

Police Service of Northern Ireland

PD 05/04

POLICY DIRECTIVE

RISK MANAGEMENT POLICY

1. POLICY IDENTIFICATION

POLICY TITLE: Risk Management Policy

POLICY OWNERSHIP:

DEPARTMENT	Operational Support
BRANCH	Corporate Development
AUTHOR	Inspector Corporate Development

POLICY APPROVED BY:

CCF REF/OTHER	Audit and Risk Committee
DATE OF APPROVAL	28 June 2004

IMPLEMENTATION DATE: 28 June 2004

DATE OF ISSUE: 26 November 2004

DATE VERSION 2 ISSUED: 30 July 2007

REVIEW DATE: 29 July 2008

INDEX

SECTIONS 1- 6

Section	Subject	Page
1	Policy Identification Page	1
2	Policy Statements	3
3	Introduction	3
3(1)	Background	3-4
3(2)	Approach to Risk Management	4-5
3(3)	Legislative Requirements	5
4	Implications of the Policy	5
4(1)	Efficiency	5
4(2)	Bureaucracy	5
4(3)	Consultation	5
5	Human Rights/Equality/Integrity/Freedom of Information	5
6	Review	5-6

SECTION 7

Paragraph

Procedures and Guidance

1.	Risk Management	7-8
2.	Risk Registers and the Management of Risk	8-13
3.	Glossary	14-20
4.	Roles and Responsibilities	20-23

Appendices

Appendix 'A'	Stewardship Statement	24
Appendix 'A'	Stewardship Statement	25

2. POLICY STATEMENTS

- (1) The Police Service of Northern Ireland (PSNI) recognises the importance of managing risk in the achievement of its aims, objectives and policies. The PSNI will ensure it has internal controls that provide assurance that it is providing policing at its best.
- (2) Policing involves inherent risks. We can never totally avoid risk in the delivery of a professional, progressive policing service. The PSNI approach to risk is therefore focused on effectively managing risk to an acceptable level. When properly employed, risk management provides an opportunity to improve our service delivery and should never be viewed as a mechanism for not taking action or making difficult decisions.

3. INTRODUCTION

(1) Background

- (a) Risk management is one of a series of processes designed to provide assurance that a sound system of internal control is in place and operating effectively. It is a requirement of HM Treasury that all public bodies have such processes and procedures in place. This Risk Management Policy has been developed in line with best practice as defined by HM Treasury and the Office of Government Commerce.
- (b) In order to meet Treasury requirements, PSNI has developed this Risk Management Policy. Risk management means having in place a corporate and systematic process for identifying and evaluating the risks associated with the activities and responsibilities of PSNI, assessing and addressing their impact and providing for appropriate disclosure of the progress made in managing the risks identified. The Policy explains the PSNI approach to risk management, documents the roles and responsibilities of the Chief Constable, senior management and other relevant parties such as line management, and provides detailed guidance on how risk management is to be operated by all members of the organisation.
- (c) PSNI recognises that risk management is not an end in itself, but a process, which will contribute to a range of benefits. These include:
 - (i) better service delivery;
 - (ii) increased certainty and fewer surprises;
 - (iii) more effective management of change;
 - (iv) more efficient and effective use of resources;
 - (v) minimising waste, fraud and poor value for money;
 - (vi) more innovative approaches to the delivery of objectives;
 - (vii) improved strategic and operational planning;
 - (viii) Improved decision making.
- (d) Given the potential benefits involved, PSNI's Policy with regard to risk management is as follows:
 - (i) Risk management should be embedded in the line management processes of PSNI.
 - (ii) The Chief Constable's Forum (CCF) owns, supports, promotes and accepts leadership responsibility for the adoption of risk management procedures and practice throughout the organisation.

- (iii) CCF has developed a corporate risk register, which clearly sets out the key strategic risks facing the organisation and how they are managed. The risk register will be reviewed and updated by CCF and updated as necessary on a monthly basis. The Corporate Risk Register will also be reviewed on a quarterly basis by the Audit and Risk Committee and any recommendations from the committee will be reported to CCF on a timely basis.
- (iv) Departmental and District Command Unit registers will be maintained, reviewed and updated as necessary on a monthly basis.
- (v) Branches and other operational units/areas will maintain risk registers if deemed appropriate by the relevant Head of Department or DCU Commander.
- (vi) The Accounting Officer (Chief Constable) will make an annual public statement on the operation of internal controls put in place to manage risks. This will be informed inter alia by assurance statements provided by CCF members on the operation of controls within their areas of responsibility.

(2) Approach to Risk Management

- (a) This Policy explains the underlying approach to Risk Management.

As Accounting Officer for the PSNI, the Chief Constable has responsibility for maintaining a sound system of internal control that supports the achievement of PSNI's policies, aims and objectives, set by the Northern Ireland Policing Board (NIPB), whilst safeguarding the public funds and assets for which he is personally responsible, in accordance with the responsibilities assigned to him in Government Accounting.

