DEPARTMENT OF FINANCE AND PERSONNEL

POLICY AND FRAMEWORK FOR RISK MANAGEMENT

EFFECTIVE FROM 21st OCTOBER 2011

Contents

Background

1. DAO (DFP) 5/01 introduced a requirement for Accounting Officers to sign a 'Statement on Internal Control' (SIC) which is published with the Accounts each year. The SIC provides an assurance that the control systems underpinning all activities within the Department are effective. A key element to providing such assurance is the requirement for managers to conduct risk assessments at both corporate and operational levels. DAO (DFP) 25/03 reinforces the need to maintain and develop the risk management and review process to ensure continuing effectiveness. More Recently DAO (DFP) 18/05 introduced the HMT Good Practice Guide on Corporate Governance in Central Government Departments. This further promotes the integral role of risk management in overall governance arrangements.

Purpose

2. This document defines the Department of Finance and Personnel's Risk Management Framework, and describes the process for identifying and managing risk within the Department. It has been endorsed by the Departmental Board and draws on the principles and approach set out in 'The Orange Book, Management of Risk – Principles and Concepts, issued by HM Treasury and 'Management of Risk: Guidance for Practitioners' issued by OGC.

Definitions of Risk and Risk Management

3. For current purposes a **risk** can be defined as "uncertainty of outcome, whether positive opportunity or negative threat, of actions or events". (The Orange Book - Management of Risk – Principles and Concepts 2004).

4. **Risk Management** is the culture, process and structures that are directed towards the effective management of potential opportunities and threats facing an organisation striving to meet its objectives. (Cabinet Office Framework for Risk-Based Decision Making)

5. There are many reasons why an organisation should risk manage their risks, both positive and negative, i.e.:

   - It is a tried and tested system;
   - It represents accepted good practice;
   - Increases engagement of management in achieving objectives;
   - Enables prioritisation of management effort, therefore more efficient;
   - Structured approach to managing risks keeps business on plan;
   - Strengthens corporate governance;
   - Enhances planning process; and
   - Fulfils mandatory requirement (HMT,DAOs).

6. The DFP Risk Management Framework is concerned with the identification and management of risk and of ensuring that exposure to risk is kept to an acceptable level where possible, and recognises where it is not possible. Also, it is important to note risk management is concerned with events that **may** occur, rather than issues that **have** occurred and in this regard is a proactive rather than reactive process.

Strategic Framework for the Management of Risk

7. Risk Management is a key element of the effective accountability and corporate governance arrangements supporting the Statement on Internal Control. The Departmental Board has overall responsibility for ensuring a robust risk management process is established and is responsible for agreeing the Department's Risk Management Framework.

8. For the purpose of the Framework all risks will be managed at one of three levels:-

- **Corporate/Strategic Risks** – High level risks which could have a major impact on the Department's business objectives. They may also include cross NICS risks and interdependencies on other NICS initiatives or activities. These risks are managed primarily by Departmental Board in conjunction with Core Directors and Agency Chief Executives and, are subject to challenge by the Departmental Audit and Risk Committee.

- **Directorate Risks** – Risks that relate to activities within the control of a Directorate or Agency, which could have a major impact on the delivery of service or achievement of objectives for that area. These risks are managed by Core Directors and Agency Chief Executives, and may be escalated to corporate level or de-escalated to Divisional level as appropriate.

- **Divisional Risks –** Risks which could impact on the delivery or timescale of activities or deliverables at Divisional level. These risks will be managed by Heads of Divisions and may be escalated to Directorate or, indeed Corporate level as appropriate.

9. Branch, Unit, systems or individual risks will also exist, which may impact on service delivery. However, these risks will usually be managed at the discretion of the Agency/Division, and as necessary can be included in the Divisional or Agency Risk Register.

10. **Programme and Project Risks** also exist and will usually be managed within the methodology used to manage the Programme or Project level by way of a project management methodology (e.g. PRINCE2, Gateway process). Managers responsible for projects must assure themselves that risks are being tracked and dealt with effectively. The mechanisms in place for monitoring and reporting risk will vary according to the size and

complexity of the programme or project, ranging from the use of a risk register to the appointment of a risk manager.

