Keeping People Safe

Service Procedure

RISK MANAGEMENT

SP Identification Number	1/11
Protective Marking	Not Protectively Marked
Policy Ownership:	
Department	Deputy Chief Constable's Office
Branch	Executive Business Support
Author	Corporate Risk Manager (C110458)
Procedure Approved By:	
Service Executive	Deputy Chief Constable
Department or Branch Head	Head of Corporate Governance (C142792)
Date Of Approval	8 July 2015
Date First Issued:	14 February 2011
Version Number	4
This Version Issued:	30 July 2015
Review Date:	1 April 2017
Governing Policy Directive:	Corporate Governance

Abstract:

The aim of the Service Procedure is to provide the policy and procedure in relation to risk management processes within the PSNI. This Service Procedure is for use by all Risk Managers; in particular those at Area and Department levels and for all other persons involved in the Risk Management Process.

INDEX

2. INTRODUCTION

(1) "Risk management is a highly topical issue for all government departments and their sponsored bodies and has a vital role to play in promoting and securing value for money in the use of public funds." (Northern Ireland Audit Office Good Practice in Risk Management June 2011). As Accounting Officer for the Police Service of Northern Ireland (PSNI), the Chief Constable has a responsibility for maintaining a sound system of internal control that supports the achievement of the aims and objectives, in the context of the PSNI strategic principals, in particular the overall aim of keeping people safe, while achieving the prudent use of public resources.

(2) 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. Risk management is not an end in itself but a process which complements business, operational and organisational planning.

(3) The delivery of policing services inevitably gives rise to risks and the PSNI recognises the importance of managing risk in the achievement of its policing and business objectives.

(4) Risk management is designed to manage rather than eliminate the risk of failure to policing and business objectives. The approach to risk is therefore focused on effectively managing risk to an acceptable level. It therefore provides reasonable and not absolute assurance of effectiveness.

(5) The PSNI recognises the importance of making prudent assessment and disclosure to the Parent Department, the Service Executive Board and the Audit and Risk Assurance Committee of the financial and non-financial implications of risks. The Service adopts an open and receptive approach to discussing and addressing risks at all levels within organisation.

(6) This Service Procedure explains the PSNI's approach to risk management, documents roles and responsibilities and provides detailed guidance on how risk is to be managed by all members of the organisation.

3. IMPLICATION OF SERVICE PROCEDURE

(1) **Financial Implications/Best Value/Continuous Improvement/Efficiency**

Implementation of effective Risk Management will bring significant organisational benefits. It assists in identifying operational and business risks that may hinder the PSNI from delivering against its core objectives and targets. Identification, evaluation and control of risk at all levels serves to enhance efficiency, encourages effective management of resources and assists the organisation in achieving core objectives.

(2) **Human Resources/Training**

This Service Procedure provides sufficient guidelines on the Risk Management process that should be followed. However workshops will be provided to Area and Departmental Risk Managers by Executive Business Support (EBS) staff at no additional cost to the organisation. Training in use of the PRiDE Risk Management software will also be provided by staff from EBS.

(3) **Risks**

The overall success of the Risk Management process is dependent upon how well risk is embedded into the organisation. To that end risk management should be used as a management tool to drive the business forward and achieve organisational aims and objectives, in the context of the PSNI strategic principals.

(4) **Bureaucracy**

Some minor administration by those involved in the process will be required. No additional bureaucracy will be placed on front line policing.

(5) **Contribution**

The adoption of this Risk Management procedure will provide assurance that a sound system of internal control is in place and operating effectively.

(6) **Application**

This Service Procedure is for use by all Area Coordinators/Heads of Department, Risk Managers and for all others persons involved in the Risk Management Process.

4. LEGAL BASIS

Although there is no legislative requirement to conduct Risk Management, the UK Corporate Governance Code highlights this important function as a key element of internal control within organisations. The Chief Constable, as Accounting Officer, is required to sign an annual Governance Statement and include it with the Annual Report and accounts, and a six monthly Stewardship Statement for the Parent Department to demonstrate the management, accountability and ownership of Risk within the Service. [(11) (c) on page 13 refers].

