



**PUBLIC PROSECUTION SERVICE  
FOR NORTHERN IRELAND**

**POLICY AND FRAMEWORK  
FOR RISK MANAGEMENT**

**Last Revised February 2016**

## Contents

| <b>Section</b> | <b>Heading</b>  | <b>Page</b> |
|----------------|---|-------------|
| 1.             | Introduction  | 3           |
| 2.             | Purpose   | 3           |
| 3.             | What is Risk Management?  | 3           |
| 4.             | Risk Management Principles  | 4           |
| 5.             | Strategic Framework for the Management of Risk                        | 4           |
| 6.             | The Risk Management Process   | 5           |
| 7.             | Identification of New Risks   | 9           |
| 8.             | Risk Appetite   | 9           |
| 9.             | Risk Registers  | 11          |
| 10.            | Annual Reviews  | 12          |
| 11.            | Assurance Statements  | 12          |
| 12.            | Roles and Responsibilities  | 13          |
| 13.            | Other Areas of Risk Assessment  | 16          |
| 14.            | Useful References   | 16          |
| 15.            | Review  | 16          |
|                | <b>Annex 1: Common Categories of Risk</b>                             | <b>17</b>   |
|                | <b>Annex 2: Risk Identification Process – Corporate Risk Register</b> | <b>18</b>   |
|                | <b>Annex 3: Possible Responses to Risk</b>                            | <b>19</b>   |
|                | <b>Annex 4: Corporate Risk Management Process</b>                     | <b>20</b>   |
|                | <b>Annex 5: Risk Appetite and Tolerance</b>                           | <b>21</b>   |
|                | <b>Annex 6: Risk Register Template</b>                                | <b>25</b>   |
|                | <b>Annex 7: Other Areas of Risk Assessment</b>                        | <b>26</b>   |
|                | <b>Annex 8: Useful References and Websites</b>                        | <b>27</b>   |

# PPS Risk Management Policy and Framework

## 1. Introduction

The policy of the Public Prosecution Service (PPS) is to ensure that effective risk management processes are maintained which serve to improve the quality of decision making and the ability to deliver on strategic and operational objectives.

## 2. Purpose

This document defines the Public Prosecution Service's Risk Management Framework, and describes the process for identifying and managing risk within the Service. It has been endorsed by the Management Board and draws on the principles and approaches 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.

## 3. What is Risk Management?

Risk management is the combination of structures, management systems and organisational culture which enables an organisation to manage the threats and opportunities which might impact on the achievement of the objectives of the organisation. It is a process that involves the systematic application of management policies, procedures and practices to the task of identifying, evaluating, controlling, monitoring and communicating risk.

For the purpose of this document 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).

There are many reasons why an organisation should implement a risk management framework:

- It is a tried and tested system and represents accepted good practice;
- It increases engagement of management in achieving objectives;
- It enables prioritisation of management effort;
- A structured approach to managing risks assists in keeping the organisation 'on plan';
- It has an integral role in internal corporate governance and accountability arrangements and is should be regarded as a governance requirement (e.g. as set out in HMT 'DAOs').

#### 4. Risk Management Principles

The following principles will be followed as part of our risk management processes:

- Risk management will be applied at both strategic and operational levels within the organisation (see section 5 below);
- The risk management framework will consider both internal risks and external risks arising from relationships with key stakeholders and criminal justice partners;
- All risk management activity will be aligned to the strategic aims, objectives and priorities of the Service and will aim to protect and enhance the reputation and standing of the organisation in the community;
- Risk management in the organisation will be proactive; i.e. risk management will be concerned with events that **may** occur, rather than issues that **have** occurred. We will aim to anticipate, and where possible, avoid risks rather than having to deal with their consequences. Where appropriate we will develop contingency plans for dealing with the consequences of events;
- Strategic and operational risks will be identified, assessed, addressed, reviewed and reported on a regular basis; and
- In determining an appropriate response to risk, the cost of developing controls and the impact of the risk occurring will be balanced with the benefits of reducing the risk. It is as important to avoid over control of minor risks as under-control of serious risks.

#### 5. Strategic Framework for the Management of Risk

Risk Management is a key element in ensuring that effective accountability and corporate governance arrangements are in place, supporting the Service's Governance Statement. The Director, supported by the PPS Management Board, has overall responsibility for ensuring that an effective risk management process is established and maintained and is responsible for agreeing the Service's Risk Management Framework.

Within the PPS risk management framework, all risks will be managed at one of three levels:

- **Corporate Risks:** These are high level risks which could have a major impact on the Service's business objectives. They may also include inter-agency risks and involve interdependencies with other CJSNI initiatives or activities. These risks are managed primarily by the Management Board, in conjunction with the Senior Management Group, and are subject to challenge / scrutiny by the PPS Audit and Risk Committee.
- **Region / Section Risks:** These are risks that relate to activities within the control of an Assistant Director (SCS Grade 5), which could have a

major impact on the delivery of service or achievement of objectives for that area. These risks are managed by Assistant Directors, and may be escalated to corporate level or de-escalated to section level as appropriate.

