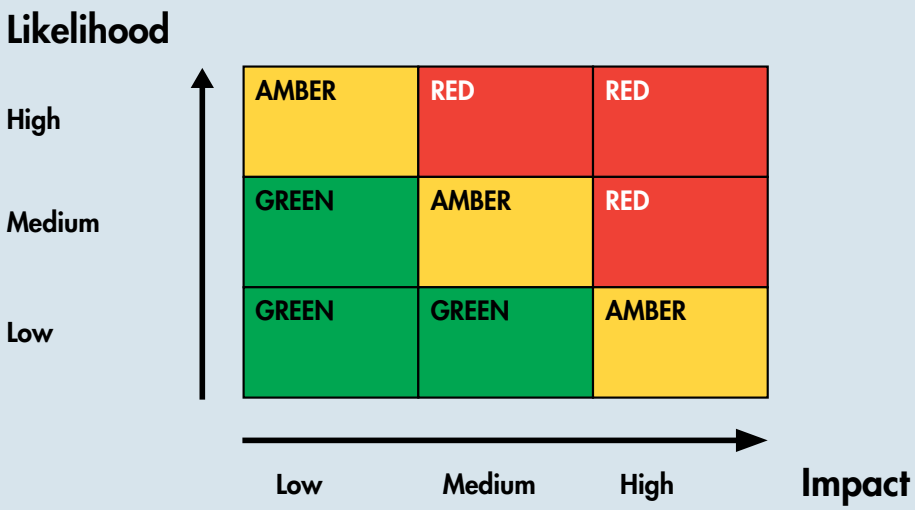
Step 2: Risk assessment

3.11 The next step in the process is to assess the "***inherent***" risk to a organisation's activity. Inherent risk can be described as the exposure arising from a specific risk before any action is taken to manage it.

3.12 This involves assessing the 'likelihood' of a risk occuring and its potential 'impact' on the relevant business objective. The impact and likelihood of risks occuring will be reassessed later in the risk management process (step 4) to reflect how the risk exposure has changed as a result of the risk response. This is referred to as "***residual***" risk and can be described as the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

3.13 As a minimum the impact and likelihood should be assessed as high, medium or low in a simple 3x3 risk matrix as illustrated in figure 4. A more detailed analytical scale can be applied if appropriate: Appendix 7 shows how the Department of Education has developed its own model. Each department should reach a judgement about the level of analysis that is most suitable for its circumstances.

Figure 4 – Simple 3x3 risk assessment matrix



3.14 This initial risk assessment focuses on inherent risk. Once organisations have completed step 4 in the risk management process the risk will be reassessed to identify the residual risk. Figure 5 provides an example of how this information might be presented in a risk register.

Figure 5 – Extract from risk register

Risk	Inherent Risk Assessment (Impact/ Likelihood)		Risk Response	Residual Risk Assessment (Impact/ Likelihood)	
Project deadline will not be met.	H	H	**Controls:** 1. Project Board established and Senior Responsible Owner identified to manage project 2. Regular monitoring of reported progress against milestones 3. Contract penalites for project overruns	M	L

Part Three:
Risk management process

Step 3: Risk appetite

3.15 An organisation's risk appetite is the extent of exposure to risk that is judged tolerable for that organisation. The concept may be looked at in different ways depending on whether the risk being considered is a threat or an opportunity.

- When considering threats, risk appetite clarifies the level of exposure which is considered tolerable and justifiable should it be realised. 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; or

- When considering opportunities, risk appetite clarifies how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. It is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

3.16 Some risks are unavoidable and it is not always within the ability of the organisation to manage risk to a tolerable level – for example, many organisations have to accept that there are risks arising from terrorist activities, extreme weather, industrial action etc which they cannot control. In this case the organisation needs to make *contingency plans* to minimise any potential negative impact of a risk maturing.

Setting the risk appetite

3.17 Risk appetite will best be expressed as a series of boundaries, appropriately authorised by management, which give each level of the organisation clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it. Risk appetite will be expressed in the same terms as those used in assessing risk. An organisation's risk appetite is not necessarily static; in particular the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time. Risk appetite should be considered at different levels including:

- corporate risk appetite;

- delegated risk appetite; and

- project risk appetite.

Appendix 8 explores these concepts in more detail in a model of risk appetite that was developed by HM Treasury.

Applications of risk appetite

3.18 As part of its procedure manual the Department for Regional Development has developed a grid (see figure 7) which identifies how risk appetite will influence the behaviour of decision makers when considering the various categories of risk.

Figure 7: Department for Regional Development: Risk appetite and categories

	Averse	**Open**	**Hungry**
	Avoidance of risk and uncertainty or for safe options that have a low degree of inherent risk and may only have limited potential for reward is a key objective.	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.	Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risk).
Category of Risk	*Example behaviours when taking key decisions…*		
Reputation, Political and Societal	• Minimal tolerance for any decisions that could lead to scrutiny of the Department or Agency is limited to those events where there is little chance of any significant repercussion should there be a failure	• Appetite to take decisions with potential to expose the Department or Agency to additional scrutiny but only where appropriate steps have been taken to minimise exposure	• Appetite to take decisions which are likely to bring scrutiny of the Department or Agency but where potential benefits outweigh the risks
Operational	• Defensive approach to objectives – aim to maintain or protect, rather than to create. Innovations generally avoided unless necessary • Priority for tight management controls and oversight with limited devolved decision making authority • Decision making authority generally held by senior management • General avoidance of systems/technology developments. Occasional developments are limited to improvements to protection of current operations	• Innovation supported, with demonstration of commensurate improvements in management control • Systems/technology developments considered to enable operational delivery • Responsibility for non-critical decisions may be devolved	• Innovation pursued – desire to 'break the mould' and challenge current working practices • New technologies viewed as a key enabler of operational delivery • High levels of devolved authority – management by trust rather than tight control

Part Three:
Risk management process

Category of Risk	*Example behaviours when taking key decisions…*		
Financial	• Avoidance/limited financial loss is a key objective • Only willing to accept the low cost option • Resources withdrawn from non-essential activities or restricted to core operational targets	• Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level • Value and benefits considered (not just cheapest price) • Resources allocated in order to capitilise on potential opportunites	• Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place). • Resources allocated without firm guarantee of return – 'investment capital' type approach
Compliance – legal / environmental	• Avoid most things which could be challenged, even unsuccessfully • Limited tolerance for sticking neck out. Would want to be reasonably sure of successful outcome of any challenge • Play safe	• Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences	• Chances of losing are high and consequences serious. But a win would be seen as a great coup

Step 4: Addressing the risk

3.19 There are four standard traditional responses to addressing risk (see figure 8). The choice of approach taken will depend on factors such as cost, feasibility, probability and potential impact. By addressing the risks identified, organisations can constrain threats and take advantage of opportunities.