11. Large programmes, including NICS wide programmes in which DFP has the lead, will always have a governance structure set up in line with the OGC Gateway process. These include a Senior Responsible Owner (SRO), a programme manager and a programme board supported by a project team and project manager. This represents best practice and is essentially about accountability for managing and delivering the project. In each case the SRO is a senior Civil Servant who provides support and assurance to the DFP Accounting Officer.

Risk Management Process

12. This details the risk management process to be followed in the identification and management of risk within the Department. The Department's Risk Opportunity Process is summarised in **Appendix 1**.

13. The Risk Management Process includes:

- risk identification;
- assignment of ownership;
- response to risk;
- evaluation;
- assurance; and
- embed and review.

14. Risks should be related to objectives as set out in the relevant business plan/Balanced Scorecard. Some risks and targets may be relevant to more than one objective. The timescale for the life of the business objective, and associated risks will usually be 2-5 years. However risk identification and assessment should not be confined to the process of drawing up annual business plans. Risk management should be a continuous process which identifies new risks, changes in existing risks and risks which are no longer relevant to the department.

Identification of Risks

15. All types of risks should be identified (e.g. political, structural, financial, reputational, technical, programme). A summary of some of the most common categories of risk with examples is included in **Appendix 2**. Risks should be identified throughout the Department and managed at the appropriate level. Statement of risk should encompass the cause of the impact and the impact to the objective (cause and consequence).

16. In identifying risks, managers should not just consider threats to the achievement of their objectives but also consider opportunities for improved performance and enhanced capacity.

17. Assessment of risk is largely judgemental but it is necessary to adopt a systematic approach for the identification of risk. **Appendix 3** sets out the process for identifying and managing DFP's corporate risks. The process helps develop a clear and common understanding amongst the relevant management of the risks facing their business and the scope for mitigating and managing key risks.

Assignment of Ownership

18. It is important to identify the most important areas to which resource should be allocated in risk management and to allocate responsibility for management of these risks. Ownership of key risks will usually be assigned at Grade 5 level or above. Although the owner of the risk may not always be the person tasked with the assessment or management of the risk, they are responsible for ensuring the risk framework is applied.

Response to risk

19. Once a risk has been identified consideration must be given to the appropriate response. Responses to risk can be divided into four categories:

    - Transfer;
    - Tolerate;
    - Mitigate (Treat); or
    - Terminate

20. **Appendix 4** describes these categories. In many cases Departmental risks will fall into the *"Mitigate"* category. Where this is the case, actions will be identified and put in place to manage these risks and contain them to as low a level as is reasonably practical (i.e. adopt a proportionate response). Such actions may take the form of either Current Controls or Risk Management Actions. Guidance on the nature of current controls and risk management actions is provided at **Appendix 5**.

Evaluation

21. In order to decide how to handle a risk it is essential not only to identify the existence of the risk but also to evaluate the likelihood of it occurring and the impact on the delivery of business objectives if it occurs. The Department will adopt a consistent approach to evaluating the likelihood and impact of key risks. Guidance on the evaluation of likelihood and impact of risks is provided at **Appendix 6** and a sample risk matrix is provided at **Appendix 7**.

Assurance

22. The Department obtains assurance on its risk management process through regular monitoring and reporting by way of the DFP Corporate Planning Application as well as from the quarterly Corporate Performance Reports to the Departmental Board, Stewardship Statements, provided twice yearly by Business Areas, the Internal Audit Mid and Annual Assurance Reports and the Departmental and Business Area Audit and Risk Committees.

Embed & Review

23. The Department integrates risk management with all aspects of the business planning process and Risk Management awareness and training sessions are provided to managers.

New Risk Identification

24. A risk assessment will be carried out on all new business activities or functions and the results will be incorporated in the appropriate Risk Register.