- **Branch / Unit Risks:** These are risks which could impact on the delivery or timescale of activities or deliverables at branch level (for example, within Corporate Services Branches). These risks will be managed by the Heads of the individual branches and may be escalated to region / section or corporate level as appropriate.

Project Risks also exist and will usually be managed within the methodology used to manage the project level by way of a project management methodology (e.g. PRINCE 2). 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 project. For larger projects, we will have a governance structure which is set up broadly in line with the OGC Gateway process. These include a Senior Responsible Owner (SRO) and a project 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 will be a senior Civil Servant who provides support and assurance to the Director.

## 6. The Risk Management Process

The Service's risk management process includes a number of steps, as follows:

- Identification of risk;
- Assignment of ownership;
- Prioritisation of risks;
- Risk Responses;
- Assurance; and
- Embedding and review.

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. 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 PPS.

### *Identification of Risk*

All types of risks should be identified (e.g. political, structural, financial, reputational, technical, programme). A summary of some the most common categories of risk is included at Annex 1.

Identification and assessment of risks is viewed as a management function, to be considered at all management levels throughout the Service.

Any statement of risk should encompass the cause of the impact and the impact to the objective (cause and consequence). 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.

Whilst the assessment of risk is largely judgmental, it is necessary to adopt a systematic approach for the identification of risk. Annex 2 sets out the steps to be taken in identifying the PPS's corporate risks. The process helps to develop a clear and common understanding amongst the relevant managers of the risks facing their business and the scope for mitigating and managing key risks.

#### *Assignment of Ownership*

The Director has overall responsibility for the Service's risk management framework. However in order for risk management to be effective it is essential that responsibility for individual risks is delegated to the appropriate level. Therefore all identified risks will have an 'owner', so that responsibility and authority for implementing action plans is clearly understood.

Within the PPS ownership of corporate 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.

#### *Rating of Risks*

A key element in any risk management framework is that it should allow managers to identify the areas of risk in which action needs to be taken and their relative priority.

There is a degree of risk in all of the Service'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 therefore 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 4 for both likelihood of occurrence and degree of impact. In order to ensure consistency of approach, a simple 'traffic light' system is used which categorises risk priorities as 'high', 'medium', 'moderate' or 'low'. In line with accepted practice, this will be based on an assessment of the likelihood that an event will occur and its potential impact on the organisation, as follows:

**(a) Likelihood x (b) Impact = Risk Priority**

**(a) Likelihood**

| Score | Probability | Description                       |
|-------|-------------|-----------------------------------|
| 1     | 0-25%       | Unlikely to occur                 |
| 2     | 26-50%      | Fairly likely to occur            |
| 3     | 51-75%      | More likely than not to occur     |
| 4     | 75%+        | Very likely to occur / will occur |

**(b) Impact**

| Score | Rating   | Description   |
|-------|----------|---|
| 1     | Very Low | Minimal loss, delay, inconvenience or interruption  |
| 2     | Low      | Minor loss, delay, inconvenience or interruption<br>Short to medium term effect   |
| 3     | Medium   | Significant waste of time and resources<br>Impact on operational efficiency, output and quality<br>Medium term effect which may be difficult or expensive to recover  |
| 4     | High     | Major impact on costs and objectives. Serious impact on output / quality and reputation.<br>Medium to long-term effect which may be difficult or expensive to recover |

A simple 4 x 4 matrix will be used to prioritise risks according to priority (see below).

## PPS Risk Assessment Matrix

|            |               |   |   |   |   |
|------------|---------------|---|---|---|---|
| Likelihood | 4             |   |   |   |   |
|            | 3             |   |   |   |   |
|            | 2             |   |   |   |   |
|            | 1             |   |   |   |   |
|            |               | 1 | 2 | 3 | 4 |
|            | <b>Impact</b> |   |   |   |   |

### Key:

|                 |   |
|-----------------|---|
| <b>High</b>     | <p>The consequences of the risk materialising would be severe and possibly disastrous. Some immediate action is required plus the development of a comprehensive action plan. Red risks require immediate action.</p> <p>'Showstopper' risks are those that would:</p> <ul style="list-style-type: none"> <li>• Stop you from meeting your objectives or targets;</li> <li>• Be likely to have major impact on your processes;</li> <li>• Cause severe damage to corporate reputation or public embarrassment.</li> </ul> |
| <b>Medium</b>   | <p>Consequences of risk not severe and can be managed via contingency plans. Action plans developed later and budget bids mobilised. Status of risk should be monitored regularly. Amber risks need to be monitored and managed down to yellow / green.</p> <p>Potential risks are those that could:</p> <ul style="list-style-type: none"> <li>• Prevent you from meeting certain objectives/targets but do not endanger others;</li> <li>• Inconvenience the Department.</li> </ul>                                     |
| <b>Moderate</b> | <p>Consequences of risk remain relatively unimportant to business. However closer monitoring is required. The Service should consider what contingencies (at minimal additional cost) could be put in place to prevent negative outcomes.</p>   |
| <b>Low</b>      | <p>Consequences of risk relatively unimportant to business. Status of risk should be reviewed periodically. <i>Green risks do not require action.</i> Minor risks are those that have minor impact but do not affect a successful outcome.</p>  |

## *Risk Responses*

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;
- Treat (Mitigate); or
- Terminate.