Figure 8: Actions to address risk

Terminate	A decision is made not to take the risk or cease the activity which causes the risk. Where the risks outweigh the possible benefits, risk can be terminated by doing things differently and thus removing the risk, where it is feasible to do so. This is not always possible in the provision of public services or mandated or regulatory measures but the option of closing down a project or programme where the benefits are in doubt must be a real one. **For example, DFP took the decision to terminate Procurement for the Workplace 2010 programme when it became apparent in late 2008 that the prevailing conditions in the financial markets meant that it would be extremely difficult for bidders to raise the finance required to fund the project. This, coupled with the fact that the two companies shortlisted to submit best and final offers (BAFOs) announced a possible merger during the BAFO process, meant there was a serious risk that value for money could not be achieved on the project.**
Tolerate	Accept the risk. This may be where the risk is external and therefore the opportunity to control it is limited, or where the probability or impact is so low that the cost of managing it would be greater than the cost of the risk being realised. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised. **For example, cuts in departments' budgets presents a serious risk to the delivery of some services. However, cuts to budgets are outside the control of public bodies and departments must accept the cuts and develop a plan for dealing with the loss of resources.**
Transfer	Where another party can take on some or all of the risk more economically or more effectively. For example, through another organisation undertaking the activity or through obtaining insurance. It is important to note that some risks are not (fully) transferable - in particular it is generally not possible to transfer reputational risk even if the delivery of the service is contracted out. The relationship with the third party to which the risk is tranferred needs to be carefully managed to ensure successful transfer of risk. **For example, PPP projects such as the Roads Service Westlink project and the Department of Education's Pathfinders project are examples of where risk has, to some extent, been transferred to third parties.**
Treat	Mitigate the risk. In practice, this is the most common response to risk. It is achieved by eliminating the risk or reducing it to an acceptable level by prevention or another control action. **Case Studies 3 and 4 illustrate the steps taken by Invest NI to reduce risk to an acceptable level when supporting two manufacturing projects.**

Part Three:
Risk management process

3.20 Organisations may also want to exploit the opportunity that a risk presents and provided this is managed well, it should be encouraged. There are two aspects to this:

- at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages; and

- circumstances arise which, whilst not generating threats, offer positive opportunities for example, a drop in the cost of goods or services frees up resources which can be redeployed.

3.21 Invest Northern Ireland's (Invest NI) role is to grow the economy by helping new and existing businesses to compete internationally, and by attracting new investment to Northern Ireland. In order to deliver on its business objectives and support economic growth in Northern Ireland, Invest NI must embrace risk to a greater extent than other public sector bodies. Therefore, Invest NI will have a greater appetite for risk than other public sector bodies. While Invest NI has a unique outlook on risk as a result of its operating environment, there are lessons that can be learnt by other public sector bodies.

Case Study 3
Invest NI - Risk management in a successful project

Background: Invest NI provided approximately £3.5 million of a £10 million investment to support a high technology manufacturing company in Belfast whose parent company had withdrawn its support. The project proposed the creation of 52 new posts, many of which would be filled by highly skilled PhD engineers and scientists.

Risk assessment: Invest NI undertook a risk assessment of the project and identified the project as high risk for the following reasons:

- Sales achievability - a functioning prototype had not achieved commercialisation;
- A specific technical issue in the manufacturing process required resolution;
- There was a dependency on customers to incorporate the company's product into their own products; and
- There was a reliance on a small number of key individuals.

Rationale for proceeding: Whilst the project was regarded as high risk, the appraisal identified the potential for significant commercial returns. The management team was assessed to be credible; a clear market opportunity had been identified and verified by a detailed market appraisal; an external technical appraisal identified there was a reasonable expectation that the Research and Development

required to develop the product was achievable; and it was checked and confirmed that the promoters had ownership of the intellectual property underpinning their product.

How Invest NI ensured that risk was reduced to an acceptable level: Reflecting the balance between project risk and the potential commercial return, Invest NI's financial assistance contained a significant element of ordinary share capital offering a return to the tax payer should the project be implemented successfully.

Use of pre-conditions (to be satisfied in full before any assistance could be paid) and general conditions offered clarity and surety around:

- access to, and rights over, intellectual property;
- evidence of introduction of cash by other investors;
- timely provision of management and year end accounts to Invest NI;
- restrictions on making loans, paying dividends and remuneration levels to directors and senior managers; and
- payment of financial assistance dependent on the achievement of specified milestones including the introduction of additional capital by the promoters.

Outcome of this project: The project, which was initiated in 2005, is currently the subject of a Post Project Evaluation. Whilst loss making, manufacturing operations continue at the premises, employment is in line with projections and the Research and Development objectives of the project have been largely met. On the basis of the latest funding round, there is evidence to suggest that the value of Invest NI's shareholding has increased measurably and there is the potential that Invest NI's investment can be re-couped either by additional external investment or further investment by existing shareholders.

How risk management contributed to the outcome: The risk element of this project was managed by maintaining a close relationship with the company; by ensuring that all pre-conditions were met before any payment of grant was made; that all general conditions were fully applied and met; and by regular monitoring of performance against targets and milestones, including receipt of copies of papers related to the company's Board meetings.

Source Invest NI

Part Three:
Risk management process (paragraph 1.4)

Case Study 4
Limiting exposure in an unsuccessful project through risk management

Background: A small and technically skilled management team established a company having previously worked at the Northern Ireland site of a large international organisation. The promoters had identified a number of complex software solutions for global markets. An estimated 80 jobs were to be created.

Invest NI provided grant support of some £85,000 and preference share capital of approximately £1.2m to the new venture to assist in the development of a number of software applications to a marketable point.

Risk assessment: As a start up venture with no track record and substantial Research & Development to carry out, the project was regarded as high risk, for the following reasons:

- whilst some applications were technically feasible and market ready, no sales had been achieved to date;
- further products required substantial development;
- reliance on 3rd party joint ventures and alliances to develop market opportunities;
- time slippage;
- management – technically able but lacking in commercial experience and acumen; and
- cash flow and funding – the company required skilled and expensive engineers to develop and support the software applications.

Rationale for proceeding: Whilst the project was regarded as high risk, independent commercial appraisal identified a credible market opportunity.

The company had secured venture capital funding and a number of products were market ready. The management team had been strengthened and Invest NI had structured its investment to minimise risks.

How Invest NI ensured that risk was reduced to an acceptable level: Invest NI supported the project by convertible redeemable preference shares offering a return to the tax payer and an option to convert to ordinary share capital. Invest NI funds were released in tranches against specified milestones such as the introduction of match funding from the promoters and securing additional bank funding.

The management team was strengthened by the introduction of marketing expertise and an experienced company chairman.

Invest NI made its investment payments in tranches in order to ensure that sufficient progress had been made against product development objectives.

Outcome of this project: The project did not succeed as planned. Sales were slower than expected, cash flow became critical and the company was unable to complete a further funding round.

The company went into administration approximately three years after Invest NI's initial funding. Invest NI sought to recover monies paid to the company, but there were insufficient assets.

How risk management contributed to the outcome: Invest NI recognised that this project presented significant challenges. The technical skills of the promoters and employees were impressive and independent appraisals had confirmed the potential market opportunity. The project was closely monitored, which allowed Invest NI to limit its exposure when the risks became too great to add to.

The company's technology and business were subsequently taken on by a newly established company under new control. This company continues to trade successfully with a number of employees from the original company.

Source: Invest NI

Good Practice - Pursuing opportunities

- Organisations should give careful consideration to the opportunity that risks may present when designing their risk responses. The project identified in Case Study 1 was considered to be high risk however, this was outweighed by the potential opportunity that the project presented for the NI economy. The project has been very successful to date despite the initial risk assessment and this is due largely to risk being managed well.

- It is important to recognise that although risk may be managed well, a project may not achieve the desired outcomes. Provided there is sufficient evidence that risk has been managed appropriately, organisations should avoid a culture of blame but should take the opportunity to identify lessons that can be applied in the future.

- The case studies outlined above illustrate that projects may have entirely different outcomes despite managing risks in a consistent manner. This is because it is not possible to entirely eliminate risk; there will always be a level of residual risk that cannot be addressed. It is essential, therefore, that public bodies identify their risk appetite and minimise risk to an acceptable level.