Risk Appetite

25. The risk appetite sets out the level of risk that management is prepared to accept, tolerate, or be exposed to at any point in time. It also takes account of the adequacy of the control to manage the risk. The level of risk tolerated is likely to be dependant on a number of factors including budget, impact, likelihood, systems and controls and manpower. Managers should set clear boundaries for unacceptable risk and risks that should be escalated to a higher level.

26. The following principles have been agreed:

- Risks assessed as extremely high (in the red zone on the Risk Matrix – see **Appendix 7**) require urgent proactive actions to be taken in order to ensure they are managed effectively and risks are reduced to an acceptable level (i.e. medium or below.)
- Risks assessed as medium (amber zone in the Risk Matrix) require proactive management with appropriate actions to be taken.
- All risks assessed as low (green zone in the Risk Matrix) require minimal risk management. However, although no actions may be required at this time these risks should be kept under review.

Risk Analysis and Risk Registers

Risk Analysis and Risk Rating

27. There is a degree of risk in all of the Department's activities and its ability to take positive action about some risks may be limited or the cost of taking that action may be disproportionate to the potential benefit gained. Control costs money and it is important that any potential loss associated with a risk materialising should be weighted against the cost of controlling it. Each risk is graded using rankings on the likelihood of the risk occurring and the impact it would make if it did occur. Risks are quantified on a scale of 1 to 5 for likelihood of occurrence and degree of impact. The table in **Appendix 6** may be used to assist in the determination of the risk rating.

Recording of Risks - Risk Registers

28. Each identified risk is recorded on one or more of the Departments Risk Registers (i.e. Corporate, Directorate or Divisional). The Risk Register records the:-

    - inherent risk description;
    - controls currently in place;
    - risk management actions to be/being undertaken;
    - current status of the residual risk in terms of red, amber or green based on the probability of the risk occurring and the impact of the risk should it occur;
    - risk owner; and
    - links to departmental business plan objectives.

    A copy of the Department's Risk Register template is provided at **Appendix 8**.

Contingency Planning

29. Contingency planning is needed to ensure that if a risk does materialise there are effective arrangements in place to minimise the impact and enable the Department to continue to deliver its service. Where appropriate, contingency plans should be developed and agreed with Departmental Board for all key risks within the red zone.

Annual Review

30. At the end of the financial year the Departmental Board:-

    - reviews the effectiveness of the Department's system of internal control;

    - assesses whether the key risks that face the Department have been identified for the following year and agree management controls; and

- approves the Departmental Risk Register for the incoming financial year.

31. The annual assessment of internal controls considers:-

- the changes since the last annual assessment in the nature and extent of significant risks;
- the scope and quality of the ongoing monitoring of risks and of the system of internal control;
- reports received from review bodies, e.g. Internal Audit, the Northern Ireland Audit Office etc;
- the effectiveness of the Department's reporting processes; and
- other relevant reviews.

Stewardship Statements

32. At mid year and year end in reviewing the effectiveness of the system of internal control Core Directors and Agency Chief Executives are required to sign Stewardship Statements for their areas of responsibility. By completing the Stewardship Statements Directors and Chief Executives are acknowledging their responsibility for managing the Corporate Risks and key Directorate Risks appropriate to their Business Areas, and for monitoring the risks assigned to members of their Management Team. The Statement also provides assurance to the Accounting Officer that risks are being managed appropriately. The Stewardship Statements should therefore:-

- confirm the appropriateness of risks and that controls identified are adequate, effective and have been operated throughout the period.
- highlight areas where deficiencies are possible or breakdowns in control have actually occurred and state corrective actions taken to address these; and
- recommend changes, as appropriate, to the Corporate Risk Register. The review of risks associated with the achievement of PSA and departmental objectives and targets helps to inform this process. All suggestions should be supported by sufficient information to enable decisions to be reached.

33. The Stewardship Statements also require Directors and Chief Executives to confirm that they have complied with a range of governance and control requirements including those applying to financial management and approvals and delegations, for example, on the engagement of external consultants, business cases, procurement, special payments and provision and acceptance of gifts and hospitality. In addition, the Stewardship Statements require an assurance from Directors and Chief Executives that

they have complied with the Department's information assurance requirements.