Annex 3 describes these categories in more detail.

In many cases PPS 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).

## *Assurance*

The Department obtains assurance on its risk management process through regular monitoring and reporting (via the Management Board, Senior Management Group, Performance and Accountability Meetings and relevant project groups), as well as from the Quarterly Statements of Assurance, the Audit and Risk Committee and periodic review by Internal Audit.

## *Embed and Review*

The Service integrates risk management within all aspects of the business planning process. Relevant induction / awareness training sessions are also provided to all managers and staff.

Annex 4 provides an overall summary of the risk management process.

## **7. Identification of New Risks**

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 (see below).

## **8. Risk Appetite**

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.

Corporate risk appetite (Statement of Risk Appetite – see Annex 5) is the overall amount of risk judged appropriate for an organisation to tolerate. The purpose of the corporate risk appetite is to identify general boundaries for

unacceptable risk (or at least for risks that should always be referred to / escalated up to the Management Board for discussion and decision when they arise). It should be used as an adjunct to the risk management process and is intended to assist Assistant Directors and other managers in the compilation of their risk registers.

The level of risk tolerated is likely to be dependent on a number of factors including the nature of the risk, available budgets, impact and likelihood.

Managers should set clear boundaries for unacceptable risk and risks that should be escalated to a higher level (see below). The following principles have been agreed:

- Risks assessed as extremely high (in the red area of the Risk Matrix – see above) 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 area in the Risk Matrix) require proactive management with appropriate actions to be taken.
- All risks assessed as low (green area in the Risk Matrix) require minimal risk management. However, although no actions may be required at this time these risks should be kept under continuous review.

### *Risk Escalation*

Within PPS risk is to be managed at the most appropriate level to achieve effective mitigation / control and robust contingency planning. If risk cannot be managed at the level to which responsibility has been assigned, risk owners and/or managers at the current level should consider whether it is appropriate to escalate responsibility for ownership and management of a risk to a higher management level. Decisions to escalate risks must be made by current risk owners and/or managers *in agreement* with management at the level to which the risk is to be escalated.

Consideration as to whether or not a risk should be escalated may happen at any time; i.e. managers should not be restricted to formal review stages such as the completion of quarterly Assurance Statements (see para 11).

When escalated to a new level there must be an objective review process. This should include consideration of whether the risk is within the remit or area of effective control of the new level of management. Risk severity will also be reviewed to reflect the impact of the risk at the level to which it has been escalated.

When it has been agreed that a risk should be escalated the existing risk register should be noted accordingly and the risk included in the higher-level risk register.

Examples of trigger points for risks requiring escalation include:

- Risks outside of the control of individual managers (or that are not felt to be effectively managed at the current level of responsibility);
- Risks with a wider impact than solely within a specific project or function;
- Risks which will have a significant impact on wider strategic objectives, business processes or key operational activities;
- Cross cutting dependencies and resource conflicts;
- Risks with ineffective mitigation measures and / or inadequate control measures;
- ICT / technology risks that may have a significant impact on service delivery.

It will be acceptable for management at the higher level to decide *not* to accept the escalation of a risk, for example where it is felt that the existing risk owner has not taken sufficient action to manage the risk effectively. The reasons for such a decision will need to be recorded in a similar manner to those risks that have been escalated (i.e. in the appropriate risk register).

#### *'Prohibited' Risk Areas*

Where the Service's policies and guidance manuals define *mandatory* processes and procedures (e.g. Health and Safety), full compliance with these standards is required. ***Non-compliance constitutes an unacceptable risk.***

## **9. Risk Registers**

All agreed risks will be recorded in the appropriate 'risk register' (i.e. corporate, region / section or branch / unit). The template to be used for all registers is attached at Annex 6.

The risk register should record the:

- The status of the risk at the commencement of the monitoring period;
- The current status of each risk;
- The risk owner;
- Progress update against each risk on the actions taken in the previous period;
- Actions to be taken in the following period to manage / mitigate the risk.
- Persons responsible;
- Original target dates for action;
- Current target dates for action (if different from above); and
- Anticipated Risk Assessment (after planned mitigating actions).

## 10. Annual Review

At the end of the financial year the Director and Management Board:

- Review the effectiveness of the Service's system of internal control;
- Assess whether the key risks that face the Service have been identified for the incoming financial year and agree management controls; and
- Approve the risk register for the incoming financial year.