- (b) The system of internal control, with regard to risk management, is designed to manage rather than eliminate the risk of failure to achieve policies, aims and objectives. It can therefore only provide reasonable and not absolute assurance of effectiveness.
- (c) The system of internal control is designed to:
 - (i) Identify and prioritise risks to the achievement of organisational policies, aims and objectives;
 - (ii) To evaluate the likelihood of those risks being realised and the impact should they be realised; and
 - (iii) To manage them efficiently, effectively and economically, using appropriate controls and techniques.
- (d) The following key principles underline PSNI's approach to risk management:
 - (i) PSNI recognises the importance of making prudent assessment and disclosure of the financial and non-financial implications of risks;
 - (ii) The Chief Constable has overall responsibility for risk management within the organisation;
 - (iii) CCF encourages management to adopt an open and receptive approach to discussing and addressing risks at all levels within PSNI;
 - (iv) DCU Commanders and Departmental Heads are responsible for risk management within each business area and are also responsible for notifying CCF where exposure to risks are of a material nature. Where it is considered appropriate, Departmental Heads may institute branch level risk registers;
 - (v) The actual risk management system shall be owned by line management and be co-ordinated by the Corporate Risk Manager on behalf of ACC Operational Support who will report to CCF and the Audit and Risk Committee on specific risk related matters;

- (vi) Annual reports will be made by ACC Operational Support via the Audit and Risk Committee to CCF as to the nature and management of significant corporate risks identified.

(3) **Legislative Requirements**

Although there is no legislative requirement to adopt a Risk Management Policy, the Chief Constable is obliged as Accounting Officer to sign a Statement of Internal Control that is published as part of PSNI's annual accounts. This reflects Association of Chief Police Officers (ACPO) and Office of Government Commerce (OGC) good practice recommendations and confirms that effective corporate governance processes have been in place throughout the year across the organisation.

4. IMPLICATIONS OF THE POLICY

(1) **Efficiency**

For PSNI, implementation of risk management across the organisation (reflecting ACPO and OGC good practice recommendations) will bring significant benefits. It will assist in identifying key strategic and operational risks, which may prevent PSNI from delivering against core objectives and targets. The process is inextricably linked to the development of corporate and operational plans and other projects, which are currently ongoing throughout the organisation. Identification, evaluation and control of risk at all levels enhances efficiency, encourages effective management of resources and assists the organisation in achieving its core objectives.

(2) **Bureaucracy**

- (a) Application of this Policy will require some minor additional administration by those involved in the process.
- (b) It will however, place no additional bureaucracy on those involved in front line policing.

(3) **Consultation**

The following have been consulted in relation to this Policy:

- (a) PSNI's Top Team;
- (b) Audit and Risk Committee;
- (c) Association of Chief Police Officers;
- (d) HM Treasury.

5. HUMAN RIGHTS/EQUALITY/INTEGRITY/FREEDOM OF INFORMATION

- (1) This Policy Directive and accompanying Procedure is deemed to be Human Rights compliant. It has been screened for Section 75 considerations and meets the organisations integrity standards.
- (2) This Policy is suitable for public disclosure in accordance with the Freedom of Information Act 2000 however the accompanying Guidance Manual is suitable for internal dissemination only.

6. MONITORING AND REVIEW

- (1) This Policy was first approved in June 2004 by the Audit and Risk Committee.
- (2) The Corporate Risk Manager is responsible for reviewing the contents of this Policy on an annual basis.
- (3) This Policy was subsequently reviewed in December 2006 by the Corporate Risk Manager.

- (4) The Audit and Risk Committee reviewed this Policy in January 2007.
- (5) CCF approved this policy in April 2007.
- (6) Feedback relating to this Policy should be made to the Risk Manager, Corporate Development Branch, Operational Support Department.

SECTION 7

PROCEDURES AND GUIDANCE

1. RISK MANAGEMENT

(1) What is Risk Management?

Following several high profile failures in the public and private sectors during the 80s and 90s, government increasingly focused on providing assurance to stakeholders that large corporations and public bodies were subject to good governance. The management of risk has emerged as a key method of providing such assurance. Risk management enables us to strike a balance between progress and change on the one hand, and failure and confusion on the other. In the private sector, risk management is frequently applied to opportunities as well as threats. Experience in the public sector shows that risk management tends to focus more on threats, however when applied to opportunities, it provides key information to decision makers on the viability of new projects. It complements the planning process and provides another layer of control to managing performance. Used appropriately, it can provide us with the confidence and authority to take on new challenges because the risks to our business have been identified, understood and controlled. Put simply, Risk Management is Good Management.

(2) The key benefits of risk management are summarised below:

- (a) Provides a framework for control;
- (b) Encourages improved and better informed decision making;
- (c) Enables efficient allocation of resources;
- (d) Affords increased certainty and fewer surprises;
- (e) Protects and enhances image;
- (f) Improves operational effectiveness/efficiency;
- (g) Facilitates better service delivery;
- (h) Enables more effective management of change;
- (i) Minimises waste, fraud and poor value for money;
- (j) Promotes more innovative approaches to the delivery of objectives;
- (k) Improves strategic and operational planning.

(3) Who is involved?

Managing risk is the responsibility of all staff, however there are roles within the process which carry major responsibility and are crucial to the successful management of risk.