34. Completed Stewardship Statements are used to inform the preparation of the Department's Statement on Internal Control. A copy of the Department's Stewardship Statement template is available within the Risk Management section of the DFP Governance and Control Framework.

Monitoring and Controls

35. The DFP Corporate Planning Application (CPA) is an integrated business planning/risk monitoring process which exists in electronic form and is maintained by Business Planning and Corporate Governance Branch (BPCG). Business areas are required on a regular basis to complete updates on progress against:-

- identified risks;
- consideration of any new risks (for both existing and new business); and,
- recommendations on risks to be removed.

36. The Corporate Risk Register will be provided quarterly to Departmental Board (DB) and to all meetings of the Departmental Audit and Risk Committee (DARC) highlighting risks against departmental objectives.

37. Departmental Board will consider the risk register and agree appropriate action. The Departmental Audit and Risk Committee provides assurance to the Accounting Officer on the effective management and reporting of corporate level risks.

Roles and Responsibilities

Accounting Officer

38. The Permanent Secretary, as Accounting Officer, provides the top level commitment and support for the risk management process and has overall responsibility for managing the risks faced. He is responsible for ensuring that risks faced by the Department are appropriately managed and that the necessary controls are in place.

Departmental Board

39. The Departmental Board has executive responsibility for:

- taking major decisions affecting the management of risk within the Department;
- annually reviewing the Department's approach to risk management;
- ownership of the Corporate Risk Register; and

- representation as appropriate on the Departmental Audit and Risk Committee.

Core Directors and Agency Chief Executives

40. Responsibilities of Core Directors and Agency Chief Executives include:

- agreeing the key risks, risk owners and controls to manage risks identified in the Risk Register at Corporate and Directorate/Agency level;
- taking decisions affecting the management of risk within their Directorate/Agency;
- monitoring the management and control of key risks to reduce the likelihood of unforeseen occurrence;
- ownership of the Directorate/Agency Risk Register; and
- chairing the Directorate/Agency Audit and Risk Committee.

Risk Owners

41. Heads of Divisions (HODs) are usually appointed risk owners. Risk owners will have the authority to assign resources to manage key risks. They are responsible for managing assigned risks by ensuring controls are in place and properly actioned at all levels throughout their Division. They are also responsible for:

- implementing the Department's Risk Management Policy and procedures on internal controls;
- encouraging relevant staff to actively consider and manage risk
- communicating progress, identifying control weaknesses and recommending remedial actions for their assigned risks to the Director and Directorate Audit and Risk Committee; and
- ensuring that a suitable system of internal control operates in their area of responsibility.

Line Management

42. Line management are expected to:

- work within the Department's policy on risk management;
- alert HODs to emerging risks or control weakness; and
- ensure controls are actioned within their own areas of work.

Corporate Services Group (CSG)

43. CSG supports the Department's Risk Management Framework as an integral part of the business planning cycle by co-ordinating reports to the Departmental Board. Within the Risk Management Framework, CSG also:

- provides the secretariat function to the Departmental Audit and Risk Committee;
- provides advice on Risk Management to managers;
- arranges appropriate training for managers; and
- is the central point for liaison on matters relating to Risk Management. Advice may also be sought from Internal Audit and the Northern Ireland Audit Office.

Departmental Audit and Risk Committee (DARC)

44. The Audit and Risk Committee provides the Accounting Officer with objective advice on issues concerning the risk, control and governance of the organisation and the associated assurances. To enhance the objectivity of the advice given, the Committee is chaired by a non-executive Director. Although it has no authority in its own right over the operations of the organisation, the Committee:

    - supports the Accounting Officer in monitoring the corporate governance and control systems in the organisation; and
    - assists the Departmental Board, in an advisory function, in discharging its responsibilities with respect to overseeing all aspects of financial reporting and audit functions.