The annual assessment of internal controls considers:

- The changes since the last annual assessment in the nature and extent of corporate 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, Criminal Justice Inspection etc.; and
- The effectiveness of the Service's reporting processes.

## 11. Assurance Statements

In reviewing the effectiveness of the system of internal control and preparing the overall Governance Statement on an annual basis, all Assistant Directors are required to sign quarterly Assurance Statements for their areas of responsibility. By completing the Assurance Statements, Assistant Directors acknowledge their responsibility for managing relevant corporate risks / risks appropriate to their business areas and for monitoring the risks assigned to members of their team. The statements also provide assurance to the Director, as Accounting Officer, that risks are being managed appropriately. The Assurance Statements should therefore:

- Confirm that risk management arrangements have operated throughout the period; and
- Highlight areas where serious deficiencies are possible or breakdowns in control have actually occurred *and state corrective actions taken / planned to address these*.

In reviewing the quarterly Assurance Statements, Senior Assistant Directors will provide feedback to Assistant Directors regarding any risk areas flagged. This will include comment on the corrective actions taken or planned and any requirement to escalate risk.

## **12. Roles and Responsibilities**

### *Accounting Officer*

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

### *Management Board*

The Management Board has responsibility for:

- Ownership of the corporate risk register;
- Reviewing the corporate risk register at each scheduled meeting of the Board;
- Reviewing the Service's approach to risk management on an annual basis; and
- Non-executives to act as chair / members as appropriate on the Audit and Risk Committee.

### *Senior Management Group*

- Development of a first draft of the corporate risk register on an annual basis;
- Reviewing the corporate risk register at each monthly meeting; and
- Advising the Director and Management Board with regard to major decisions affecting the management of risk within the PPS;

In reviewing the risk register, the range of issues considered by Management Board / Senior Management Group should include:

- Have any new significant risks been identified?
- Are risks previously identified still acceptable?
- Do risks need to be promoted or relegated in the corporate risk register?
- Do control strategies need to be changed?
- Do amendments need to be made to procedures?

### *Performance and Accountability Meetings*

Each Region / Section risk register is reviewed on a quarterly basis at the Performance and Accountability Meetings, led by the Deputy Director and SAD Serious Crime & Regions, attended by the Assistant Director / Business Manager.

### *Assistant Directors*

The responsibilities of Assistant Directors include:

- Agreeing the key risks, risk owners and controls to manage risks identified in the risk management framework at corporate and region / section level level as appropriate;
- Taking decisions affecting the management of risk within their area of responsibility;
- Monitoring the management and control of key risks to reduce the likelihood of unforeseen occurrence;
- Highlighting emerging risks or control weaknesses at Performance and Accountability meetings; and
- Ownership of the region / section risk register.

### *Risk Owners*

Each risk that is identified in a risk register will have a corresponding 'risk owner'. Ownership must sit at the appropriate level, ideally with the person who can take effective action. For example risk owners must 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 branch / unit. If a risk owner feels that they cannot take appropriate action, then the risk needs to be escalated to the next level.

They are also responsible for:

- Implementing the Service's risk management policy;
- Encouraging relevant staff to actively consider and manage risk;
- Communicating progress, identifying relevant control weaknesses and recommending remedial actions for their assigned risks; and
- Ensuring that a suitable system of internal control operates in their area of responsibility.

### *Line Managers*

All line managers are expected to:

- Work within the Service's policy on risk management;
- Alert management to emerging risks or control weakness; and
- Ensure appropriate controls are actioned within their own areas of work.

### *Audit and Risk Committee*

The Audit and Risk Committee (ARC) provides the Director 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 comprised of a non-executive chair and membership.

Although it has no authority in its own right over the operations of the organisation, the Committee:

- Supports the Director in monitoring the corporate governance and control systems (including the risk management framework) in the organisation; and
- Assists the Management Board, in an advisory function, in discharging its responsibilities with respect to overseeing all aspects of financial reporting and audit functions.

The ARC 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;
- Reviewing the effectiveness of the controls;
- Considering any new risks that may have emerged;
- Assessing the current status of major risks; and
- Considering quarterly assurances provided by risk owners and at the year-end and advising the Director on the Governance Statement.

#### *Internal Audit*

Internal Audit provides an independent and objective opinion on risk management, control and governance arrangements, by measuring and evaluating their effectiveness in achieving the Service's agreed objectives.

The Head of Internal Audit provides the Director with an independent opinion on the management and control of risk through the completion of individual audit assignments which are agreed annually by the Management Board and the Audit and Risk Committee. Additionally, findings and recommendations assist management in the audited business areas in strengthening their risk management and internal control processes and procedures.

#### *Northern Ireland Audit Office*

The Northern Ireland Audit Office (NIAO) is headed by the Comptroller and Auditor General (C&AG) and is independent of Government. NIAO audits the accounts of all Government Departments and other public bodies. While the Governance Statement, which forms part of the annual 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.