- All projects should be subject to a post project evaluation to identify and promulgate any lessons learnt.

Part Three:
Risk management process

3.22 The option to "treat" in addressing risk can be further analysed into four different types of controls:

Preventative controls are designed to limit the possibility of an undesirable outcome being realised. The majority of controls implemented belong to this category. Examples include password access to computers, supervisory checks and independent authorisations on payments made to suppliers.

Directive controls are designed to ensure that a particular outcome is achieved. Examples include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff are trained before being allowed to work unsupervised.

Corrective controls (reversibility) are designed to correct undesirable outcomes which have been realised. Applied after the event, these may consist of contractual remedies to recover overpayments or obtain damages or a detailed contingency plan that will be triggered by an event (e.g. disaster recovery or business contingency plans).

Detective controls are designed to identify occasions of undesirable outcomes having been realised. By definition these are after the event, so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks, reconciliations, post implementation reviews.

3.23 HM Treasury's 'Orange Book'[3] emphasises that in designing controls, *"it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of human life) it is normally sufficient to design controls to give reasonable assurance of confining likely loss within the risk appetite of the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to constrain risk rather than eliminate it."*

3.24 Taking account of the controls that have been put in place organisations should repeat the earlier risk assessment in terms of likelihood and impact to identify the "**residual**" risk. This risk assessment will generally result in a lower rating for likelihood. The impact of a risk maturing can be reduced by putting in place a contingency plan that will address how the risk will be dealt with in the event of it maturing.

Step 5: Recording and reviewing risk

3.25 The risk management process is evidenced through the maintenance of risk registers. Risk registers should be maintained throughout the organisation at both operational and strategic level. The aim of the risk register is to capture, maintain and monitor information on the risk to realisation of a specific objective and the associated control actions that have been put in place to mitigate that

3 The Orange Book: Management of Risk – Principles and Concepts, HM Treasury, October 2004.

risk. Although each department will develop its own template for recording risk, the key components are as follows (see Appendix 7 for illustration):

- the business/corporate objective affected;
- details of risk(s);
- inherent risk assessment – impact and likelihood;
- risk response;
- residual risk assessment – impact and likelihood;
- planned action;
- target date; and
- risk ownership.

Risk registers are living documents which should be updated regularly.

Good Practice – Use of Information Technology

Many public bodies use Microsoft Excel to record and monitor their risk registers. The Department of Finance and Personnel (DFP) has developed and implemented a bespoke Information Technology system which records the department's targets, objectives and associated risks and is used to provide quarterly information to the Board and the Audit and Risk Committee. The application enables individual business areas to update departmental targets and risks and can also be used to monitor progress against business plans.

DFP identified a number of benefits of using this application:

- It provides the ability to link risks to business plan targets;
- It provides the ability for business areas to update the risk status and the controls and management actions that have been put in place to mitigate against the risks;
- It assigns risk owners at departmental board level for corporate risks;
- Risks can be escalated to divisional, directorate and departmental levels as appropriate; and
- It produces the corporate risk register which is provided to both the Board and the Audit and Risk Committee.

Fraud risk assessment

3.26 All organisations are subject to fraud risks and therefore should complete a fraud risk assessment on a periodic basis. A detailed fraud assessment needs to be performed by division and/or function. Functions and services that need to be included in the assessment are finance and accounting, human resources management (payroll), purchasing and contracting, and information technology. As a part of the assessment, organisations

need to look at the control environment and information technology, as both have a significant effect on fraud risk for most functions.

3.27 An effective fraud risk management assessment should identify where fraud may occur and who the perpetrators might be. Control activities should always consider both internal and external fraud.

3.28 A fraud risk assessment will include the same three key elements of any other risk assessment:

- *Identify inherent fraud risk* — Gather information to obtain the population of fraud risks that could apply to the organisation. Included in this process is the explicit consideration of all types of fraud scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organisation;

- *Assess likelihood and significance of inherent fraud risk* — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with relevant staff, including business process owners; and

- *Respond to reasonably likely and significant inherent and residual fraud risks* — Decide what the response should be to address the identified risks.

Appendix 9 provides a practical example of a fraud risk assessment.

Part Four:
Accountability

Part Four: Accountability

Responsibilities

4.1 With the right culture risk management should become inherent in the organisation's operations and in the roles and responsibilities of staff. In order to promote and embed such a risk management culture organisations should focus on the following key drivers:

- **Communication:** Everyone should be aware of the organisation's risk appetite, along with the corresponding policy, strategy and processes. Staff should be aware of the process to raise risk related issues which should be clearly documented and communicated. It is important that staff feel confident in raising risk related issues even when this may present negative impacts for the organisation. Staff must also be confident that any issues or concerns that they raise will be considered at an appropriate level and will, where necessary, be acted upon;

- **Leadership:** The Accounting Officer and senior managers have a key role in embedding the risk management culture. They should promote risk management through their own behaviours and actions by encouraging others;

- **Resource:** Risk owners should have the necessary resources at their disposal to implement risk responses. They should also be well equipped and supported to manage risk. This will involve providing the relevant training and access to risk management advice and expertise; and

- **Ownership and responsibility:** Risk management responsibilities should be clearly linked to personal objectives and to the performance appraisal system. Relevant staff should be empowered to take well managed risks in the knowledge that they will not be blamed for any negative outcomes providing risk has been managed in a way which is consistent with the organisation's risk appetite.

Governance

4.2 A public body's Board and Audit and Risk Committee have vital roles to play in the governance of risk management (see figure 2). In line with good governance, the Board should include non-executive directors and the Audit and Risk Committee should be chaired by a non-executive director. This should contribute to an independent review of the risk management strategy and the corporate risk register.

Good Practice – Risk review group

The Department of Agriculture and Rural Development (DARD) established a Risk Review Group (RRG) in June 2007 as a committee to coordinate and champion risk management and reporting of risk. The RRG is a sub group of the Corporate Governance Audit Committee

(CGAC), is chaired by a non-executive director and comprises representatives of all business groups within the department. It meets four times per year and reports back to the CGAC.

4.3 The public bodies that we reviewed indicated that the risk register was a standing item on the agenda of the Audit and Risk Committee and in most cases the full Board reviewed the corporate risk register either monthly or quarterly.

Good Practice – Provision of information to the Board

DARD currently prepares a risk commentary which is presented to and reviewed by the Board on a monthly basis. The risk commentary is coordinated by the Head of Financial Policy and commentary is sought from across all business areas. This process assists the Board in conducting a high level review of the corporate risk register on a regular basis.

Reporting

4.4 An organisation's system of internal control is designed to manage risk to an acceptable level. In accordance with Managing Public Money Northern Ireland, the Accounting Officer must report annually on the system of internal control by preparing and signing a Statement on Internal Control. The Statement on Internal Control should reflect on the system of internal control in operation in the department and its ALBs throughout the year, and should highlight any significant internal control weaknesses or failures.

4.5 In order to assist the Accounting Officer in fulfilling his or her responsibilities, departments indicated that they have put in place a process for stewardship reporting. In most cases this involves the head of each division in the core department, and the Accounting Officer in each ALB submitting a stewardship statement to the Accounting Officer at least biannually (in some cases quarterly). The stewardship statements should reflect any significant internal control issues in the relevant ALB or division and should be timed to support the Accounting Officer in his/her preparation of the Statement on Internal Control. The National Audit Office has produced guidance on the arrangements for the production of the Statement on Internal Control[4,5].