These are:

(a) The Accounting Officer:

This is the senior manager in the organisation, who is ultimately responsible for the management of risk and for providing assurance to stakeholders that sound systems of internal control are in place and are effective. In PSNI this role is fulfilled by the Chief Constable.

(b) Risk Director:

This is the senior manager in the organisation responsible for the management and co-ordination of the organisation's risk policies and activities. In PSNI this role is fulfilled by the Assistant Chief Constable, Operational Support.

(c) Risk Owners:

These are senior managers responsible for the identification, evaluation and control of risks within their specific area of responsibility. They are also responsible collectively for the management of risks which have strategic or cross-departmental implications for the organisation. In PSNI this role is fulfilled by Heads of Department and District Commanders.

(d) Risk Action Owners:

These are managers with responsibility for implementing risk control measures and reporting progress to Risk Owners.

(e) Corporate Risk Manager:

This person has responsibility for co-ordinating and overseeing the risk management processes and systems in place at all levels within the organisation. The Corporate Risk Manager performs this function on behalf of the Risk Director. In PSNI this role is assigned to an Inspector, Policy Planning & Performance.

(f) Risk Managers:

Risk Managers maintain risk registers on behalf of risk owners and provide administrative support to the risk management process within their area of responsibility. This role is often performed alongside other administrative and business management functions. In PSNI this role is performed by a suitable person appointed by the relevant District Commander/Head of Department.

Further detail on these and other roles can be found on pages 20-23.

2. RISK REGISTERS AND THE MANAGEMENT OF RISK

(1) What is a risk register?

Risk registers document the nature and extent of risks and record the actions taken to control the risk and mitigate their effects. A risk register will typically contain at least 6 risks and no more than 12. In theory, the risk register is a dynamic document which is updated regularly and whose content will change frequently as risks are "managed out" and new risks emerge. There is therefore no requirement for a "yearly" risk register. In practice, the publication of the policing plan provides an annual opportunity to fundamentally review the risk register and to restart the risk management process. This is because risks are intrinsically connected to business objectives and it is the policing plan that sets those objectives for the coming year. It follows that the first step in risk management should be a consideration of the objectives contained in the policing plan. There may also be risks falling outside business objectives, which have the potential to cause disruption or failure of core duties and responsibilities and these should also be considered.

(2) Completing the Risk Register

A risk register is the primary tool used in the management of risk and reflects the roles responsibilities and techniques associated with the process. The following guidance therefore, defines each step of the process, maps it on to the risk register, and provides advice on how to complete each section. Reference to distinct roles and other key definitions are highlighted. These roles and definitions are explained further in the glossary at the end of the Guidance Manual.

(3) **Managing the Risk Register**

- (a) The Risk Register will be reviewed and updated on a monthly basis at the NIM T&CG meeting. Each risk on the register will be considered in turn and with a view to establishing:
- (i) The effectiveness of risk actions;
 - (ii) The achievement of risk actions;
 - (iii) The current status of the risk (residual risk rating);
 - (iv) The requirement for the risk to remain on the register;
 - (v) The emergence of new risks for addition to the register.
- (b) The Risk Owner and the management team are responsible for ensuring that risk is managed appropriately and effectively and should ensure that any relevant information or decision emerging from the NIM meeting is communicated to the Risk Manager as soon as possible.

(4) **Identify & Describe**

The first step in the process is to identify the risks to your business objectives. Taking each objective in turn, consider what events could threaten their achievement.

Identify all of the risks to your **business objective**. Consider all risks, however insignificant or serious they appear to be at this stage. A useful tool for identifying risk is the **Bowtie Matrix**. This tool allows for detailed examination of risks associated with an issue or event.

- Begin your risk description with the words “There is a risk that...”
- Describe the risks in the following way: **Event – Consequence**

Risks are frequently described as one or the other, resulting in vagueness and confusion.

“lack of resources” frequently appears on risk registers, as does *“failure to meet agreed targets”*. However one is an event, the other is a consequence. Descriptions of risk should always combine the two AND be directed towards a defined business activity, for example:

“There is a risk of a failure to appoint suitably trained investigators resulting in reduced detections and clearances”

This description combines a lack of resources and failure to achieve targets but is more specific and focused thus allowing for a more specific and focused response.

(5) **Evaluate**

Most risks will be deemed acceptable or insignificant. It therefore important to prioritise risks in order to concentrate responses to the most serious risks. This is best achieved using the **Risk Assessment Matrix**. The matrix will also provide an **Inherent Risk Rating**. Typically, this will result in the selection of between 6 and 12 risks to be placed on the risk register. Those risks which have not been prioritised *are still risks*. These should be noted and communicated to all staff involved.

(6) **Assess and Analyse the Risk**

This is the intermediate stage between knowing what the risk is and deciding how to handle it. Professional judgement, problem solving and decision-making skills are all required to ensure that identified risks are subject to appropriate controls.

Consider any events which may provide early warning that the risk is occurring and will have an effect on the business objective. This can assist in deciding what **Treatment or Controls** are required. Much of this information may be obtained from reviewing the **Bowtie Matrix** used at the **Identification** stage, however all available information and expertise should be considered

(7) **Treatment and controls**

There are two types of controls – **Existing Mitigation** and **Risk Actions**. Both should be considered in turn and listed. When the existing mitigation has been considered, the risk rating should be revisited and revised if appropriate;

For example, if there are existing policies, checks or initiatives in place, which will make the risk less likely to happen, or have less of an impact if it does, then the risk rating should be reduced. This provides a **Residual Risk Rating**.