A representative from NIAO may attend Audit and Risk Committee meetings at which corporate governance, internal control and risk management matters are considered

### *Central Management Unit*

The PPS Central Management Unit (CMU) supports the development of the Annual risk management framework as an integral part of the business planning cycle by coordinating the initial completion and monitoring of the corporate risk register.

Within the risk management framework, CMU also:

- Provide the secretariat function to the Audit and Risk Committee;
- Provide advice on risk management to managers;
- Arranges appropriate training for managers; and
- Acts as 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.

### **13. Other Areas of Risk Assessment**

In addition to identifying key risks against the Service's strategic business objectives and associated targets, risk assessments are also conducted against specific areas of the business.

Examples of other areas of risk assessment are attached at Annex 7.

### **14. Useful References**

Useful references and websites which cover the risk management process are listed at Annex 8.

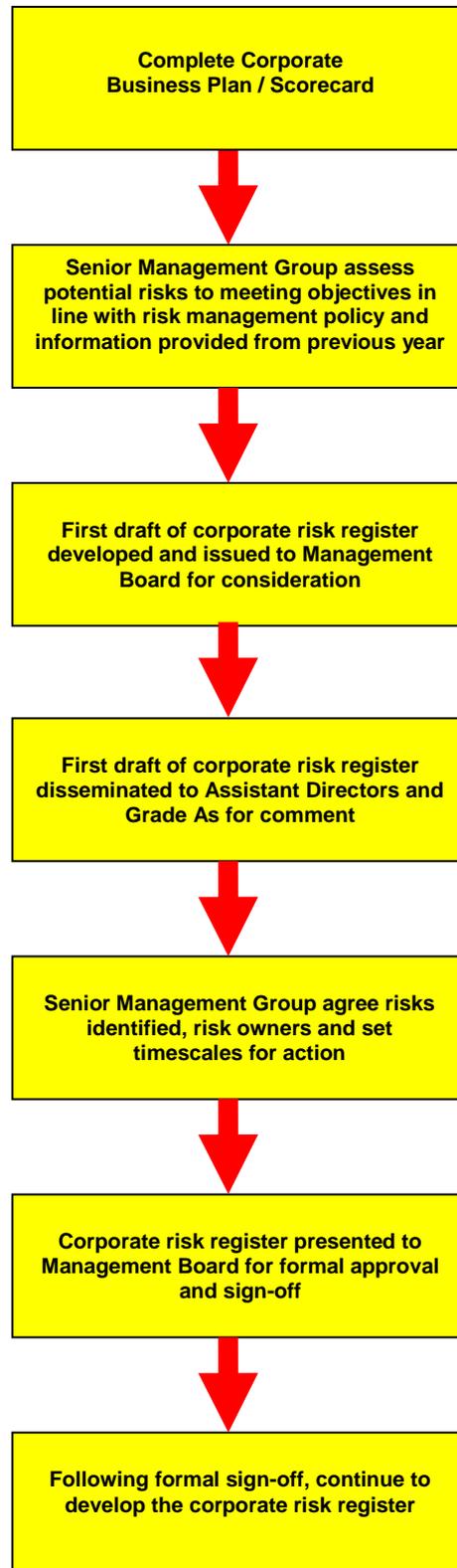
### **15. Review**

This policy and framework will operate for an initial period of two years after which it will be reviewed to take into account the changing circumstances under which we operate.