Good Practice - Stewardship reporting

The Office of the First Minister and Deputy First Minister (OFMDFM) recently redesigned and expanded its stewardship reporting process to address a wider range of governance and control issues and issued guidance on corporate/business area risk frameworks to staff. The framework provides a checklist for completion of quarterly stewardship statements which covers eleven key areas of risk (OFMDFM's pro forma stewardship statement is provided at Appendix 10).

In completing the stewardship statements, directors and Accounting Officers reflect on:

4 A Good Practice Guide to the Statement on Internal Control, National Audit Office, 2010
5 DAO (DFP) 02/10 The Statement on Internal Control a Guide for Audit Committees

Part Four: Accountability

- any findings emerging from recent internal audit reviews undertaken in the business area;
- findings emerging from the year-end audit of the department's Resource Accounts by NIAO;
- any control and approval issues highlighted by the Department of Finance and Personnel's annual review of consultancy spend;
- matters arising from in-year asset verification exercises; and,
- any issues that may have emerged in relation to the sponsorship of Non-departmental Public Bodies.

Significant internal control issues should be identified and commented on in the statement, including proposed remedial action to minimise the impact of identified risks materialising.

Assurance

4.6 HM Treasury Guidance states that *"assurance draws attention to the aspects of risk management, governance and internal control that are functioning effectively and the aspects which need to be given attention to improve them. Assurance helps a Board to judge whether or not its agenda is focussing on the issues that are most significant in relation to achieving the organisation's objectives and whether best use is being made of resources".*[6] There are a number of ways in which organisations might seek assurances that the risk management strategy and procedures in place provide an adequate level of assurance to their Board and audit committee:

- Internal Audit – conduct and report on an annual programme of work. The Head of Internal Audit will adopt a risk based approach to planning its work, referring to organisational risk registers in identifying topics for review. In addition to individual audit reports that the Head of Internal Audit will produce to record the audit findings of individual audit assignments, he/she will prepare an annual report giving his/her opinion on risk management, control and governance which is generally timed to support and inform the Accounting Officer's Statement on Internal Control. The annual report will provide an overview of the internal audit work undertaken throughout the year and will highlight any limited assurance ratings. HM Treasury Guidance highlights that, *"the work of Internal Audit is likely to be the single most significant resource use by the Audit Committee in discharging its responsibilities. This is because the Head of Internal Audit, in accordance with the Government Internal Audit Standards, has a responsibility to offer an annual audit opinion on the overall adequacy and effectiveness of the organisation's risk management, control and governance processes".*

Good Practice - Internal Audit review of the risk management process

As part of the Department of Culture, Arts and Leisure's recent review of its risk management framework it has introduced a requirement for Internal Audit to perform an annual review, with the objective of providing the Board and the Audit and Risk Committee with an opinion on the Department's risk management process and risk registers. This review will be timed to support the Accounting Officer in signing the Statement on Internal Control.

- External audit – will issue a report to those charged with governance as part of the year-end audit of the financial statements. This report will highlight any internal control or governance issues that have been identified during the external audit procedures.

- Other audit and verification exercises – public bodies may be subject to a range of additional audit, inspection and verification exercises as a result of the nature of their business and the funding that has been received. These exercises may result in other audit bodies bringing internal control issues to the attention of the Audit and Risk Committee and the Board.

- Statement on Internal Control – should be reviewed by the Audit Committee to ensure that the information presented in the statement is complete and accurately reflects other information relating to risk and internal control that has been presented to the committee throughout the year. National Audit Office published guidance in 'The Statement on Internal Control: A Guide for Audit Committees' in 2010.

- Self-assessment – it is recognised that it is good practice for Audit and Risk Committees to conduct a self assessment annually. National Audit Office published 'The Audit Committee Self-Assessment Checklist' in November 2009 and this includes a section on internal control.

Good Practice - National Audit Office

Audit Committee self-assessment – Internal control issues for consideration

- Does the Audit Committee consider whether corporate governance is embedded throughout the organisation, rather than treated as a compliance exercise?

- Does the Audit Committee consider whether the system of internal reporting gives early warning of control failures and emerging risks?

- Does the Audit Committee consider whether the Statement on Internal Control is sufficiently comprehensive and meaningful, and the evidence that underpins it?

- Does the Audit Committee satisfy itself that the system of internal control has operated effectively throughout the reporting period?

Part Four: Accountability

- Does the audit committee consider whether financial control, including the structure of delegations, enables the organisation to achieve its objectives and achieve good value for money?
- Does the audit committee monitor whether the organisation's procedures for identifying and managing business risk have regard for the relevant legislation and regulation?

- Third-party review – public bodies may seek independent assurance from third parties on their risk management process and risk registers.

Good Practice – Third party reviews

As part of a wider review of its risk management processes, the Department for Social Development recently engaged another NICS department to conduct a review of its corporate risk register. This worked well in practice as it provided an independent assessment of the risk register. Due to the similar nature of the body undertaking the review there was a common understanding of how risk management should be applied in the public sector environment.

The Department for Regional Development employed consultants to undertake a performance assessment of its risk management strategy. This exercise provided valuable lessons on how to apply best practice.

4.7 The assurance provided by the various methods identified above should assist the audit and risk committee in identifying where risk is:

- managed adequately and appropriately;
- controlled inadequately; or
- controlled excessively.

Where risks are managed adequately and appropriately no further action is required other than to monitor and review the risk. However, where a risk is controlled inadequately, measures to improve the risk response must be implemented. In the current economic climate there is an increasing pressure on resources. It is therefore essential that public bodies take a measured approach in managing risk and consider the cost/benefit that controls represent. Due to the traditionally risk averse nature of the public sector it is not uncommon to find excessive controls in operation. This can result in significant waste and by identifying such measures it may be possible to identify cost savings. The role of the Audit Committee is to advise the Board on such matters, to enable it to make an informed decision. The Audit Committee must, however, ensure that it maintains independence to avoid becoming involved in executive risk management responsibilities.

Appendices

Appendix 1
Risk management checklist (paragraph 1.4)

1. Risk Management Framework		
		Response
1.1	Does the organisation have an established risk management function, e.g. a risk champion, risk manager, risk management department, risk committee?	
1.2	How is risk management sponsored by the Accounting Officer, and responsibility shared with the Board and the Senior Management team?	
1.3	Is the organisation's approach to risk fully documented and widely distributed? (i.e. risk appetite)	
1.4	How has risk management been embedded in the following processes: – Performance management – Operational management – Financial management – Business planning	
1.5	How have the following contributed to the development of risk management within your organisation? – HM Treasury Orange Book – Internal Audit – External Audit – Other (please detail)	
1.6	Does the organisation have a risk management strategy and/or policy?	
1.7	Has the risk management strategy/ policy been endorsed by the Accounting Officer/Board/Audit and Risk Committee?	

1.8	How has the risk management strategy/policy been promulgated to staff?	
1.9	How often is the risk management strategy/policy reviewed? When was the strategy/policy last reviewed/updated?	
1.10	How does the risk management strategy promote the need for effective communication to all relevant stakeholders?	
1.11	How does the risk strategy/ policy outline how risk should be considered at each level, (strategic and operational), throughout the organisation?	
1.12	What process is in place for escalating risks throughout the organisation?	
1.13	Is there a contingency or business continuity plan in place? If so, how often is it tested?	
1.14	Is there an IT recovery plan in place If so, how often is it tested?	
1.15	Is there a communications strategy in place that can be applied in the event of risk maturing?	
2. Risk Management Process		
2.1	Are the responsibilities of all staff clearly defined and regularly reviewed?	