Directorate and Agency Audit and Risk Committees

45. Each Directorate or Agency has its own Audit and Risk Committee (ARC), usually chaired by the Core Director or Chief Executive of the relevant Core Business Directorate or Executive Agency. The ARCs will ensure that the effectiveness, relevance and accuracy of the risk register is kept under regular review by:

    - reviewing progress on the management of the status of risks relevant to their business plan;
    - reviewing the effectiveness of the controls;
    - considering any new risks that may have emerged;
    - assessing the current status of major risks; and
    - considering of assurances provided by risk owners mid-year and at the year-end and advising the Director/Agency Chief Executive on the completion of the Stewardship Statement.

Internal Audit

46. Within the Department, Internal Audit is responsible for providing the internal audit service to the Core Department and its Agencies.

47. The Head of Internal Audit provides Accounting Officers with an independent opinion on the management and control of risk through the completion of individual audit assignments which are agreed annually by the Agency/Directorate and Departmental Audit Committees. Additionally,

findings and recommendations assist management in the audited business areas in strengthening their risk management and internal control processes and procedures.

48. Additionally, Internal Audit is available to provide advice and guidance on all matters relating to the management and control of risk.

Northern Ireland Audit Office

49. The Northern Ireland Audit Office (NIAO) is headed by the Comptroller and Auditor General (C&AG). The NIAO is totally independent of Government. NIAO audits the accounts of all Government Departments and other public bodies. While the Statement on Internal Control which forms part of the Accounts is not audited per se, the C&AG may report on it if does not meet the requirements for disclosure specified by DFP, or if the statement is misleading or inconsistent with other information he is aware of from his audit of the financial statements. The C&AG has a statutory authority to report to Parliament on the economy, efficiency and effectiveness with which Departments use their resources. A representative from NIAO attends Audit Committee meetings at which corporate governance, internal control and risk management matters are considered.