5. POLICY LINKS

This Service Procedure should be read in conjunction with the following:

Policy Directive 02/12 – Corporate Governance.

6. CONSULTATION

The following have been consulted in relation to this Service Procedure:

(1) Chief Officers;

(2) Audit and Risk Assurance Committee (ARAC).

7. HUMAN RIGHTS/UNITED NATIONS CONVENTION ON THE RIGHTS OF THE CHILD (UNCRC)/EQUALITY/CODE OF ETHICS/FREEDOM OF INFORMATION

(1) This Service Procedure does not engage any Human Rights issues. (Managing risk in a policing context often involves Human Rights issues although no specific Human Rights issues are engaged by this Service Procedure.)

(2) This Service Procedure does not adversely affect any section of the community.

(3) This Service Procedure meets the organisations integrity standards.

(4) This Service Procedure is suitable for public disclosure in accordance with the Freedom of Information Act 2000.

8. FURTHER INFORMATION

The following publications contain further information on the Management of Risk:

(1) Management of Risk (The Orange Book) – HM Treasury;

(2) Good Practice in Risk Management – NI Audit Office;

(3) Managing risks with Delivery Partners – HM Treasury/OGC.

9. MONITORING AND REVIEW

(1) The Corporate Risk Manager is responsible for reviewing the contents of this Service Procedure.

(2) Feedback relating to this Service Procedure should be made to the Corporate Risk Manager, EBS.

10. POLICE SERVICE OF NORTHERN IRELAND'S APPROACH

The PSNI's underlying approach to risk management is as follows:

(1) The Chief Constable is Accounting Officer but delegates on a day to day basis the responsibility for organisational governance, including the management of risk, to the Deputy Chief Constable (DCC);

(2) The Service Executive Board (SEB) owns, supports, promotes and accepts leadership responsibility for the adoption of risk management procedures and practice throughout the organisation;

(3) The Corporate Risk Register (CRR) sets out the key strategic risks facing the organisation and how they are managed. The CRR is driven by risks directly affecting performance against policing objectives and risks arising from business, resourcing, finance or reputational risks.

(4) The CRR is reviewed at the ServiceFirst Board (SFB) on a monthly basis. Decisions regarding the removal, addition or significant change to Corporate Risks will be ratified at SEB and also reported to the Audit and Risk Assurance Committee (ARAC) for information.

(5) Risk management processes, the review of risks and inspection of same will be undertaken by the Corporate Risk Manager and monitored through the Corporate Governance Committee Structure.

(6) On a semi-annual basis the Corporate Risk Manager will advise SFB and ARAC on the effectiveness and robustness of the risk management processes throughout the organisation.

(7) The day-to-day management of risk will be undertaken by line management. (It is strongly suggested that at Area, Branch and Departmental levels risk is a standing agenda item at monthly Management Meetings);

(8) Departmental and Area registers will be maintained, reviewed and updated as necessary on a monthly basis.

(9) Branches and other operational areas will maintain risk registers if deemed appropriate or on the direction of the relevant Head of Department or Area Coordinator.

(10) Consideration should be given to a Partnership Risk register if the PSNI is the principal organisation in the partnership. (Page 12 refers).

(11) All risk registers will be managed electronically on PRiDE, the corporate risk management system.

11. GUIDANCE

(1) **What is risk?**

(a) A ‘risk’ is defined as ‘an uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives’.

(b) A risk can be either a ‘threat’ or an ‘opportunity’. A ‘threat’ is used to describe an uncertain event that could have a negative impact on the achievement of objectives; an ‘opportunity’ is used to describe an uncertain event that could have a favourable impact on achievement of objectives.

(c) A risk consists of a combination of the likelihood of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.

(2) **What is Risk Management?**

(a) Following several high profile failures in the public and private sectors, 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.

(b) Every organisation manages its risk, but not always in a way that is visible, repeatable or consistent, to support effective decision-making. The task of risk management is to ensure that an organisation makes cost-effective use of a risk management process that includes a series of well-defined steps.

(c) The aim is to support better decision-making through a good understanding of risks and their likely impact. This provides a disciplined environment of proactive decision-making. It complements the planning process and provides another layer of control to managing performance.

(d) 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.

(3) 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.