Further control measures can then be devised to further mitigate the risk. These should be listed with target dates for completion and assigned to a named individual (**Risk Action Owner**) who will have responsibility for carrying out the action and reporting on compliance. As risk actions are completed the residual risk rating should be revisited and revised if necessary.

Risk Actions are aimed at:

Prevention – Removal of the cause of the risk

Reduction – Curtail the impact or lessen the likelihood of the risk

Avoidance – Alternative courses of action to achieve objectives which do not involve risk

Control – Acceptance of the risk but with measures in place to ensure it is appropriately controlled

Transfer – The risk is passed to a third party and becomes their risk.

(8) **Monitor**

Responsibility for monitoring the risk and directing how it will be controlled lies with the **Risk Owner**. Monitoring should occur on a monthly basis when all risks are reviewed at TCG meetings. Any changes, including; completed actions, new actions, personnel changes and realignment of target dates should be notified to the **Risk Manager** who will update the risk register.

As actions are completed the **Residual Risk Rating** may be revised and reduced to the extent that the risk is no longer significant. At this stage the risk may be removed from the risk register.

Consideration should also be given as to whether any risk is sufficiently serious to warrant **Escalation** to the next level of management.

(9) **Review**

The risk register is subject to ongoing review via the TCG process, however a more structured formal review should take place at six monthly intervals. These should take place in March and September to coincide with the planning cycle and ACC Accountability ("Patten 78") meetings. A Formal Review should consider the following questions.

- Are the identified risks still the most significant?
- Are target dates for actions being met?
- Have any new risks been identified?
- Are control measures effective?
- Overall, is there an effective risk management process in place

The March review should consider risks to the annual policing plan objectives.

Following these 6 monthly reviews, a **Stewardship Statement** should be prepared and forwarded to the Corporate Risk Manager






(10) **Managing Risks**

- (a) The risk register is discussed monthly at T&CG meetings under the NIM process of structured management meetings. Each risk on the register should be considered in turn and the owner of the risk required to provide a report on how the risk is being managed, it's current status (risk rating) and any new actions to be included.
- (b) In addition the meeting should consider removing risks from the register (due to reduced impact/probability) and adding new or emerging risks which have been identified as significant.
- (c) The Risk Register documents the identification, evaluation and treatment of risks and allows effective monitoring and review of actions taken in respect of the risk. It is maintained by the risk manager, on behalf of the risk owner, using Topease. A sample of the risk report generated by Topease is reproduced below with descriptions of the content of each section. On the following page, a completed Risk Register entry is reproduced by way of example.

Risk	Risk Rating
A description of the risk in the following format: Event – consequence.	Impact: From risk assessment matrix Likelihood:
Number each risk 01, 02 etc for identification purposes	Residual Risk Rating
	Impact Category: Rating following the consideration of controls in place Impact: Likelihood:
Risk Owner (Responsibility)	Specific Objective (Poses a threat to)
Named individual. Typically a Chief Officer, Dept Head, Head of Branch or DCU Commander	☰ From Policing Plan
Risk Indicators	Potential business implications
Early warning indicators. Events which may indicate that the risk is occurring.	The consequences or actual impact of the risk upon the business objectives, should the risk occur.
See Bowtie Matrix	See Bowtie Matrix
Potential root causes (Reason)	How is this risk currently managed (Existing Mitigation)
Self explanatory	Control measures already in place which will have a mitigating affect on the risk

Additional Actions required to fully manage the risk	Criticality (H,M,L)	Owners (Concerned Party)	Estimated Date (Start)	End Date
List of other treatments and control measures which can be put in place to mitigate against the risk. Number each action 01, 02 etc for identification purposes.	High Medium or Low	The Risk Action Owner . The specific person assigned with the responsibility of carrying out each risk action.		

Example

Risk		Risk Rating		
01. There is a risk of insufficient resources/skills base to deal with major incidents/public disorder, leading to a lack of public confidence.		Impact: Serious (3) Likelihood: Very Likely (3)		
		Residual Risk Rating		
		Impact Category: Injury Impact: Significant (2) Likelihood: Possible (2)		
Risk Owner (Responsibility)		Specific Objective (Poses a threat to)		
 Supt AN Other (Operations Manager)		 1.0 To continue to build, broaden and sustain public confidence in the Police		
Risk Indicators		Potential business implications		
Increase in public disorder incidents.		Loss of public confidence/public criticism.		
Increase in number of officers injured as a result of disorder.		Bad media publicity.		
Decrease in number of arrests for public order type offences.		Costs resulting from injured officers.		
Increase in number of complaints against police arising from public disorder.		Increase in number of public disorder incidents.		
Reduced availability of level 2 trained officers.				
Potential root causes (Reason)		How is this risk currently managed (Existing Mitigation)		
High percentage of probationary officers in District Command Unit		Provision of relevant training.		
Lack of officers with significant length of service.		Compliance with planning process for major incidents/public order events.		
Lack of training.		Risk Assessments regularly reviewed.		
Lack of local knowledge.		Bids for TSG support at major incidents/public order events.		
High turnover of officers in district.				
Additional Actions required to fully manage the risk	Criticality (H,M,L)	Owners (Concerned Party)	Estimated Date (Start)	End Date
01. Consider physical measures to improve safety/reduce potential for disorder	H	 Supt AN Other (Operations Manager)	01/04/2006	31/12/2006
02. Increase dialogue with community representatives to reduce disorder around major incidents/public order events	H	 Supt AN Other (Operations Manager)	01/04/2006	31/12/2006
03. Increase use of CCTV/video evidence	H	 D/Inspector Person (Crime Manager)	01/04/2006	31/03/2007