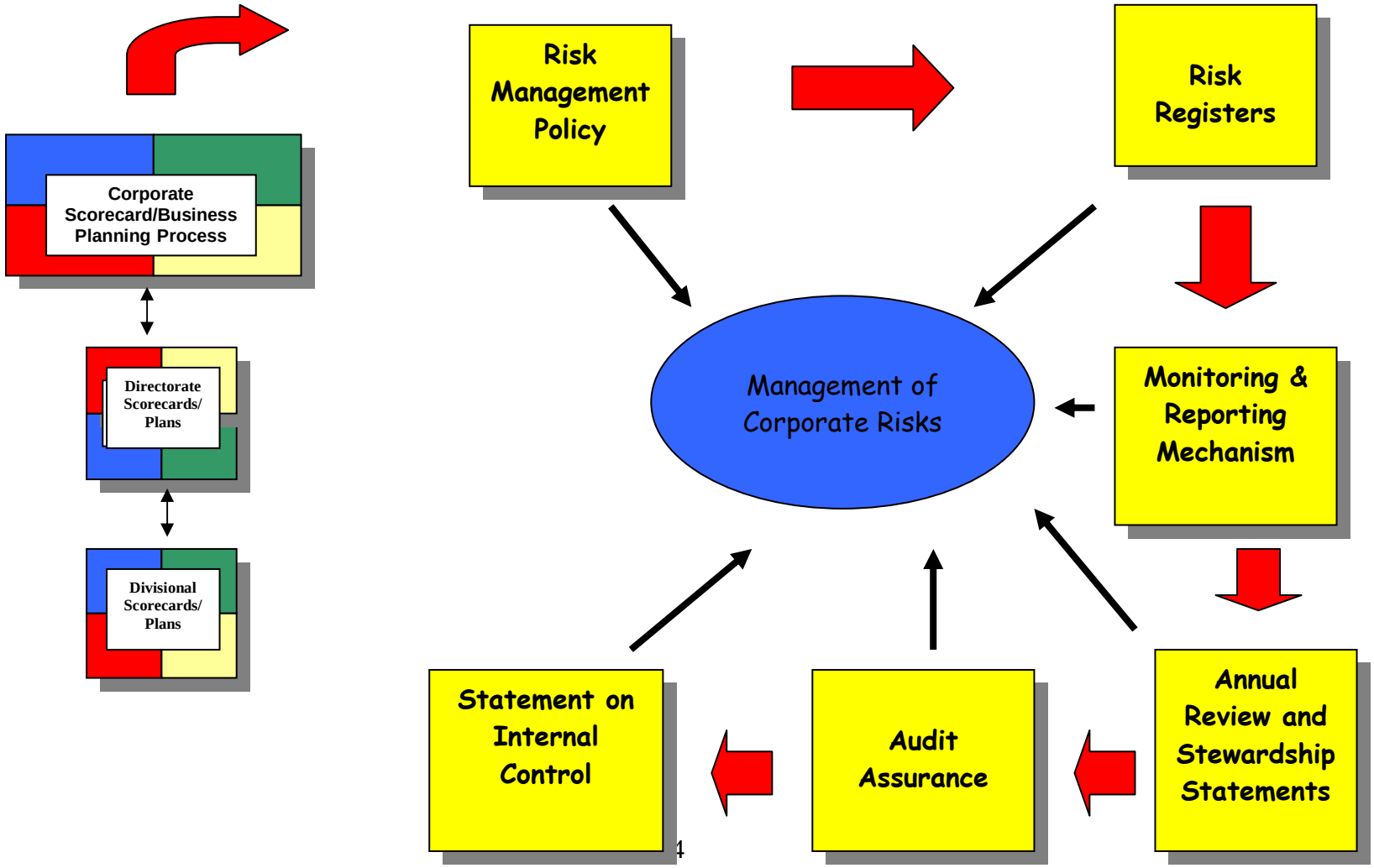
Other Areas of Risk Assessment

50. Examples of other areas of risk assessment are attached in **Appendix 9**.

Useful References

51. Useful references and websites which cover the Risk Management Process are listed in **Appendix 10**.

Risk Opportunity Process



Appendix 2

Criteria for Helping Identify Risks

Management of Risk – A Strategic Overview (The Orange Book)
HM Treasury

The table below offers a summary of the most common categories of risk with examples of the nature of the source and effect issues. The table does not claim to be comprehensive – some organisations may be able to identify other categories of risk applicable to their work.

CATEGORY OF RISK	
Financial	
Budgetary	Relating to the availability of resources or the allocation of resources.
Fraud or theft	Relating to the unproductive loss of resources.
Insurable	Relating to potential areas of loss which can be insured against.
Capital investment	Relating to the making of appropriate investment decisions.
Liability	Relating to the right to sue or to be sued in certain circumstances.
Activity	
Policy	Relating to the appropriateness and quality of policy decisions.
Operational	Relating to the procedures employed to achieve particular objectives.
Information	Relating to the adequacy of information which is used for decision making.
Reputational	Relating to the public reputation of the organisation and consequent effects.
Transferable	Relating to risks, which may be transferred, or to transfer of risks at inappropriate cost.
Technological	Relating to the use of technology to achieve objectives.
Project	Relating to project planning and management procedures.
Innovation	Relating to the exploitation of opportunities to make gains.
Human Resources	
Personnel	Relating to the availability and retention of suitable staff.
Health and safety	Relating to the well being of people.

Appendix 3

DFP Risk Identification Process

Complete Corporate Business Plan/Balanced Scorecard.

↓

Potential risks to meeting corporate objectives/measures identified by Business Areas using criteria provided and information from previous year.

↓

Draft Corporate Risk Register developed and presented as part of the Corporate Performance Report for Quarter 1 each year to the Departmental Board and Departmental Audit and Risk Committee.

↓

Departmental Board to discuss content of the Corporate Risk Register and agree proposed changes and actions necessary to manage risks.

↓

Agree risks identified, set timescales of actions and risk owner with all Directors/Agency Chief Executives.

↓

Take into account comments provided by Internal Audit.

↓

Business Areas review and update corporate risks as part of quarterly monitoring through the departmental Corporate Planning Application.

↓

Corporate Risk Register presented to quarterly meetings of Departmental Board and all meetings of the Departmental Audit and Risk Committee.