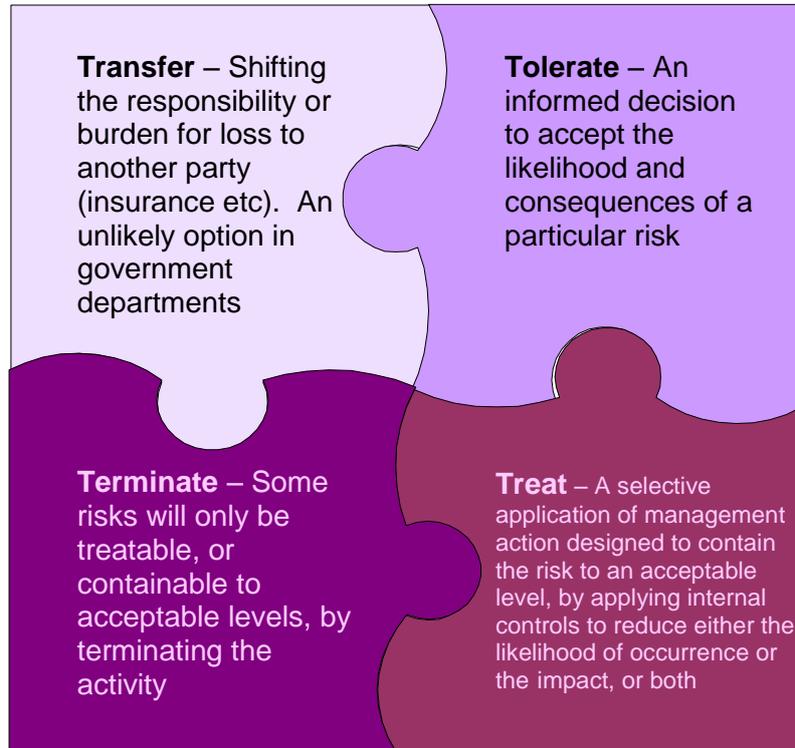
## ANNEX 1: COMMON CATEGORIES OF RISK

|  |  |
|--|--|
| <p><b>External</b></p> <ul style="list-style-type: none"> <li>• Political: political constraints/pressures.</li> <li>• Security: developments in the security/public order situation.</li> <li>• Legal and Regulatory: e.g. equality, regulatory and propriety.</li> <li>• Infrastructure: transport for staff, power supply, suppliers, business relationships with partners, dependency on internet and email.</li> <li>• Economic: interest rates, exchange rates, inflation.</li> <li>• Environmental: fuel consumption, pollution.</li> <li>• Market: competition and supply of goods.</li> <li>• “Act of God”: fire, flood, earthquake.</li> </ul> | <p><b>Activity</b></p> <ul style="list-style-type: none"> <li>• Policy: appropriateness and quality of policy decisions.</li> <li>• Departmental Security: protecting people, buildings, information.</li> <li>• Operational: procedures employed to achieve particular objectives.</li> <li>• Information: adequacy of information used for decision making.</li> <li>• Reputation: public reputation of the organisation and consequent effects.</li> <li>• Technological: use of technology to achieve objectives.</li> <li>• Project: project planning and management procedures.</li> <li>• Innovation: exploitation of opportunities to make gains.</li> </ul> |
| <p><b>Financial</b></p> <ul style="list-style-type: none"> <li>• Budgetary: availability and allocation of resources.</li> <li>• Fraud or theft: unproductive loss of resources.</li> <li>• Capital investment: making appropriate investment decisions.</li> <li>• Liability: the right to sue or be sued in certain circumstances.</li> </ul>  | <p><b>Human Resources</b></p> <ul style="list-style-type: none"> <li>• Personnel: availability and retention of suitable manpower skill mix.</li> <li>• Health and Safety: safeguarding staff, clients and the public.</li> <li>• Equality: equal treatment for all.</li> <li>• Data Protection: protecting individuals rights under legislation.</li> <li>• Training / Development: access for all to meet training and development needs.</li> </ul>   |