Appendix 1
Risk management checklist (paragraph 1.4)

2.2	Do risk registers record the following information: – Identified risks – Inherent risk assessment (impact and likelihood) – Response to risk – Residual risk assessment (impact and likelihood) – Risk ownership – Timescale for actions required	
2.3	Is there a risk register in place which has identified the risks to the organisation at a strategic (organisational) level?	
2.4	Are risk registers maintained at an operational (divisional) level?	
2.5	Are risk registers maintained at a project level or does evidence exist that risks are assessed for projects individually?	
2.6	How often are risk registers reviewed?	
2.7	What techniques are used by the organisation in identifying risks?	
2.8	How have the risks identified been linked to the objectives of the organisation?	
2.9	How have risks been ranked and prioritised for action?	
2.10	How regularly are the responses to key risks monitored?	
2.11	Who is responsible for monitoring the risks?	

2.12	Is there any early warning system in place to identify any threats that may contribute to the realisation of key risks?	
2.13	Is there a policy in place for managing the risks associated with working with partners at project level?	
2.14	How are risks associated with working with partners at project level identified and managed?	
2.15	What is the process in place for reviewing the risk assessment throughout the project lifecycle?	
2.16	How does the rigour of this process vary according to the size/duration/ profile of the project?	
2.17	What IT software does the organisation use in its risk management process?	
2.18	How is risk management incorporated into the organisation's training programme? Is risk management included in induction training for all new staff?	
2.19	Is there any form of ongoing risk communication across the organisation?	
2.20	Does the organisation maintain a risk database?	
3. Accountability		
3.1	Have responsibilities for identifying, managing and reporting risk been established? How regularly are these responsibilities reviewed?	

Appendix 1
Risk management checklist (paragraph 1.4)

3.2	Are responsibilities in relation to risk reflected in personal objectives and the performance appraisal system?	
3.3	What measures have the executive directors put in place for reporting on the risk management process to the Board and the Audit and Risk Committee?	
3.4	How frequently does risk management appear on the Board agenda?	
3.5	How does the Board/Senior Management team assure themselves that they have identified all of the organisation's risks?	
3.6	What references have been made to the risk management process in the annual report?	
3.7	Have any significant internal control issues relating to identified risks been highlighted in the Statement on Internal Control in recent years?	
3.8	How does the Internal Audit Service use the risk management framework when planning their work?	
3.9	How does the organisation ensure that systems of internal control are operating robustly?	
3.10	How does the organisation gain independent assurance on the effectiveness of its risk management process?	

Appendix 2
Participants (paragraph 1.4)

The following public sector bodies assisted our review by completing the risk management checklist.

1.	Department of Agriculture and Rural Development
2.	Department of Culture, Arts and Leisure
3.	Department of Education
4.	Department for Employment and Learning
5.	Department of Enterprise, Trade and Investment
6.	Department of Finance and Personnel
7.	Department of Health, Social Services and Public Safety
8.	Department of the Environment
9.	Department of Justice
10.	Department for Regional Development
11.	Department for Social Development
12.	Invest Northern Ireland
13.	Northern Ireland Assembly
14.	Northern Ireland Ombudsman and Commissioner for Complaints
15.	Office of the First Minister and Deputy First Minister
16.	Public Prosecution Service

Appendix 3
HM Treasury Audit Committee Handbook Key questions for an Audit Committee to ask (paragraph 2.5)

On the strategic processes for risk, control and governance, how do we know:

- that the risk management culture is appropriate?
- that there is a comprehensive process for identifying and evaluating risk, and for deciding what levels of risk are tolerable?
- that the Risk Register is an appropriate reflection of the risks facing the organisation?
- that appropriate ownership of risk is in place?
- that management has an appropriate view of how effective internal control is?
- that risk management is carried out in a way that really benefits the organisation or is it treated as a box ticking exercise?
- that the organisation as a whole is aware of the importance of risk management and of the organisation's risk priorities?
- that the system of internal control will provide indicators of things going wrong?
- that the Accounting Officer's annual 'Statement on Internal Control' is meaningful, and what evidence underpins it?
- that the Statement on Internal Control appropriately discloses action to deal with material problems?
- that the Board is appropriately considering the results of the effectiveness review underpinning the Statement on Internal Control?

On risk management processes, how do we know:

- how senior management and Ministers support and promote risk management?
- how well people are equipped and supported to manage risk well?
- that there is a clear risk strategy and policies?
- that there are effective arrangements for managing risks with partners?
- that the organisation's processes incorporate effective risk management?
- if risks are handled well?
- if risk management contributes to achieving outcomes?

Appendix 4
Department of Health, Social Services and Public Safety
Extract from communications plan (paragraph 2.12)

Devising a Communications Strategy

The following strategic questions are to be considered when devising the Communications Strategy.

- What is the nature of the event or incident that has occurred and has a commonly understood picture of the incident been reached?
- Does the incident point to a deeper issue or problem that could impact upon the reputation of the Department?
- Has the incident finished or is there potential for more to come and if so what are the time scales?
- How bad could this get and what is the most realistic worst-case scenario?
- What will our stakeholders (internal and external) make of this situation?
- What does the Department stand to lose because of this incident?
- What allies can the Department involve?

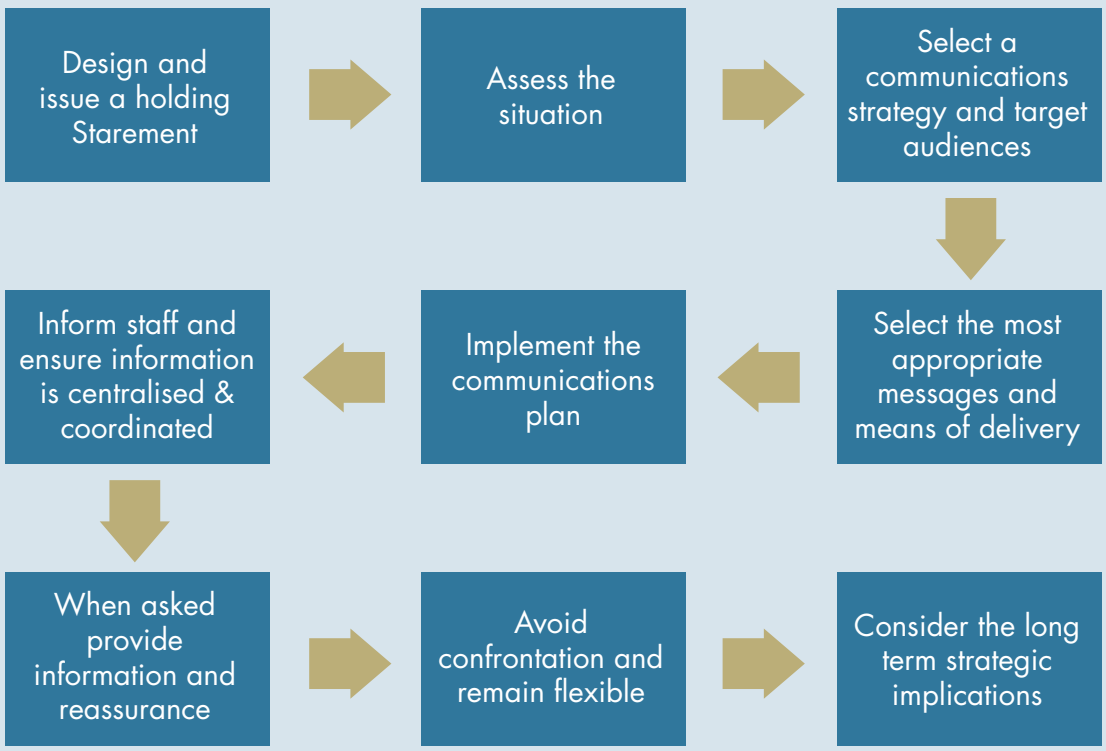
Key Message Checklist

The following should be considered in relation to message content and tone:

- Provide as much information on the incident that is available and verified as factual.
- Provide a human face that shows the Department cares.
- Provide reassurance that any risks have passed, or that action is underway to mitigate any risks and tell people what they too can do.
- Outline a solid history in regards to incidents and incident management.
- Provide details of when and how further information will be made available.
- Provide written background briefs on the Department outlining the role of the DHSSPS and its main services.
- Provide detailed evidence to back any claims made.