Appendix 4

Response to Risk Criteria

Response	Description
Transfer	For some risks the best response may be to transfer. For example by conventional insurance or by buying a third party to take the risk in another way
Tolerate	The ability to do anything about some risk may be limited, the risk may be considered to be low priority or the cost of taking action may be disproportionate to the potential benefit gained.
Terminate	Some risks will only be treatable or containable to acceptable levels by terminating the activity or redesigning/simplifying a business process to avoid or reduce the risk.
Mitigate (Treat)	The purpose of the treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level.

Appendix 5

CURRENT CONTROLS

For most of our risks the most traditional response is to **TREAT** or mitigate against the risk. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk**, control** is taken to constrain the risk to an acceptable level. Such controls can be further sub-divided into the following categories according to their particular purpose:

Type of Control	**Purpose**	**Examples**
PREVENTIVE	To limit the possibility of an undesirable outcome being realised. The more important it is that the undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls. The majority of controls implemented in organisations tend to belong to this category.	- Governance Structures, such as Programme/Project Boards - Regular reporting/ monitoring of progress against business plan/balanced scorecard targets - Supervisory checks, password controls etc
CORRECTIVE	To correct undesirable outcomes that have been realised. These provide the route to recourse to achieve some recovery against slippage, loss or damage.	- Contract terms to allow recovery of loss - Contingency Plans, business continuity after events over which we had no control
DIRECTIVE	To ensure that a particular outcome is achieved. Particularly important when it is critical that an undesirable event is avoided.	- PSA/Business Plan targets - Financial controls/targets - Security/Information assurance and data protection measures
DETECTIVE	To identify occasions of undesirable outcomes having been realised. Their effect is by definition “after the event” so they are only appropriate when it is possible to accept the loss or damage incurred.	- Post Implementation Reviews - Post Project Evaluations - Lessons learned reports

It is important that controls are proportionate to the risk. Every control will have an associated cost and should therefore offer value for money in relation to the risk it is controlling. The purpose of control is to constrain rather than eliminate risk.

RISK MANAGEMENT ACTIONS

The purpose of **risk management action** is to take further steps to **TREAT** or mitigate against risks after all of the relevant controls have been put in place. Risk management actions may take many forms but it is important that they include, where possible, specific dates for completion in order for progress to be assessed. Some examples of **risk management actions** might include:

- Development/revision of policy or procedures by **[DATE]**
- Development/implementation of action plans to address specific issues or improvements by **[DATE]**
- Development/approval of Strategic Outline Cases / Full Business Cases by **[DATE]**
- Procurement/implementation of specific services or facilities such as IT systems by **[DATE]**
- Assessment of external factors or developments which may influence the achievement of specific objectives by **[DATE]**
- Identification of future threats or opportunities by **[DATE]**
- Consideration of the potential to engage with third parties to assist with delivery by **[DATE]**

Appendix 6

GUIDANCE ON IMPACT AND PROBABILITY

Impact

	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
Service Delivery	Short term disruption of service to some customers.	Widespread disruption of service lasting less than 2 hours.	Widespread disruption of service lasting up to one day.	Failure to meet SLAs on an ongoing basis; or widespread disruption of service lasting more than one day.	Failure to meet key SLAs on an ongoing basis; or widespread disruption of service lasting more than one week.
Business Objectives	Unlikely to have any impact on meeting business plan objectives or targets.	Some impact on business objectives resulting in slight but redeemable deviation to target timescales or quality of outcomes.	Failure to deliver a Business Area objective, requiring action and regular monitoring at BA level.	Failure to deliver a key DFP / PfG business objective requiring intervention and regular monitoring at Board level.	Failure to deliver a key DFP / PfG business objective requiring ongoing reporting at Ministerial level.
Financial	Unlikely to have any budgetary or financial implications.	Financial implications requiring re-alignment of budgets (<£500k).	Financial implications requiring re-allocation of resources and/or additional funding (>£500k).	Significant financial implications with failure to achieve DFP's financial targets and/or compliance with financial and accounting policies.	Very significant financial implications resulting in qualification of the Departments accounts and/or financial impropriety.
Reputation **Political Criticism** **Press/Media coverage**	None.	Some interest possible, but likely to be localised and short-term.	Adverse coverage, usually on a one-off basis.	Significant adverse coverage, likely to recur on several occasions.	Very significant adverse coverage, sustained over a considerable period.