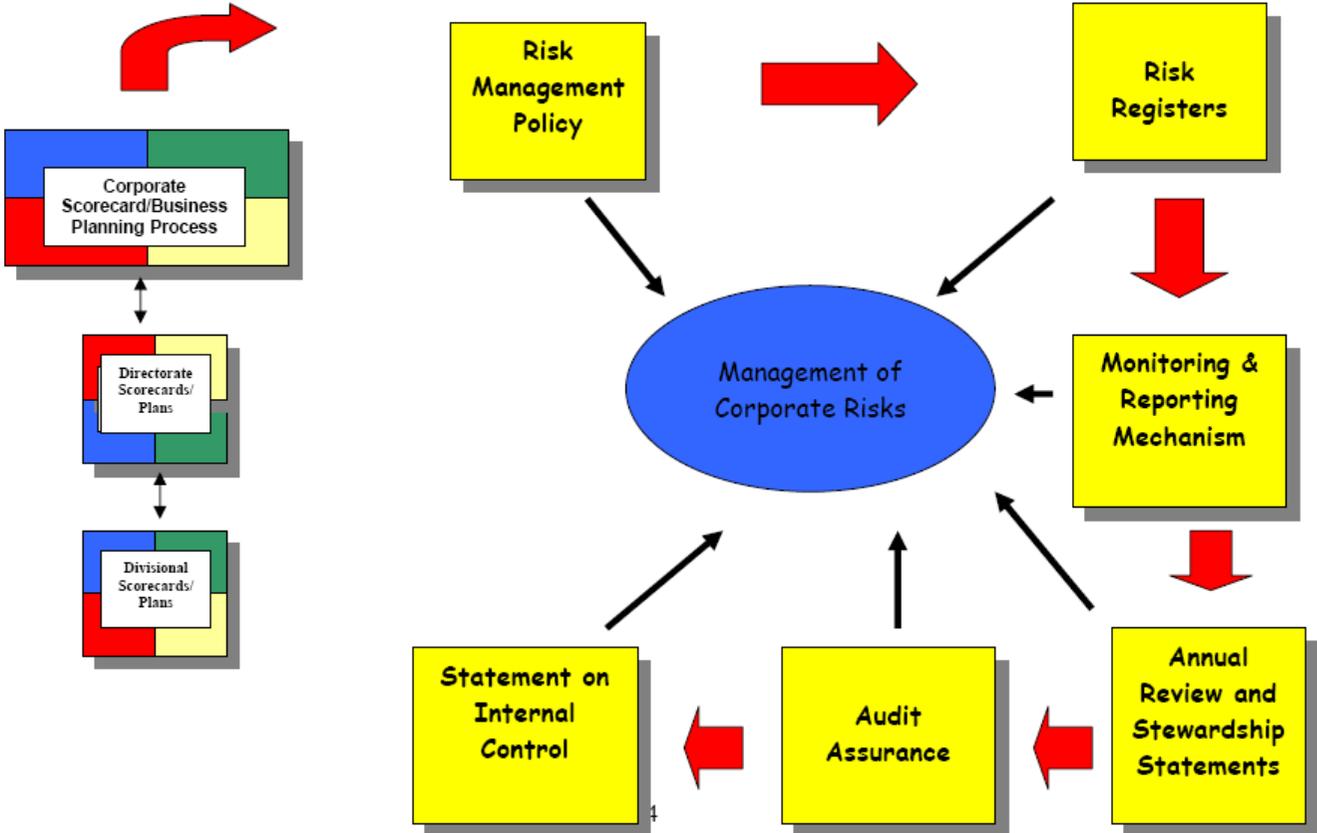
## ANNEX 2: RISK IDENTIFICATION PROCESS – PPS CORPORATE RISK REGISTER



## ANNEX 3: POSSIBLE RESPONSES TO RISK



**ANNEX 4: CORPORATE RISK MANAGEMENT PROCESS**



## ANNEX 5: RISK APPETITE AND TOLERANCE

### Purpose and Definitions

The PPS strategy for controlled and structured improvement in performance is founded on innovative policy and process development. The extent to which the PPS is prepared to 'push the boundaries' (the risk appetite) must be carefully balanced against the advantage of higher delivery and the consequences of failure (the risk tolerance).

### The Risk Appetite Framework

Whilst core activities across operational PPS Regions and Sections are broadly similar, it would be too simplistic to apply the same level of risk appetite across all parts of the Service. However it is essential that any variations are set in a context which defines a coherent decision making framework for those involved in operational areas and provides the Director and Management Board with an assurance that effective control measures are in place.

This framework defines the extent to which risk is encouraged and tolerated across the Service's responsibilities. It provides a profile which identifies the areas of high and low risk tolerance and indicates where it **may** be necessary to refer decisions up the chain of command. The latter is generally referred to as 'risk escalation'.

Treasury guidance outlines 25 risk areas that apply to government business<sup>1</sup> (see table below). These have been adapted to fit PPS business needs to produce seven primary risk groups against which risk tolerance levels are assessed.

1. Legal and Professional Standards;
2. Policy & Guidance;
3. Processes and service delivery;
4. Human Resources;
5. Regularity, Propriety and Accountability;
6. Reputation; and
7. External.

#### 1. Legal and Professional Standards

The aim of the PPS is to deliver a fair, independent and effective prosecution service. In the interests of justice, all actions must be undertaken with complete impartiality, to the highest ethical and professional standards. Prosecutions may only be initiated by the PPS where it is satisfied that the Test for Prosecution is met. At all times prosecutors working for, or on behalf of the PPS, must act in accordance with the Code for Prosecutors and Code

---

<sup>1</sup> "Management of Risk - A Strategic Overview" (HM Treasury)

of Ethics as issued by the Director of Public Prosecutions. As a result, this is an area where the tolerance of failure or non-compliance is low and hence the risk appetite should be **LOW** with associated levels of control to ensue an extremely low residual risk.

## **2. Policy and Guidance**

The PPS, as a relatively young body, is concerned with the delivery of change in many areas of work. If policy initiatives are to effect improvements, value for money etc., a high level of innovative thinking is often required. Too much control would tend to lead to over-cautiousness and stifle innovation. However the development of policy must consider potential negative impacts on reputation and legal and professional standards. Accordingly the PPS appetite for risk-taking in these areas is **MEDIUM**, *provided appropriate controls are in place in the form of consultation with staff and stakeholders, proper management scrutiny etc. as appropriate.*

## **3. Processes and Service Delivery**

As outlined above, the PPS is concerned with the delivery of change and improved services and therefore innovative thinking is required in all aspects of service delivery (e.g. through the use of ICT or re-engineering of processes) if radical improvements are to be achieved. Therefore the PPS appetite for risk-taking in these areas is **HIGH**, *provided that appropriate controls are in place in the form of consultation with staff and stakeholders, pilot projects, gateway reviews, management scrutiny etc. as appropriate.*

## **4. Human Resources**

Human Resource risk mainly involves 'people' issues that affect business continuity and everyday working – e.g. recruitment, equal opportunities, security, health and safety etc. These require precision and are largely 'prohibited' risk areas i.e. where compliance with organisational policies and guidance is mandatory. As a result this is an area where the tolerance of failure is low and hence the risk appetite should be **LOW** with associated levels of control to ensue a very low residual risk.