Appendix 4
Department of Health, Social Services and Public Safety
Extract from communications plan (paragraph 2.12)

The following steps form a useful guide for Communications Planning:



Appendix 5
HM Treasury Orange Book Categories of risk (paragraph 3.2)

External (arising from the external environment, not wholly within the organisation's control, but where action can be taken to mitigate it)	
Political	Change of government; cross cutting policy decisions; machinery of government changes (eg devolution)
Economic	Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect of global economy on NI economy
Socio-cultural	Demographic changes affects demand for services; stakeholders expectations change
Technological	Obsolence of current systems; cost of procuring best technology available; opportunity arising from technological development
Legal/regulatory	EU requirements/laws which impose requirements (such as health and safety or employment legislation)
Environmental	Buildings need to comply with changing standards; disposal of rubbish and surplus equipment needs to comply with changing standards
Operational (relating to existing operations – both current delivery and building and maintaining capacity and capability)	
Service/product failure	Fail to deliver the service to the user within agreed/set terms
Project delivery	Fail to deliver on time/budget/specification
Resources	Financial (insufficient funding, poor budget management, fraud) HR (staff capacity, skills, recruitment and retention) Information (adequacy for decision making, protection of privacy) Physical assets (loss,damage,theft)
Relationships	Delivery partners (threats to commitment to relationship, clarity of roles) Customers/service users (satisfaction with delivery) Accountability (particularly to the Assembly)
Operations	Overall capacity and capability to deliver
Reputation	Confidence and trust which stakeholders have in an organisation
Governance	Regularity and propriety/compliance with relevant requirements/ethical considerations
Scanning	Failure to identify threats and opportunities
Resilience	Capacity of systems/accomodation/IT to withstand adverse impacts and crises (including war and terrorist attack) Disaster recovery/contingency planning
Security	Of assets and information

Appendix 5
HM Treasury Orange Book Categories of risk (paragraph 3.2)

Change (risks created by decisions to pursue new endeavours beyond current capability)	
PSA targets	New PSA targets challenge the organisation's capacity to deliver/ability to equip the organisation to deliver
Change Programme	Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity
New projects	Making optimal investment decisions/prioritising between projects which are competing for resources
New policies	Policy decisions create expectations where the organisation has uncertainty about delivery

Appendix 6
Department for Regional Development – Risk checklist (paragraph 3.3)

A risk checklist is an in-house list of risks that were identified or occurred during previous organisational activities. They permit managers to capture lessons learned and assess whether similar risks are relevant to current activities.

This checklist should be used as a means of kick starting and facilitating discussions on risks which may impact on the achievement of business objectives. It should be noted that these risks are not exhaustive and it is expected that business areas will develop and tailor this to meet their own needs as specific business risks are identified. The checklist will be updated annually following input from Departmental Risk Coordinators.

People

- Will the business area have the personnel in place to meet business objectives?
- Does everyone know and understand their roles and responsibilities?
- Do we have clear Job Descriptions, PPAs and PDPs?
- Do we have the processes and procedures in place to facilitate recruitment?
- Do we know the knowledge, skills and experience required to do the job?
- Are staff appropriately trained to deliver business objectives?
- Are staff appropriately trained in navigating the HR Connect system?

Finance

- Has the achievement of the business objectives been effectively budgeted for in terms of financial resources?
- Are controls in place to monitor financial performance against business objectives?
- Does the business area have appropriate systems in place to report on financial performance?
- Are staff appropriately trained on Account NI procedures?

Data Management

- Can the business area be assured that personal details of staff and/or the public are sufficiently safeguarded?
- Does the business area have suitable data management/ICT systems in place?
- How does the business area store and transport confidential/sensitive information?
- Are passwords regularly changed and updated?
- Is everyone aware of the Departmental Data Management and Security arrangements?
- Are staff trained in using the TRIM system?

Appendix 6
Department for Regional Development – Risk checklist (paragraph 3.3)

Arms Length Bodies

- Does the sponsoring division have appropriate governance arrangements with its sponsor organisation?
- Is performance of the Arms Length Body monitored and reported to Senior Management in the Department?
- Are the objectives of the ALB in line with Departmental objectives?

Service Providers

- Is the business area content that its contracts and SLAs with service providers are adequate and reflect the needs of the Department?
- Is the behaviour and performance of Service Providers monitored and reported to Senior Management?

Policy Issues

- Are project management arrangements in place to ensure the effective and timely delivery of policy?
- Does the business area have political agreement for any policy decisions?
- Have the views of stakeholders and the public been factored in to the decision making process?

Emergency Planning

- Does the business area have adequate contingency planning arrangements in place in the event of an emergency?
- Are staff and/or the public (where appropriate) aware of the emergency arrangements?

Appendix 7
Department of Education - Assessment categories for impact and likelihood (paragraph 3.13)

Risk Evaluation - Impact

Category	Minor (low)	Moderate (low-medium)	Significant (medium)	Major (medium-high)	Critical (high)
Achievement of Objectives	No risk to DE demonstrating achievement of its key objectives (to deliver on time, within budget etc.). Failure to deliver more than one Directorate/ Programme level objective.	One or more key objective is only just delivered (eg. significant delay or a downward trend).	Failure to deliver one key objective.	Failure to deliver more than one key objective.	Failure to deliver the majority of DE key objectives (PSA's/Ministerial Priorities)
Operational Delivery	No interruption to service. Minor industrial protest.	Some disruption manageable by altered operational routine.	Disruption to a number of operational areas within a location and possible flow on to other locations.	All operational areas of a location compromised. Other locations may be affected.	Total system dysfunction. Total shutdown of operations.
Financial	Financial loss, loss of funding or inescapable unfunded pressures under £20K +/- 1% variance to budget.	Financial loss, loss of funding or inescapable unfunded pressures under £100K +/- 2% variance to budget. NIAO criticism	Financial loss, loss of funding or inescapable unfunded pressures under £250K +/- 5% variance to budget. NIAO qualification of accounts Fraud, corruption and serious irregularity below SCS or within NDPBs.	Financial loss, loss of funding or inescapable unfunded pressures under £500k +/- 10% variance to budget. NIAO qualification of accounts Fraud, corruption and serious irregularity at SCS or NDPB Senior Management level.	Financial loss, loss of funding or inescapable unfunded pressures over £1m +/- 15% variance to budget. NIAO qualification of accounts Fraud, corruption and serious irregularity at Ministerial / Board or NDPB CE level.