Probability

	1 Very low	2 Low	3 Medium	4 High	5 Very High
Probability Range	< 5% Has not occurred previously and unlikely to occur in future.	5 – 20% Although unlikely, there is a chance of the risk materialising.	20 – 50% The outcome is in the balance, and is almost as likely to occur as not.	50 – 75% More likely to occur than not.	> 75% Very likely.

EXAMPLE OF RISK MATRIX

Severity = Impact by Probability

Probability						
	5 Very High	5	10	15	20	25
	4 High	4	8	12	16	20
	3 Medium	3	6	9	12	15
	2 Low	2	4	6	8	10
	1 Very Low	1	2	3	4	5
		1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Severe**
		Impact				

Appendix 8

Department of Finance and Personnel - Corporate Risk Register 2011/12
TEMPLATE

Inherent Risk Description	Controls (currently in place)	Risk M'ment Actions (to be / being undertaken)	Residual Risk					Owner	Link to Business Plans / Comments
			Date	Status	Prob.	Impact	Rating		
RISK X **Risk Title** **Risk Description**	1. 2. 3. 4. 5.	1. 2. 3 4. 5.	**Current**	**Red** **Amber** **Green**	**1** **to** **5**	**1** **to** **5**	**Prob.** **X** **Impact**		**Departmental Business Plan Number** **Departmental Target Description**

Appendix 9

Other Areas of Risk Assessment

In addition to identifying key risks against the Department's strategic business objectives and associated targets, risks assessments are also conducted against specific areas of the business. This can include:-

- *Business Continuity* – All business areas have a responsibility to develop & maintain a Business Continuity Plan to deal with disruption at a local level e.g. unable to gain access to a building or disruption to administering services to customers and are subject to six monthly reviews.

- *Health & Safety* – Risk Assessments on the work environment are carried out by designated Risk Assessors on an annual basis and when deemed necessary e.g. redesign of office.

- *Internal Audit* - Internal audit primarily provides an independent and objective opinion to the Accounting Officer on risk management, control and governance, by measuring and evaluating their effectiveness in our strategic objectives. However, in addition, their findings and recommendations assist line management in the audited areas in identifying weaknesses and risks in processes and systems.

- *IT Security Accreditation* - The process of accreditation is mandatory for systems which handle protectively marked data. The basis of accreditation is a risk assessment including evidence that all the relevant risks have been properly considered/assessed and also specify the measures taken to manage risk in accordance with government approved standards. Ultimately accreditation is a statement by the Accreditor confirming that the use of the system to process, store and/or forward protectively marked information does not present an unacceptable risk to the business of the Department.

Appendix 10

USEFUL REFERENCES AND WEBSITES

- The Orange Book - Management of Risk – Principles and Concepts (Oct 2004). HM Treasury
- The Audit Committee Handbook. HM Treasury
- Risk Management Assessment Framework. HM Treasury Risk Support Team
- Risk: Improving Government's capability to handle risk and uncertainty. Strategy Unit Report – November 2002
- OGC Management of Risk: Guidance for Practitioners. HMSO
- DAO (DFP) 5/01 and DAO (DFP) 25/03 - Statement on Internal Control
- Corporate Governance in Central Government Departments – Code of Good Practice. HM Treasury - July 2005 http://www.afmdni.gov.uk/pubs/DAOs/dao1805att.pdf
- Accounting Officer Responsibilities for DFP led Projects – Minute from John Hunter to PSG (15 September 2005)
- Guidance about the process of IT Security Accreditation is contained in HMG Infosec Standard 2 available from CESG website.
- National Technical Authority for Information Assurance http://www.cesg.gov.uk/
- Office of Government and Commerce (OGC) http://www.ogc.gov.uk
- Risk Portal http://www.cabinet-office.gov.uk/risk/
- Her Majesty's Treasury http://www.hm-treasury.gov.uk
- Strategy Unit http://www.strategy.gov.uk
- Northern Ireland Audit Office http://www.niauditoffice.gov.uk