3. GLOSSARY

(1) Bowtie Matrix

- (a) The bowtie matrix is a tool, which can be used to identify risks surrounding a particular issue or event. It can subsequently be used to decide on appropriate control measures.
- (b) By working outwards from any issue or event of concern, it can be used to specify the associated causes and consequences. This assists in the process of identifying and describing risks as part of the risk management process. In addition, the identification of causes and consequences can trigger the identification of appropriate controls.
- (c) There is no requirement to use the Bowtie Matrix for every risk, however it can be useful in “mapping out” all the elements of any particular risk.
- (d) A blank template and example of a completed Bowtie Matrix as it may be applied to a specific risk are reproduced on the following pages.

(2) Business Objective

- (a) The relevant objective(s) from the policing plan which are affected by the risk.

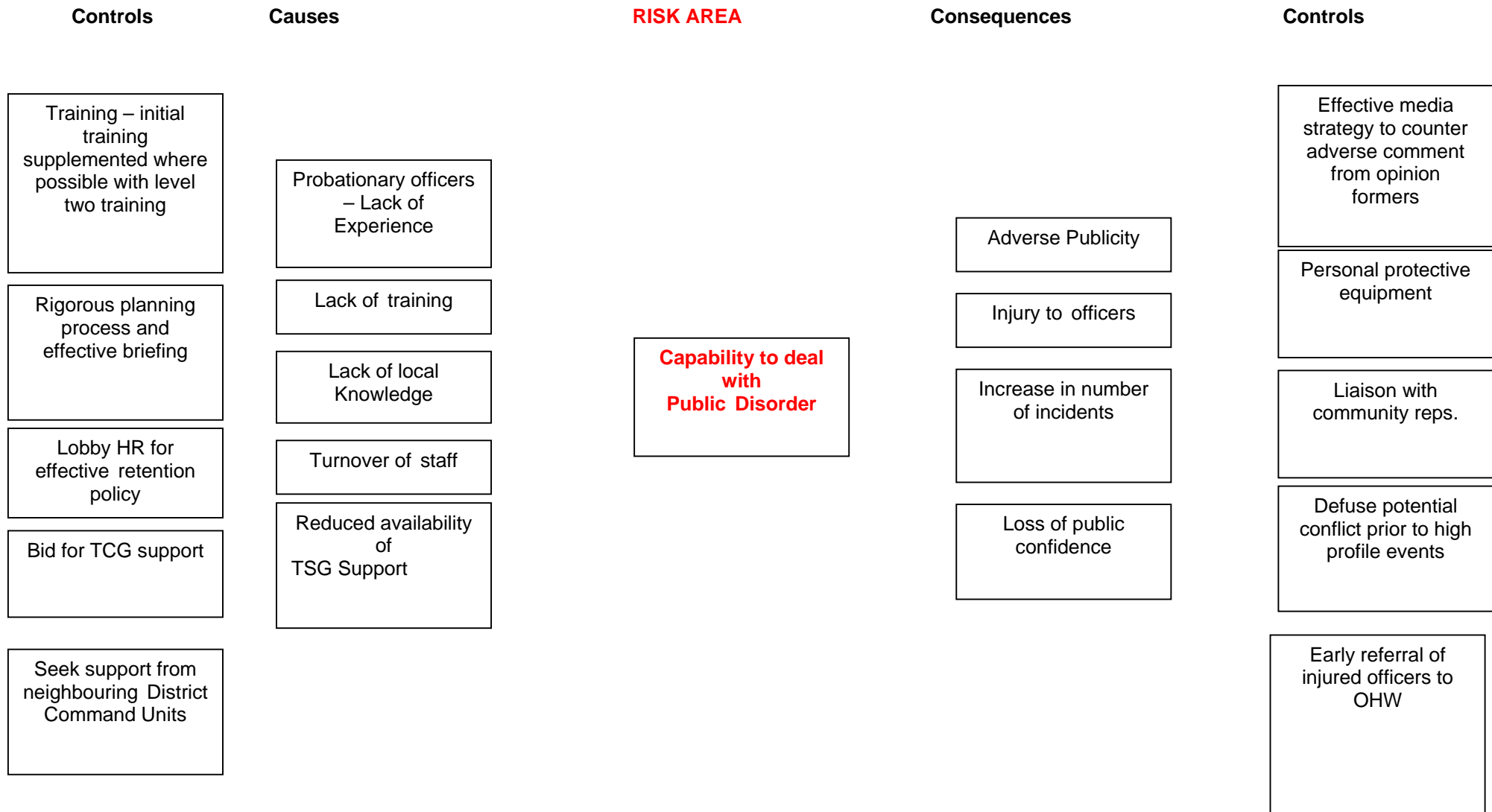
For example:

“There is a risk that we will fail to manage sickness levels resulting in impaired ability to deliver agreed crime reduction targets”.