Appendix 7
Department of Education - Assessment categories for impact and likelihood (paragraph 3.13)

Category	Minor (low)	Moderate (low-medium)	Significant (medium)	Major (medium-high)	Critical (high)
Compliance/ Regulatory/ Legal	Breach of local procedures not requiring external intervention/ sanction.	Breach of National Procedures/ Standards. Potential for minor legal challenge to DE.	Breach of subordinate legislation. Failure to comply with relevant guidance results in expenditure being deemed irregular. Potential for moderate legal challenge to DE. Potential for moderate legal challenge to DE.	Breach of Primary legislation. Potential for significant legal challenge to DE. Likelihood that damages will be awarded against DE or changes will be required to subordinate legislation to ensure compliance	Breach of national or international statutory duties. Legal challenge which halts delivery of policy. Major damages awarded against DE or changes will be required to primary legislation to ensure compliance
Security	Non-notifiable or reportable incident.	Localised incident. No effect on operations.	Localised incident. Significant effect on operations.	Significant incident involving multiple locations.	Extreme incident seriously affecting continuity of operations.
Health & Well-being	Isolated incident – no significant health impact.	Small number of minor injuries requiring first aid treatment.	Compensatable injury/stress.	Serious injury/ stress resulting in hospitalisation. Possible fatalities. Local Child Protection issue.	Fatality Widespread Child Protection Issue

Category	Minor (low)	Moderate (low-medium)	Significant (medium)	Major (medium-high)	Critical (high)
Reputational	Minor adverse publicity in local media Event that will lead to public criticism by external stakeholders as anticipated.	Significant adverse publicity in local media Increased Assembly/ Westminster scrutiny. Event that may lead to widespread public criticism.	Significant Assembly/ Westminster scrutiny Formal communication required with public. Significant adverse publicity in national media Incompetence/ maladmin-istration or other event that will undermine public trust or a key relationship for a short period.	Oral Statement Required in Assembly Sustained adverse publicity in national media. Incompetence/ maladmin-istration or other event that will undermine public trust or a key relationship for a sustained period or at a critical moment.	Ministerial/ Board/ CE (NDPB) / Senior Management resignation/ removal Incompetence/ maladmin-istration or other event that will destroy public trust or a key relationship.

Appendix 7
Department of Education - Assessment categories for impact and likelihood (paragraph 3.13)

Risk Evaluation - Likelihood	
Descriptor	**Detailed Description**
1. Unlikely (low)	>10% chance of occurrence. May occur only in exceptional circumstances. Has never occurred before within the remit of DE or any other Department. Unlikely to occur during the lifespan of the policy/programme/project/ operation.
2. Remote (low-medium)	11-30% chance of occurrence. Might conceivably occur at some time. More likely not to occur than to occur. Has not occurred recently within the remit of DE or any other Department. There is a small chance that this may occur at some stage during the lifespan of the policy/programme/project/ operation.
3. Possible (medium)	31-59% chance of occurrence. Could occur at some time. Has occurred recently within the remit of another Department. Might occur at some stage during the lifespan of the policy/programme/ project/operation.
4. Probable (medium-high)	60-84% chance of occurrence. Will probably occur in most circumstances. More likely to occur than not to occur. Has occurred recently within the remit of DE or another Department. Likely to occur within the next 1-2 years or during the lifespan of the policy/ programme/project/operation.
5. Almost Certain (high)	85% chance of occurrence. Is expected to occur in most circumstances. This is known to occur in similar projects and programmes. Happens frequently within the remit of DE or other Departments. Highly likely to occur within the financial year or lifespan of the policy/ programme/project/operation – probably early on and possibly more than once.

Risk Assessment Matrix

Impact							
	Critical	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Significant	3	3	6	9	12	15
	Moderate	2	2	4	6	8	10
	Minor	1	1	2	3	4	5
			Unlikely (>10%)	Remote (11-30%)	Possible (31-59%)	Probable (60-84%)	Almost Certain (85%+)
			1	2	3	4	5
	Likelihood						

Escalation Triggers

In order to ensure that risks are being managed at an appropriate level, there are a number of trigger points where risks should be escalated to specified levels of management as they approach or exceed their agreed risk appetite. These are set out below. **However, in *all* cases where a risk is assessed as 'Orange', it should be brought to the attention of the DE Board. In all cases where a risk is assessed as 'Red', it should be brought to the attention of the DE Board and Minister.**

Appendix 7
Department of Education - Assessment categories for impact and likelihood (paragraph 3.13)

Escalation Triggers

Risk Category	Risk Appetite	Acceptable Range (Up to and including)	Escalation
Health and Well-being	**Averse**	**Green**	Risks should be elevated to Director level for consideration if assessed as Amber or higher.
Financial/VFM Risks **Compliance/ Legal/ Regulatory Risks** **Information and Security**	**Modest / Cautious**	**Amber**	Risks should be elevated to Director level assessed as Amber or higher.
Operational and Policy Delivery Risks **Reputation and Credibility**	**Open/Hungry**	**Orange**	Regardless of the risk appetite, DE Board should be made aware of ***any*** Directorate Risks assessed as Orange and contingency plans should be developed.
		Red	Regardless of the risk appetite, DE Board and Minister should be made aware of ***any*** Directorate Risks assessed as red and advised immediately of any early warning signals that the risk may be realised. Contingency plans should also be developed and tested.

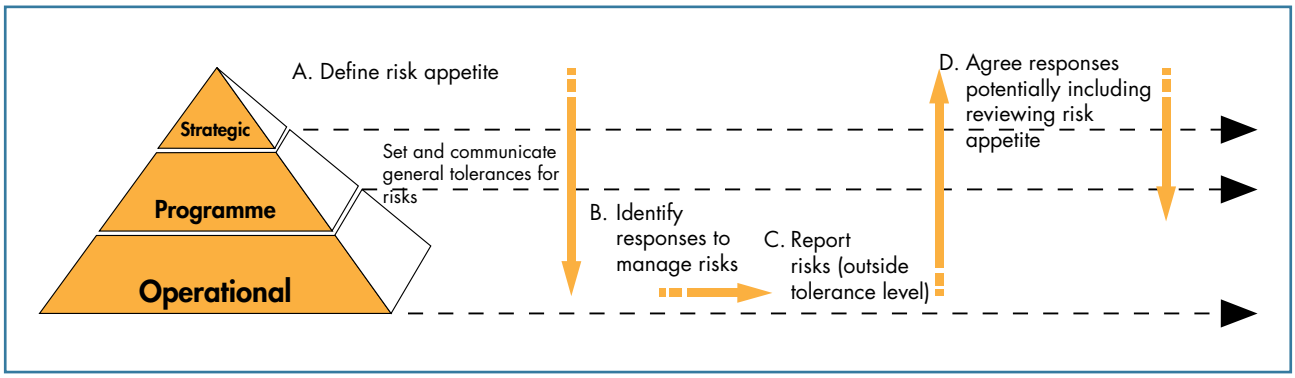
Example

- Team A identifies a risk to health and well-being that is assessed as having a residual risk score of 12. On the risk assessment matrix, 12 = Orange.

- The Department's risk appetite for risks to Health and Well-being is described as 'Averse'. Risks to Health and Well-being are therefore only at an acceptable level when they are assessed as 'Green'. Any risks in an area for which the Department's risk appetite is 'Averse' and which are assessed as higher than 'Green' should therefore be referred to the Director for consideration.

- In addition, any risks on the Directorate Risk Register which are assessed as 'Orange' should be drawn to the attention of the DE Board.

Appendix 8
HM Treasury Orange Book Model of risk appetite (paragraph 3.17)



Risk appetite can be further analysed into the following categories:

Corporate risk appetite is the overall amount of risk judged appropriate for an organisation to tolerate (point A). This may not be just one statement: The Office of Government Commerce (OGC), for example, look at 5 key risk areas (policy/guidance risk; people and internal systems risk; propriety, regularity, finance and accountability risk; reputation risk; external risk) and make a statement on risk appetite for each. The Board and senior managers should judge the tolerable range of exposure for the organisation and identify general boundaries for unacceptable risk (or at least for risks that should always be referred to/ escalated up to the Board for discussion and decision when they arise). In doing this the Board may want to take Ministerial views on risk-taking into account.