(4) **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:**

The Chief Constable is responsible for the management of risk and for providing assurance that sound systems of internal control are in place and are effective.

(b) **Risk Director:**

The Deputy Chief Constable (DCC) is responsible for the management and co-ordination of the organisation's risk policies and activities.

(c) **Risk Owners:**

Chief Officers, Department Heads and Area Coordinators (and Branch Heads if deemed appropriate) are 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.

(d) **Risk Action Owners:**

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

(e) **Corporate Risk Manager:**

The Corporate Risk Manager on behalf of the DCC has responsibility for co-ordinating and overseeing the risk management processes and systems at all levels within the organisation.

(f) **Risk Managers:**

Area Coordinators/Head of Department appoint Risk Managers to maintain risk registers on their behalf and provide administrative support to the risk management process within their area of business.

(g) **Internal Audit**

Internal Audit provide independent assurance on the effectiveness of the risk management internal control framework (and therefore risk management) to the ARAC.

(h) **Audit and Risk Assurance Committee**

A key responsibility of the ARAC is to advise the Chief Constable on the strategic processes for risk, control and governance.

(Appendix 'A' outlines full details of roles and responsibilities).

(5) **What is a Risk Register?**

(a) Risk Registers document the nature and extent of risks and record the actions taken to control the risk and mitigate their effects.

(b) A Risk Register will typically contain between 6 and 12 risks.

(c) The Risk Register is a 'living' document that must be updated regularly and whose content will change frequently as risks are mitigated and new risks emerge.

(d) All Risk Registers are held electronically on the PRiDE risk management system which is accessible through the PRiDE icon on Common Terminal Desktop.

(6) **Completing the Risk Register**

The following defines each step of the process, maps it on to the risk template, and provides advice on how to complete each section. When completing the Risk Register ensure that language is clear and unambiguous. Abbreviated words or acronyms should be explained in full at first use.

(a) **Identify and Describe**

Identify the risks to the achievement of your policing objectives. This can be achieved by taking each objective in turn and considering what events could threaten the achievement of it. Consider all risks, however insignificant or serious they appear to be at this stage.

Describe

Begin the risk description with the words "***There is a risk that***…."
Descriptions of risk should always combine the Cause, the Event and the Effect eg "**There is a risk** that due to a reduction in resources **(cause)** we may fail to appoint suitably trained investigators **(event)** which will result in reduced detections and clearances **(effect)**. The description should be short and succinct.

(b) **Assess and Analyse**

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

(ii) Consider any events which may provide **early warning** that the risk is occurring and will have an effect on the business objective. Also consider the **reasons** why this risk has occurred and the **general impact** it will have on the achievement of your Policing objectives should it not be addressed. This can assist in deciding what **Controls** are required.

(c) **Controls**

There are two types of controls – **Existing Mitigation** and **Risk Actions**. Both should be considered in turn and listed.

(i) **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 risk rating and should be listed in priority order in terms of their significance in mitigating the impact or likelihood of the risk.

Existing mitigations should be reviewed, and if necessary updated, on a monthly basis at Management Meetings and assurance provided that they are working effectively.

(ii) **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 SMART (Specific, Measurable, Achievable, Realistic and Timely) and 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 risk rating should be re-assessed in light of a reduction in the impact/likelihood of the risk occurring.

(d) **Evaluate**

(i) The evaluation (Risk Rating) should be based on the importance of the risk when mitigation is in place and before actions have been completed.

(ii) Most risks will be deemed acceptable or insignificant. It is therefore important to prioritise risks in order to concentrate responses to the most serious risks. This is best achieved using the Risk Assessment Matrix and scoring Guide. **(See Appendix B for guidance and examples)**. 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.

(7) **Monitoring and Managing the Risk Register**

(a) The Risk Owner and the Management Team are responsible for ensuring that risk is managed appropriately and effectively within their area of responsibility.

(b) The Risk Register will be formally reviewed and, if necessary, updated on a monthly basis at an appropriate Management Team meeting which will be attended by the Risk Manager.