- (b) The above risk is relevant to at least two objectives from the policing plan:

3.0 To reduce crime.

8.0 To improve effectiveness and efficiency.



Controls

Causes

RISK AREA

Consequences

Controls

(3) Escalation/Cross-Departmental Risks

- (a) It is important that risks are managed at the appropriate level within the organisation. Risk owners should consider the significance of any identified risk to their District Command or Department/Branch. They should also consider whether a risk is sufficiently serious or wide ranging that it may impact on the wider organisation. If such a risk is identified, it should be raised with the next level of authority for consideration. This process is known as “**Escalation**”. It allows for risks to be monitored and controlled at an appropriate level, taking into consideration the seriousness of the risk to the overall activities of the organisation. If a risk is accepted at a higher level, then additional control actions may be put in place to treat the risk. This does not mean that responsibility for the risk is transferred to the higher level of authority. The primary management of the risk remains with the Dept, Branch or District Command Unit who identified it. The risk will therefore appear on two or more risk registers. The Corporate Risk Manager will be responsible for monitoring and co-ordinating the responses to escalated risks in consultation with risk owners.
- (b) In addition, the Corporate Risk Manager will conduct routine analysis of all risk registers to identify common themes or frequently occurring risks. Any matters identified as representing a wider or more serious risk will be notified via Head of Corporate Development to the appropriate level for consideration.
- (c) Occasionally, risks will involve responses from more than one department. It is important that the risk owner secures commitment and co-operation from risk action owners located in other departments before actions are placed on the risk register. Where a risk requires action from more than one business area, one named risk owner should be nominated to have overall responsibility for managing the risk and co-ordinating responses.

(4) Risk Assessment Matrix

- (a) Frequently the risk identification process will result in an unmanageable list of all the potential business risks. It is important to focus on those key risks that require careful management and attention. Risks are therefore prioritised using the risk assessment matrix. This matrix enables risk owners to plot the potential impact of any individual risk against the likelihood of the risk occurring. Put simply, ask the following questions:

If this were to happen, how serious would it be?

How likely is it to happen?

- (b) The answers are plotted on the matrix, giving a score of between 1 and 16. This score is the **Inherent Risk Rating**. The higher the score, the greater the importance assigned to the risk. When all risks have been plotted on the matrix, those with the higher ratings are transferred to the risk register, those with the lower ratings are noted and managed as appropriate.
- (c) It is recommended that no less than 6 and no more than 12 risks should be transferred to the risk register. This range is generally considered to be the most manageable and effective. These figures are for guidance and occasional increases or decreases in the amount of risk being managed are acceptable.
- (d) The matrix may also be used to assign a Residual Risk Rating, however this is often achieved by simple judgement of the effect of treatments and controls.
- (e) A reproduction of the **Risk Assessment Matrix can be found on the following page.**

Impact

Major	4	8	12	16
Serious	3	6	9	12
Significant	2	4	6	8
Minor	1	2	3	4

Unlikely Possible Very Likely Almost Certain

Likelihood

(5) **Risk Rating**

(a) There are two risk ratings on any risk register; **Inherent** and **Residual**

- (i) The **inherent risk rating** is a judgement of the impact and likelihood of the risk *if no action was taken*. The Inherent Risk Rating does not change once it has been assessed. The Inherent Risk Rating is therefore the first assessment of the risk after it has been identified.
- (ii) The **residual risk rating** is an assessment of the risk taking current treatment and controls into account.

(b) For example, if you have identified the following as a risk:

- (i) "There is a risk of a shortage of sufficient trained staff resulting in failure to complete Project X within agreed timescales"
- (ii) The inherent risk rating may be 9 (Very Likely/Serious).

(c) Following consideration of a range of existing controls, eg

Services of agency staff to offset short term absence
Using seconded staff for areas of work requiring specialist knowledge

(d) The resulting assessment of the impact/likelihood of the risk may result in a residual risk rating of 6 (Possible/Serious).

(e) As further risk actions are achieved the residual risk rating should reduce still further. The objective is to treat and control the risk until the residual risk rating is as low as possible. In some cases, a risk may be treated or controlled to the extent that it is no longer considered an important or significant risk. At this stage it may be decided to remove it from the register.

(6) **Stewardship Statements**

(a) Stewardship reporting is a key element of ensuring accountability and ownership of risks and their management within the organisation. It will involve members of CCF and all DCU commanders signing a Stewardship Statement on a half yearly basis, which confirms that over a period of time they have reviewed the risk registers for their respective areas of responsibility and assessed the management of the risks identified. Stewardship Statements are requested and collated by the Corporate Risk Manager in March and September. Heads of Department and District commanders may require Branch Heads and Area Commanders to provide Stewardship Statements to provide assurance that risk is being managed appropriately at those levels of the organization.