Delegated risk appetite The agreed corporate risk appetite can then be used as a starting point for cascading levels of tolerance down the organisation, agreeing risk appetite in different levels of the organisation (point B). The anticipated effect is that what is considered a high level of risk will become a lower level of risk to a higher level of management. This facilitates both a risk escalation process for the taking of risk decisions when delegated boundaries are met and empowers people to innovate within their delegations.

Project Risk Appetite Projects that fall outside of day-to-day business of an organisation may need their own statement of risk appetite. Different types of projects may require different levels of risk appetite, for example an organisation may be prepared to accept a higher level of risk for a project that would bring substantial reward.

Different types of project could be:

- Speculative (akin to venture capitalism in the corporate sector): with high risks but potentially high rewards, e.g. Invest to Save Budget projects; Pilot projects. It may be that the bulk of these projects are unsuccessful but important lessons are learnt;
- Standard development projects: for example IT, procurement, construction, etc; and
- Mission critical projects: where organisations need to be sure of success.

The level of risk appetite will obviously vary, with a speculative project prepared to take on higher levels of risk than a "Mission Critical" project.

Effective management and application of delegated risk appetite requires escalation processes. It is possible to set 'trigger points' where risks can be escalated to the next level of management as they approach or exceed their agreed risk appetite levels (point C). The next level up in the hierarchy would then take appropriate action, which may mean managing the risk directly, or could mean adjusting the level of risk that they are happy for the level below to manage (point D). It is also often the case that a higher level of management, with a wider portfolio of risk to manage, has more scope to accept higher risks in particular areas as they can offset them against other lower risks in their portfolio.

Appendix 9
Strategic Investment Board – Fraud risk assessment (paragraph 3.28)

ID	Risk	Impact	Countermeasures	Notes
1	Suppliers may submit fraudulent invoices.	HIGH	Requirement for payment authorisation by responsible adviser/manager. Requirement for approved business cases to support all expenditure.	Payments audited annually. System subject to internal audit in Sept 2008.
2	Finance staff may abuse systems for personal gain.	HIGH	Dual authorisations of all payments. Separation of duties. Rotation of staff. Insistence on Finance Staff taking full leave entitlement, including at least one break of more than one week's duration.	Systems audited annually.
3	Temporary workers submit improperly completed timesheets.	LOW	Checks made against MyHours and IT System log-in and log-out records. Timesheets authorised by supervisor. Rates checked by HR Manager. Invoices checked by Finance staff.	
4	Improper claims for travel and subsistence.	LOW	All claims require authorisation.	Claims audited annually. Internal Audit Report 2008
5	Improper overtime claims.	LOW	Requirement for prior approval from line manager. All claims require line management approval. Checks made by HR Manager against MyHours and IT System log-in and log-out records.	Only administrative staff can claim for paid overtime.
6	Staff may abuse corporate credit cards.	LOW	Fully itemised expense claims required for all expenditure using corporate credit cards. Low expenditure limits.	Internal Audit Report 2008

Appendix 10
OFMDFM stewardship statements pro forma (paragraph 4.5)

Business area:

Report period:

Scope of responsibility

As the [Senior Officer] responsible for [ ] Directorate / Division, I have responsibility for maintaining a robust system of internal control that supports the achievement of OFMDFM's policies, aims and objectives, whilst safeguarding the public funds and Departmental assets for which I am responsible.

The OFMDFM system of internal control has been in place and adhered to for the period of this report in the business area for which I am responsible and accords with Department of Finance and Personnel guidance.

Capacity to handle risk

My Directorate / Division is carrying out appropriate procedures to ensure that it identifies its objectives and risks and a control strategy has been devised for each of the significant risks. As a result, risk ownership has been allocated to appropriate staff.

Acknowledgement of ownership

I acknowledge my responsibility for managing corporate and key Directorate/ Divisional risks and for monitoring those risks assigned to members of my management team. This statement has been informed following a thorough assessment of risk and control in my business area undertaken by each Head of Division/ Branch against each of the following risk factors as appropriate (outlined in OFMDFM guidance):

- business planning;
- legislative and other authorities;
- business cases (including economic appraisal, post project evaluation and consultancy);
- consultancy;
- forecasting and monitoring of expenditure;
- procurement;
- information assurance;
- staff (including absence, gifts & hospitality);
- ALBs, NDPBs and Third Party Organisations;
- internal & external audit reports; and
- other significant Issues.

Risk management status

I am satisfied that the controls in place to manage risks for which I am responsible are appropriate. They provide reasonable assurance that the risk will not occur or if it does occur that it will be detected and corrected in sufficient time to reduce the impact of the risk to tolerable or negligible levels.

Appendix 10
OFMDFM stewardship statements pro forma (paragraph 4.5)

Significant internal control problems

[Insert details of significant internal control problems of which the signatory is aware and the action taken to rectify these]

Head of Directorate / Division

Date:

NIAO Reports 2010-2011

Title	Date Published
2010	
Campsie Office Accommodation and Synergy e-Business Incubator (SeBI)	24 March 2010
Organised Crime: developments since the Northern Ireland Affairs Committee Report 2006	1 April 2010
Memorandum to the Committee of Public Accounts from the Comptroller and Auditor General for Northern Ireland: Combating organised crime	1 April 2010
Improving public sector efficiency - Good practice checklist for public bodies	19 May 2010
The Management of Substitution Cover for Teachers: Follow-up Report	26 May 2010
Measuring the Performance of NI Water	16 June 2010
Schools' Views of their Education and Library Board 2009	28 June 2010
General Report on the Health and Social Care Sector by the Comptroller and Auditor General for Northern Ireland – 2009	30 June 2010
Financial Auditing and Reporting - Report to the Northern Ireland Assembly by the Comptroller and Auditor General 2009	7 July 2010
School Design and Delivery	25 August 2010
Report on the Quality of School Design for NI Audit Office	6 September 2010
Review of the Health and Safety Executive for Northern Ireland	8 September 2010
Creating Effective Partnerships between Government and the Voluntary and Community Sector	15 September 2010
CORE: A case study in the management and control of a local economic development initiative	27 October 2010
Arrangements for Ensuring the Quality of Care in Homes for Older People	8 December 2010
Examination of Procurement Breaches in Northern Ireland Water	14 December 2010
General Report by the Comptroller and Auditor General for Northern Ireland - 2010	22 December 2010

NIAO Reports 2010-2011

Title	Date Published
2011	
Compensation Recovery Unit – Maximising the Recovery of Social Security Benefits and Health Service Costs from Compensators	26 January 2011
National Fraud Initiative 2008 - 09	16 February 2011
Uptake of Benefits by Pensioners	23 February 2011
Safeguarding Northern Ireland's Listed Buildings	2 March 2011
Reducing Water Pollution from Agricultural Sources: The Farm Nutrient Management Scheme	9 March 2011
Promoting Good Nutrition through Healthy School Meals	16 March 2011
Continuous improvement arrangements in the Northern Ireland Policing Board	25 May 2011

Printed in the UK for the Stationery Office on behalf of the Northern Ireland Audit Office
PC2962 05/11

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone 0870 240 3701

TSO@Blackwell and other Accredited Agents

Customers can also order publications from:
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Tel 028 9023 8451 Fax 028 9023 5401

ISBN 978-0-337-09732-4