(c) Each risk will be considered in turn with a view to establishing:

(i) The effectiveness of risk actions;

(ii) The achievement of risk actions;

(iii) The current status of the risk (Risk Rating);

(iv) The requirement for the risk to remain on the register;

(v) The identification of additional mitigating controls for managing the risk;

(vi) How assurance can be provided that each of the mitigating controls are operating effectively;

(vii) The emergence of new risks for addition to the register should also be considered.

(d) The Risk Manager will update the register with any changes, including; completed actions, new actions, personnel changes and realignment of target dates.

(e) As actions are completed the Risk Rating may be revised and reduced to the extent that the risk is no longer significant and may be removed from the Risk Register.

(f) Consideration should also be given as to whether any risk is sufficiently serious to warrant escalation to the next level of management e.g. Departmental Risk Register or Corporate Risk Register.

(g) A more structured formal review should take place at six monthly intervals in March and September. (The March review should consider risks to the annual policing plan objectives).

(h) A Formal Review should consider the following questions:

(i) Are the identified risks still the most significant?

(ii) Are target dates for actions being met?

(iii) Have any new risks been identified?

(iv) Are control measures effective?

(v) How can we be assured that the control measures for mitigating the risk are operating effectively?

(vi) Overall, is there an effective risk management process in place?

(i) The Risk Register is managed and maintained by the Risk Manager, on behalf of the Risk Owner, using PRiDE. A sample of the risk report generated by this system is reproduced below with descriptions of the content of each section. On the following page, a completed Risk Report is reproduced by way of example.

<table>
<tr><th colspan="3">Risk</th><th colspan="3">Risk Rating</th></tr>
<tr><td colspan="3">Label and Number and Title
Cause
Event
Effect</td><td colspan="3">Impact:
Likelihood:
Rating (using risk matrix) following the consideration of mitigation controls in place – prior to the completion of control actions</td></tr>
<tr><th colspan="3">Risk Owner</th><th colspan="3">Policing Plan Performance Indicator</th></tr>
<tr><td colspan="3">Senior officer who is responsible for the control of the risk</td><td colspan="3">Link to the relevant Policing Plan Performance Indicators</td></tr>
<tr><th colspan="3">Early Warning Indicators</th><th colspan="3">General Impact</th></tr>
<tr><td colspan="3">What has brought this to our attention?
(Bullet points – short and succinct)</td><td colspan="3">What impact will this have on business if it is not addressed? (Bullet points – short and succinct)</td></tr>
<tr><th colspan="3">Reason</th><th colspan="3">Existing Mitigation</th></tr>
<tr><td colspan="3">Why has this happened?
(Bullet points – short and succinct)</td><td colspan="3">What control measures are currently in place to manage this risk?

(Include key controls listed in priority order)</td></tr>
<tr><th>Additional Action to fully manage the Risk</th><th>Responsible Officer</th><th>Planned Start</th><th>Actual Start</th><th>Planned Finish</th><th>Forecast Finish</th></tr>
<tr><td>List of other treatments and control measures which can be put in place to mitigate against the risk. (All actions should be SMART)</td><td>The individual assigned with the responsibility of carrying out each risk action.</td><td></td><td></td><td></td><td></td></tr>
</table>

Risk	Risk Rating
SE 03 BUDGET – There is a risk that we will not have sufficient budget to meet operational pressures resulting in significant overspend which will negatively impact on service delivery and reputation.	**Impact:** Serious (3) **Likelihood:** Almost Certain (4)
Risk Owner	**Policing Plan Performance Indicator**
C/Superintendent xxxx	Link to the relevant Policing Plan Performance Indicators
Early Warning Indicators	**General Impact**
• Difficulty in producing a balanced budget for 2015/16. • Small Full Year Projected pressure after period 1. • Limited additional funds expected from Monitoring Rounds.	• Failure to optimise impact of funding. • Inability to meet operational demands. • Loss of credibility and confidence with key stakeholders. • Reputational damage e.g. Northern Ireland Policing Board/Dept. of Justice/NI Audit Office.
Reason	**Existing Mitigation**
• Potential for imposition of further in-year cuts and continued uncertainty over available resources. • Fluctuating or unanticipated demand. • Poor financial management.	Key Controls: 1. Monthly financial reporting to key internal and external stakeholders. 2. Focus on Full Year Projections. 3. Contingency / Scenario Planning. 4. Scrutiny of risk areas. 5. Completion of Monitoring Rounds. 6. Oversight by Performance and Assurance SET (PASET). 7. Scrutiny by ServiceFirst Board and SEB 8. Oversight by NIPB and DoJ

Additional Action to fully manage the Risk	Responsible Officer	Planned Start	Actual Start	Planned Finish	Forecast Finish
1. Develop and implement a new Head of Business Services Resource Budgetary Management (RMB) reporting mechanism.	AN Other	01/04/15	01/04/15	01/06/15	

(8) **Escalation/Cross-Departmental Risk**

(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 areas of business. 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 within the area where it was initially identified. The risk may 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 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.

(9) **Programme and Project Risk Management**

(a) Managing Successful Programmes (MSP) defines a Programme as 'being created *…to coordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to the organisations strategic objectives…'*

(b) Programmes are responsible for risks that can affect the successful delivery of their annual business plan. Programmes should consider the impact of risk on the delivery of their business plan and ensure risks are appropriately captured in the organisational risk management process.

(c) All risks relating to the work of PSNI change programmes should be managed and monitored through the PRiDE system by the Programme Manager.

(10) **Partnership Risk Management**

(a) The Audit Commission defines a partnership as '*An agreement between two or more independent bodies to work collectively to achieve an objective'.*

(b) In relation to risk management the PSNI must meet two key responsibilities for each partnership they have. They must:

(i) provide assurance that the risks to the PSNI associated with working in partnership with another organisation have been identified and prioritised and are being appropriately managed;

(ii) ensure that the partnership has effective risk management procedures in place.

(c) If the PSNI is the principle organisation in the Partnership consideration should be given to initiating a joint risk register, with those risks relating to the PSNI managed and monitored by the appropriate PSNI lead officer through the PRiDE system.

(11) **Internal Control**

(a) Management, accountability and ownership of Risk is one of the key elements of Internal Control highlighted in the six monthly Stewardship Statement, which is a requirement of the Department of Justice, and the annual Governance Statement, which is a requirement of the Northern Ireland Audit Office. Both statements are signed by the Chief Constable as Accounting Officer of the PSNI.

(b) Area Coordinators and Departmental Heads are also required to assist in this process by signing a Statement of Risk Management Assurance on a half-yearly basis. Assurance is required to show that risk is being actively managed and reflected accurately in the Risk Registers.

(c) Statements of Risk Management Assurance will be requested and collated by the Corporate Risk Manager in March and September. Heads of Department and Area Coordinators may require others, such as Branch Heads and District Commanders to also complete a Statement of Risk Management Assurance to provide assurance of internal control at those levels of the organisation.

APPENDIX 'A'

ROLES AND RESPONSIBILITIES

The roles and responsibilities of key personnel in the management of risk 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

(1) The Corporate Risk Manager is responsible for the maintenance of the Corporate Risk Register under the direction of the Chief Constable.

(2) Other responsibilities include:

(a) Regularly review Area and Departmental Risk registers and, where necessary, challenge the content on behalf of the Deputy Chief Constable (DCC);

(b) Report to the DCC on risk management within Departments and Areas;

(c) Collate and report on the Statements of Risk Management Assurance;

(d) Analyse risk registers to identify common themes/frequently occurring risks;

(e) Provide advice, guidance and assistance on risk management to the organisation;

(f) Promote and support the integration and synchronisation of risk management into the planning processes;

(g) Disseminate good practice;

(h) Liaise with Information & Communications Services Branch (ICS) regarding access to the Risk Management software;

(i) Liaise with Internal Audit regarding Risk Management;

(j) Report to the ServiceFirst Board (SFB) on the risk management process in the PSNI;

(k) Report to Audit and Risk Assurance Committee (ARAC) on Risk Management in the PSNI;

(l) Maintain contact/liaison with United Kingdom 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, Department Head or Area Coordinator. 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 National Intelligence Model (NIM) structured TCG 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 Area and for all HQ Departments and should attend the relevant monthly management meeting. 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, it is appropriate to delegate particular actions to 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. Senior Managers

Senior Managers will be responsible for ensuring that risk management processes become embedded and are fully operational within their areas of responsibility. This will involve:

(1) Implementing policies and procedures on internal control at an operational level;

(2) Encouraging staff to actively consider and manage risk;

(3) Undertaking risk reviews for their area of responsibility and carrying out necessary risk management actions;

(4) Communicating significant risks and control weakness for their area of responsibility to the Corporate Risk Manager;

(5) Notifying the Corporate Risk Manager of any potentially significant risks and control weaknesses that could materially affect the organisation's operations in the future;

(6) Ensuring that a risk register is maintained and providing up to date risk information to the Risk Manager within the predefined timescales; and

(7) Ensuring that a suitable system of internal control operates in their area of responsibility.

7. Internal Audit

(1) 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 ARAC. 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.

(2) Internal Audit also has a role to play in strengthening the overall process by:

(a) 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;

(b) Monitoring, reporting and providing assurance on the effectiveness of the risk and control mechanisms in operation; and

(c) Promoting risks and controls concepts across the department.

8. Audit and Risk Assurance Committee

(1) One of the key responsibilities of the ARAC is to advise the Chief Constable on the strategic processes for risk, control and governance and the Statement on Internal Control (SIC).

(2) The responsibilities of the ARAC in relation to risk management include the following:

(a) To oversee the risk management process and provide assurance to the Chief Constable that the risk management process is operating effectively;

(b) To receive and consider six monthly reports on risk management including significant changes to the Corporate Risk Register at each meeting;

(c) To review Area and Departmental Risk Registers as part of their annual programme of work;

(d) To consider Internal Audit reports on risk management.

APPENDIX 'B'

RISK ASSESSMENT MATRIX AND SCORING GUIDE

(1) 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:

(a) If this were to happen, how serious would it be, considering the existing mitigation in place?

(b) How likely is it to happen?

(2) The answers are plotted on the matrix, giving a score of between 1 and 25. This score is the **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.

(3) 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.

(4) The matrix may also be used to assign a revised Risk Rating, however this is often achieved by simple judgement of the effect of treatments and controls.

(5) A reproduction of the Risk Assessment Matrix and a guide on scoring impact and likelihood can be found below.

RISK MATRIX

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				

QUALITATIVE MEASURES OF RISK IMPACT

Impact	Score	Financial	Service Delivery	Litigation	Reputation	Injury
Minor	**1**	Potential or actual loss up to £50k	Little impact on Service Delivery or achievement of Departmental /District Plans.	One-off settlement – no implications beyond the instant case.	Complaints from individuals. Minor impact on our ability to engage with local communities.	Minor or Slight Injury to individual.
Significant	**2**	Potential or actual loss £51k - £249k	Significant reduction in Service Delivery or Non-achievement of 1-2 targets on Departmental/ District Plans.	Moderate financial impact on limited range of cases.	Adverse local publicity. Significant impact on our ability to engage with local communities.	Major/Significant Injury to an individual or several people.
Serious	**3**	Potential or actual loss £250k - £499k	Serious reduction in Service Delivery or Non-achievement of a number of targets in Departmental/ District Plans.	Serious financial impact on larger range of cases. Prosecution for minor criminal charges.	Adverse local publicity of a persistent nature. Serious impact on our ability to engage with local communities.	Single Fatality or Severe Injury to several people.
Major	**4**	Potential or actual loss £500k or more	Major failure in Service Delivery or Non achievement of the majority of Departmental /District Plans.	Serious and long term effects on organisation. Loss of credibility and public confidence. Officers facing prosecution for serious criminal offences.	Regional/National adverse media coverage. Major reputational damage resulting in major inability to engage with local communities.	Multiple Fatalities or Multiple Permanent Injuries.

QUALITATIVE MEASURES OF LIKELIHOOD

Score	Descriptor	Description	Value
1	Unlikely	The event may occur only in exceptional circumstances	>25%
2	Possible	The event might occur at some time	26-49%
3	Very likely	The event will probably occur at some time	50-74%
4	Almost certain	The event is expected to occur in most circumstances	76-100%

RISK QUANTIFICATION MATRIX

High	**9 - 16**
Medium	**6 - 8**
Low	**1 - 5**