(b) Stewardship Statement Templates Appendix 'A' (as Head of Department) and Appendix 'B' (as Commander of District) are attached.

(7) **Treatment and Controls**

(a) Existing Mitigation

In almost any case, there are one or more measures already in place which may reduce the impact or likelihood of a risk occurring. For example, these might include regular monitoring, reporting structures to highlight problems or training already in place. These measures are considered when judging the residual risk rating.

(b) **Risk Actions**

Risk actions are further measures designed to deal with the risk, either immediately or over a period of time, which will further reduce the impact or likelihood of the risk. Risk Actions should be assigned to a Risk Action Owner who will have responsibility for ensuring that the action is carried out on time and reported on regularly to the Risk Owner. Risk Action Owners should always be named individuals. As risk actions are completed the residual risk rating should be re-assessed in light of a reduction in the impact/likelihood of the risk occurring.

(c) In general, treatment and control is aimed at:

- (i) Prevention;
- (ii) Reduction;
- (iii) Avoidance;
- (iv) Control;
- (v) Transfer.

(d) A brief outline of each these measures can be found on page 9. It should be noted that transference of risk is rarely appropriate as the impact of the risk occurring is usually unaffected. In many cases it is not risk, but blame which is transferred.

(e) For example:

There is an identified risk of catastrophic IT failure and responsibility for managing this is transferred to a 3rd party specialist. If the IT failure occurs, the impact on the organisation will still be very serious, regardless of who was managing the risk.

4. **ROLES AND RESPONSIBILITIES**

The roles and responsibilities of key personnel in the risk management are outlined below. Good risk management depends, to a large extent, on good communication and individuals should ensure that all relevant information made available to other key individuals in the process.

(1) **All Staff**

All staff have a responsibility to identify risks and report on them to their line manager.

(2) **Corporate Risk Manager**

The Corporate Risk Manager is responsible for the maintenance of the Corporate Risk Register under the direction of CCF. Other responsibilities include:

- (a) Regularly review and quality assure District Command Unit and Departmental Risk Registers;
- (b) Report to Regional ACCs on risk management within District Command Units;
- (c) Report to DCC on risk management within departments;
- (d) Collating and reporting on Stewardship Statements;
- (e) Analyse risk registers to identify common themes/frequently occurring risks;
- (f) Provide advice, guidance and assistance on risk management to the organisation;

- (g) Promote and support the integration of risk management into the planning process;
- (h) Disseminate good practice;
- (i) Liaise with ICS regarding access to Topcase software;
- (j) Liaise with Internal Audit regarding Risk Management;
- (k) Report to Audit and Risk Committee on Risk Management in PSNI;
- (l) Maintain contact/liaison with UK Police risk managers.

(3) **Risk Owner**

The risk owner has overall responsibility for managing an individual risk. Typically, the risk owner will be a chief officer, branch or department head or DCU commander. The risk owner will have been involved in the identification/evaluation of the risk and the formulation of control measures to mitigate against the risk. The risk owner will also be responsible for deciding if a risk is sufficiently serious to be **escalated** to the next level of the organisation. Risk owners have responsibility for ensuring that additional actions to treat or control the risk are carried out and for informing the Risk Manager of any consequent updates to the risk register. Close liaison and co-operation with the Risk Manager is essential to the effective management of risk. Risk management is an active process. The causes of a risk may recede or become irrelevant and risk actions will be completed, further mitigating against the risk. The Risk Owner will therefore constantly review the Risk Rating and the necessity to keep the risk on the register. Risk Owners should make maximum use of the Monthly NIM structured meetings to manage risk actions and seek assurance that risk is being managed effectively. There should always be one named risk owner for each identified risk.

(4) **Risk Manager**

Risk managers have been appointed for each District Command Unit and for all HQ departments. The risk manager has responsibility for maintaining the risk register, under the direction of risk owners, and updating or amending the register as necessary. The role is primarily administrative and risk managers are **not** responsible for identifying risks or controls. Risk managers should ensure that they regularly review the content of risk registers with a view to ensuring that risk actions are being completed and that all details on the register are correct. This entails close liaison with Risk Owners and the ability to challenge discrepancies in the risk register.

(5) **Risk Action Owner**

Risk Action Owners are assigned by the Risk Owner to carry out the actions identified to treat or control the risk. For many risks, the Risk Owner and Risk Action Owner may be one and the same, however it may be appropriate to delegate particular actions to other named individuals. The Risk Owner remains responsible for the overall management of the risk and can monitor progress against actions via the risk register.

(6) **District Commanders and Heads of Departments**

DCU commanders and Heads of Business Units will be responsible for ensuring that risk management processes become embedded and are fully operational within their areas of responsibility. This will involve:

- (a) implementing CCF policies and procedures on internal control at an operational level;
- (b) encouraging staff to actively consider and manage risk;
- (c) undertaking risk reviews for their units and carrying out necessary risk management actions;
- (d) communicating significant risks and control weakness for their area of responsibility to the Corporate Risk Manager;

- (e) notifying the Corporate Risk Manager of any potentially significant risks and control weaknesses that could materially affect the organisation's operations in the future. Depending on the severity and time sensitivity of the actions required consideration should be given to escalating these risks to the appropriate management level;
- (f) ensuring that a risk register is maintained and providing up to date risk information to the Corporate Risk Manager within the predefined timescales; and
- (g) ensuring that a suitable system of internal control operates in their area of responsibility.