## **5. Regularity, Propriety and Accountability**

The PPS must comply with a wide range of central initiatives and Government standards. These include regulations and codes on regularity, propriety and accountability – particularly in relation to financial management. This requires compliance with mandatory central guidance and therefore the risk appetite has to be **LOW** and needs to be supported by very high levels of control.

## **6. Reputation**

The Service needs to maintain its reputation with key stakeholders and to maintain public confidence in its fairness and effectiveness as a prosecution service. It therefore has a low risk appetite in this area. On the other hand

the PPS is an organisation undergoing continuous change and which cannot avoid an element of risk taking if it is to achieve the desired outcomes. It also takes risks with its capability for delivering existing and new areas of work (e.g. via new ICT systems) even though failure to deliver could damage its reputation.

In addition it is recognised that the PPS must deliver a prosecution service which is independent of political, public or other pressures and in some instances decisions (*whilst fully in accordance with the PPS Test for Prosecution*) may not be viewed positively within the wider community. Therefore, on balance, the overall appetite for reputational risk is **MEDIUM** although this is a specific area where the final evaluation will depend on context.

## 7. External

The PPS has limited control over its exposure to external risks, such as economic change, infrastructure disruption etc. Efforts are made to mitigate the effects of such risks by introducing control factors e.g. business continuity planning and strict information assurance / security procedures and protocols. However there are circumstances where, regardless of pre-planning, situations emerge which cannot be predicted and where control is limited. Therefore the risk appetite in this area is assessed as **MEDIUM**.

## Conclusion

The result of this analysis is to provide a corporate framework for the risk appetite for the Service which looks like:

| Risk Category                            | Low | Medium | High |
|--|-----|--------|------|
| Legal and Professional Standards         |     |        |      |
| Policy & Guidance                        |     |        |      |
| Processes and Service Delivery           |     |        |      |
| Human Resources                          |     |        |      |
| Regularity, Propriety and Accountability |     |        |      |
| Reputation                               |     |        |      |
| External                                 |     |        |      |

## **Application of the Framework**

The framework sets out the context and risk profile for the Service. As a new policy or work area is developed, a risk assessment should be carried out which identifies the risk category and measures the level of risk using the Departmental risk matrix. Where the assessment shows that the level of risk is higher than the corporate profile for that category of risk, clearance should be sought by passing the assessment up the decision making chain.

## ANNEX 6: PPS RISK REGISTER TEMPLATE

| Risk Summary     |            |  | Action Plan       |   |              |                        |                                  |              |                                     |                                    |  |
|------------------|------------|--|-------------------|---|--------------|------------------------|----------------------------------|--------------|-------------------------------------|------------------------------------|--|
| Risk Description | Risk Owner | Inherent Assessment<br>(as at 1/4/xx ) | Controls in place | Residual Assessment<br>(After Mitigation) |              |                        | Planned Actions to Mitigate Risk | Action Owner | Original target date for completion | Current target date for Completion | Anticipated Risk Assessment (after planned mitigating Actions) |
|                  |            |  |                   | Likelihood (1-4)                          | Impact (1-4) | Current Rating (R/A/G) |                                  |              |                                     |                                    |  |
|                  |            |  |                   |   |              |                        |                                  |              |                                     |                                    |  |

## ANNEX 7: OTHER AREAS OF RISK ASSESSMENT

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

**Business Resilience:** All business areas have a responsibility to develop & maintain a Business Continuity Plan to deal with disruption at a local level - e.g. in the event that staff are unable to gain access to a building or there is disruption to the delivery of key services.

**Health & Safety:** Risk Assessments on the work environment are carried out by designated Risk Assessors on a quarterly basis and when deemed necessary e.g. redesign of office layouts.

**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.

**ICT 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, specifying the measures taken to manage risk in accordance with government approved standards. Ultimately accreditation is a statement confirming that the use of the system to process, store and/or forward protectively marked information does not present an unacceptable ongoing risk to the business of the Public Prosecution Service.

## ANNEX 8: USEFUL REFERENCES AND WEBSITES

### *References*

- The Orange Book - Management of Risk – Principles and Concepts (Oct 2004). HM Treasury
- The Audit Committee Handbook. HM Treasury
- OGC Management of Risk: Guidance for Practitioners, HMSO
- DAO (DFP) 3/12 - Governance Statement
- DAO (DFP) 06/13 - Corporate Governance in Central Government Departments Code of Good Practice NI 2013

### *Websites*

- Her Majesty's Treasury <http://www.hm-treasury.gov.uk>
- Northern Ireland Audit Office <http://www.niauditoffice.gov.uk>
- [www.gov.uk/government/organisations/cabinet-office](http://www.gov.uk/government/organisations/cabinet-office)