(7) Internal Audit

- (a) Although risk management and internal control are clearly management's responsibility, Internal Audit also has an interest in effective internal control. Internal Audit's primary objective in relation to risk management is to provide independent assurance on the effectiveness of the risk management internal control framework (and therefore risk management) to the Audit and Risk Committee. It does this by carrying out audits and reviews within the PSNI focused on the key risks in the business, using the output from the risk management process to direct efforts.
- (b) Internal Audit also has a role to play in strengthening the overall process by:
 - (i) acting as an independent adviser by providing advice on the management of risk, especially those issues surrounding the design, implementation and operation of systems of internal control;
 - (ii) monitoring, reporting and providing assurance on the effectiveness of the risk and control mechanisms in operation; and
 - (iii) promoting risks and controls concepts across the department.
- (c) However, it should be noted that Internal Audit is only one of a number of assurance mechanisms that will be used by the Chief Constable to meet the sign off requirements.

(8) External Audit

- (a) The role of External Audit is to provide an independent opinion on whether the financial statements give a true and fair view of the state of affairs of the PSNI and whether in all material respects the expenditure and income have been applied to the purposes intended and financial transactions conform to the authorities which govern them.
- (b) As the Accounting Officer is required to sign off on a Statement of Internal Control as part of the annual accounts, the external auditors will need to satisfy themselves that the assertions made as part of this report are in line with their understanding of the PSNI's actions in relation to the risk management processes.

(9) Audit and Risk Committee

- (a) The function of the Audit and Risk Committee is to support the Chief Constable (Accounting Officer) by monitoring and reviewing the risk, control and governance processes, which have been established within PSNI and the associated assurance processes. In addition, they will monitor the management and control of significant risks to reduce the likelihood of unforeseen occurrence.
- (b) The Committee will advise the Accounting Officer on:
 - (i) the strategic processes for risk, control and governance and the Statement of Internal Control;
 - (ii) the accounting policies and the Annual Financial Statements including the process for review of the accounts prior to submission for audit, levels of error identified, and management's letter of representation to External Audit;
 - (iii) the planned activity and results of both Internal and External Audit;

- (iv) adequacy of management's response to issues identified by audit activity, including External Audit's management letter; and
- (v) assurances relating to corporate governance requirements.

In order to facilitate the above the Audit and Risk Committee will be provided with update reports on the PSNI's Risk Management process on a periodic basis.

STEWARDSHIP STATEMENT

Letter of Representation to Chief Constable on the Risk Management Process.

1. As Head of _____ Department, I am responsible for co-ordinating risk management activities within this Department. This includes ensuring that the Risk Manager is regularly updated on progress, chairing discussions of risk at Departmental Management Meetings and developing communication to departmental staff.

2. I am satisfied that, within _____ Department, the following areas are on course for the achievement of objectives and that there are no areas of concern, other than those specified, in my areas of responsibility.
 - (1) There is an ongoing process for identifying, evaluating and managing the department's significant risks;
 - (2) A Risk Register has been developed for the department and describes the significant risks and how they are managed. They are also used as a basis for regular reviews of the risk profile and reporting to the Risk Manager;
 - (3) The status of risk is discussed at management meetings including the review of risk information and risk indicators, any early warning signs of risk materialising and/or escalating, and any significant control failings or weaknesses;
 - (4) The risk management process has been in place during the period since _____

3. Following my assessment of the risk management process and internal control framework within my area of responsibility, I am satisfied that there are no significant weaknesses in internal controls other than disclosed below:

I certify that the information recorded on this return is complete and accurate.

Signed:

Name:

Title:

Date:

STEWARDSHIP STATEMENT

Letter of Representation to Chief Constable on the Risk Management Process.

1. As Commander _____ District, I am responsible for co-ordinating risk management activities within this District. This includes ensuring that the Risk Manager is regularly updated on progress, chairing discussions of risk at District Management Meetings and developing communication to departmental staff.

2. I am satisfied that, within _____ District, the following areas are on course for the achievement of objectives and that there are no areas of concern, other than those specified, in my areas of responsibility.
 - (1) There is an ongoing process for identifying, evaluating and managing the department's significant risks;
 - (2) A Risk Register has been developed for the department and describes the significant risks and how they are managed. They are also used as a basis for regular reviews of the risk profile and reporting to the Risk Manager;
 - (3) The status of risk is discussed at management meetings including the review of risk information and risk indicators, any early warning signs of risk materialising and/or escalating, and any significant control failings or weaknesses;
 - (4) The risk management process has been in place during the period since _____

3. Following my assessment of the risk management process and internal control framework within my area of responsibility, I am satisfied that there are no significant weaknesses in internal controls other than disclosed below:

I certify that the information recorded on this return is complete and accurate.

Signed:

Name:

Title:

Date: