Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI1216
Policy Ownership	Corporate Support
Issue Date	22/12/16
Review Date	5 years from issue date
Governing Service Policy	Risk Management and Governance
Cancellation of	SP01/2011 Risk Management
Classification	**OFFICIAL [PUBLIC]**

SI1216

Risk Management

The Police Service of Northern Ireland is focused on good governance. The effective management of risk is a key element of good governance. This instruction outlines how we will address risk internally and with partners.

Keeping People Safe

Table of Contents

Table of Appendices

1. Introduction

The Police Service of Northern Ireland (PSNI) is committed to identifying and managing risk to provide effective, efficient and cost effective results. Risk Management forms an essential part of our governance and assurance approach.

The Service Instruction is for use by all Risk Managers; in particular those at Department and Area / Branch levels and for all other persons involved in the Risk Management Process.

The delivery of policing services inevitably gives rise to risks and we recognise the importance of managing risk in order to achieve policing and other organisational objectives.

2. Risk Management

The underlying approach to risk management is as follows:

- 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);
- The Service Executive Board (SEB) owns, supports, promotes and accepts leadership responsibility for the adoption of risk management procedures and practice throughout the organisation;
- 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 outcomes and risks arising from business, resourcing, finance or public confidence;
- 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;
- 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;
- On a bi-annual basis the Corporate Risk Manager will advise SFB and ARAC on the effectiveness and robustness of the

risk management processes throughout the organisation;

- The day-to-day management of risk will be undertaken by line management with risk featuring as a standing agenda item at monthly management meetings at Area, Branch and Departmental level;
- Risk Registers will be maintained, reviewed and updated as necessary on a monthly basis;
- Areas, Branches, Districts and other operational areas will maintain risk registers if deemed appropriate or on the direction of the relevant Head of Department;
- Consideration should be given to a Partnership Risk Register if the PSNI is the principal organisation in the partnership;
- All risk registers will be managed electronically on PRiDE, the corporate risk management system. The PRiDE risk management system is accessible through the PRiDE icon on the Common Terminal desktop.

3. 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.

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. Refer to Section 5 to see the process to follow when identifying and managing risks.

4. Roles and Responsibilities

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.

Appendix A outlines full details of Roles and Responsibilities – Page 12 refers

Roles and Responsibilities	
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.
Risk Director	The Deputy Chief Constable (DCC) is responsible for the management and coordination of the organisation's risk policies and activities.
Risk Register Owner	Chief Officers, Department Heads and Area Coordinators and Branch Heads if deemed appropriate have overall responsibility for all risks on the risk register within their area of responsibility. They are also responsible collectively for the management of risks which have strategic or cross-departmental implications for the organisation.
Risk Owners	These are senior managers who are allocated responsibility for specific risks by the Risk Register Owner. They are responsible for the evaluation and control of those risks on behalf of the Risk Register Owner.
Risk Action Owners (Responsible Officers)	These are managers with responsibility for implementing risk control measures and reporting progress to Risk Owners.
Corporate Risk Manager	The Corporate Risk Manager on behalf of the DCC has responsibility for coordinating and overseeing the risk management process and systems at all levels within the organisation.
Risk Managers	Branch Heads/Area Coordinators/Heads of Departments appoint Risk Managers at a suitable level to maintain risk registers on their behalf and provide support to the risk management process within their area of business.
Internal Audit	Internal Audit provides independent assurance on the effectiveness of the risk management internal control framework (and therefore risk management) to the ARAC.

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. The ARAC also advises the Chief Constable on the "adequacy and operation" of the risk management processes.

5. Completing the Risk register – Identifying and Managing Risk

The following defines each step of the process to identify and manage the risks we face 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.

STEP 1 Identify and Describe Risks

Identify the risks to the achievement of your policing/other outcomes. This is best done in groups and by the individuals responsible for delivering the outcomes / objectives.

Describe the risk by considering the Cause (the situation that gives rise to the risk)**, the Event** (the consequence if the risk occurs) **and the Effect** (the impact that the risk would have should it materialise)**.**

E.g. There is a risk that the level of sickness absence within the organisation (cause) will have detrimental impact on service delivery (event), potentially impacting delivery of policing services in the future (effect).

The description should be short and succinct and summarise the risk in a sentence.

Guidance to describe a risk

Risk Element	Linking words	Example
Cause	There is a risk that	the level of sickness absence within the organisation
Event	will have	detrimental impact on service delivery
Effect	potentially impacting	delivery of policing services in the future

(Appendix 'B' outlines the PSNI's Risk Template).

STEP 2 Assess and Treat Risks

Assess the risk by considering indicators / performance data which can be reviewed and updated on a regular basis to provide **early warning** of worsening trends, i.e. absenteeism. Also consider the **general impact** it will have on the achievement of your outcomes / objectives should it not be addressed. This can assist in deciding what **controls** are required.

Treat
List any **key controls** which are already in place to manage/mitigate the risk. *(Key controls should be listed in priority order in terms of their impact in mitigating the risk).* Also list the **key assurance** relating to each key control, i.e. how the Risk Owner will know that the key control is working effectively.
Additional Actions - List other **actions, treatments and controls** which are being put in place to mitigate the risk. These additional actions may become key controls or they may be one off actions to assist in managing the risk.

Actions should be SMART.

STEP 3 Evaluate Risks

Evaluate the risk rating by considering the following**:**

Inherent Risk Rating (untreated risk) **-** the impact of the risk occurring before any action is taken to manage it.
Residual Risk Rating (treated risk) - the impact and likelihood of the risk occurring when you consider key controls and other actions which are already in place to manage it.
Target Risk Rating – the impact and likelihood you want to get to (as defined by your Risk Appetite).
Impact x Likelihood = Risk Score/Risk Rating
(See Appendix 'C' for detailed Scoring Matrix)

Recommended Responses for Residual Risk Rating
16 - 25 HIGH (Red)
Take immediate action to reduce the impact/likelihood. Review each month at management meeting. Consider forwarding to ServiceFirst Board (Corporate Risk Manager) for consideration for the Corporate Risk Register.
8 – 15 SIGNIFICANT (Orange)
Take immediate action to reduce the impact/likelihood. Review each month at management meeting. Consider escalating to higher risk register if risk rating increases.
3 – 6 MEDIUM (Yellow)
Take practical measures to reduce risk. Manage at local level and review every 3 months. Highlight at management meeting if risk rating increases.
1 – 2 LOW (Green)
Monitor and review control measures over a period of 6 months. Is this business as usual? Does it need to be on the Risk Register?

STEP 4 Monitor and Review Risks

The Risk Register should be formally **reviewed** and, if necessary, updated on a monthly basis at an appropriate management meeting for risks which are rated at High or Significant risk. Medium or Low risks should be reviewed every 3 & 6 months. The following should be considered when reviewing the risks on the register:

1. Will the planned risk actions reduce the risk to an acceptable level?
2. Are target dates being met?
3. What is the current status of early warning indicators?
4. Are key controls still effective?
5. What is the current status of the risk rating? (As actions are completed the risk rating may be reduced).
6. Does the risk need to remain on the risk register?
7. Is the risk sufficiently serious to warrant escalation to the next level? E.g. Department or Corporate register.
8. Are there any emerging risks for inclusion on the register?

In addition to the above a more **structured review should take place annually.** (see section 6 'The Formal Review').

6. The Formal Review

In addition to the regular review of risk registers a structured formal review should take place annually in April (or as soon as possible thereafter). Risks to annual policing plan, corporate plan and annual business plan outcomes should be considered. The 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 and early warning indicators still appropriate and effective?
- How can we be assured that the control measures for mitigating the risk are operating effectively?
- Overall, is there an effective risk management process in place?

7. Escalation/ Cross – Departmental Risk

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.

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.

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

8. Programme and Project Risk Management

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 organisation's strategic objectives…'*

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.

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

9. Partnership Risk Management

"Partners are defined as any organisation with which a department works to deliver their objectives, with a formal agreement of roles (contract, funding agreement, Service Level Agreement etc.). There may be a long-term relationship." (Managing Risks with Delivery Partners – HM Treasury /OGC).

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

- 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;

- ensure that the partnership has effective risk management procedures in place.

If the PSNI is the principal 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.

10. Internal Control

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.

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.

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 is made available to other key individuals in the process.

All Staff

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

Corporate Risk Manager

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

Other responsibilities include:

- Regularly review Departmental Risk registers and, where necessary, challenge the content on behalf of the Deputy Chief Constable (DCC);
- Report to the DCC on risk management within Departments and Areas;
- Collate and report on the Statements of Risk Management Assurance;
- Analyse risk registers to identify common themes/frequently occurring risks;
- Provide advice, guidance and assistance on risk management to the organisation;
- Promote and support the integration and synchronisation of risk management into the planning processes;
- Disseminate good practice;
- Liaise with Information & Communications Services Branch (ICS) regarding access to the Risk Management software;
- Liaise with Internal Audit regarding Risk Management;
- Report to the ServiceFirst Board (SFB) on the risk management process in the PSNI;
- Report to Audit and Risk Assurance Committee (ARAC) on Risk Management in the PSNI;
- Maintain contact/liaison with United Kingdom Police risk managers.

Risk Register Owner

The Risk Register Owner has overall responsibility for all risks on the risk register within their area of responsibility. Typically, the Risk Register Owner will be a Chief Officer, Department Head or Branch Head/Area Coordinator. The Risk Register

Owner may, if appropriate, appoint a Risk Owner to manage specific risks on their risk register. The Risk Register Owner will also have ultimate responsibility for deciding if a risk is sufficiently serious to be escalated to the next level of the organisation.

Risk Register Owners should make maximum use of monthly management meetings to manage risk actions and key controls and seek assurance that risk is being managed effectively. They are also responsible collectively for ensuring the management of risks which have strategic or cross-departmental implications for the organisation.

Risk Owner

Risk Owners are senior managers who are allocated responsibility for specific risks by the Risk Register Owner. They are responsible for the evaluation and control of those risks on behalf of the Risk Register Owner.

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 the risk. The Risk Owner will therefore constantly review the Risk Rating and the necessity to keep the risk on the register, where applicable, and report and recommend significant changes to the Risk Register Owner at monthly management meetings. There should always be one named Risk Owner for each identified risk.

Risk Manager

Risk Managers have been appointed for Areas/Branches 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.

Risk Action Owner (Responsible Officer)
Risk Action Owners (Responsible Officers) 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.

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:

- Implementing policies and procedures on internal control at an operational level;

- Encouraging staff to actively consider and manage risk;

- Undertaking risk reviews for their area of responsibility and carrying out necessary risk management actions;

- Communicating significant risks and control weakness for their area of responsibility to their senior management team;

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

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

- Ensuring that a suitable system of internal control operates in their area of responsibility.

Internal Audit
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.

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

- 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;

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

- Promoting risks and controls concepts across the department.

Audit and Risk Assurance Committee

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).

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

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

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

- To review Area and Departmental Risk Registers as part of their annual programme of work;

- To consider Internal Audit reports on risk management.

Appendix B Risk Report Template

RISK										
Describe the risk by considering the Cause (the situation that gives rise to the risk)**, the Event** (the consequence if the risk occurs) **and the Effect** (the impact that the risk would have should it materialise)**.** The description should be short and succinct and summarise the risk in a sentence. E.g. *There is a risk that the level of sickness absence within the organisation (cause) will have detrimental impact on service delivery (event), potentially impacting delivery of policing services in the future (effect).*										
INHERENT RISK RATING (Untreated)			**RESIDUAL RISK RATING (Treated)**			**TARGET RISK RATING**			**RISK OWNER**	**RISK MANAGER / ADMINISTRATOR**
Impact	**Likelihood**	**Total**	**Impact**	**Likelihood**	**Total**	**Impact**	**Likelihood**	**Total**		
Impact of risk occurring before any action is taken to manage it – See Appendix C	Likelihood of risk occurring before any action is taken to manage it – see Appendix C	Impact x Likelihood	Impact of risk occurring after action is taken to manage it – see Appendix C	Likelihood of risk occurring after action is taken to manage it – see Appendix C	Impact x Likelihood	The Impact that you want to get to - Appendix C.	The likelihood that you want to get to - see Appendix C.	Impact x Likelihood	The senior officer with overall responsibility for managing the risk.	The person responsible for maintaining the risk register under the direction of Risk Owners, and updating/amending risks as necessary.
GENERAL IMPACT						**DETAILS OF EARLY WARNING INDICATORS**				
What impact will this have on business/policing objectives if it is not addressed? (Multiple impacts may be added).						Indicator / performance data / measure which can be reviewed and updated on a regular basis to identify worsening trends e.g. absenteeism, complaints. (Multiple EWI may be added, if necessary).				
KEY CONTROLS TO MANAGE/MITIGATE THE RISK			**KEY ASSURANCE**			**RESPONSIBLE OFFICER**			**REPORTING FREQUENCY**	
List any key controls which are in place to manage the risk. E.g. *(Key controls should be listed in priority order in terms of their impact in mitigating the risk).*			How will you know that the key control is working effectively? *E.g. Monthly reporting at Management Meeting; Weekly checks conducted by Sergeant etc.*			The individual responsible for the Key Control.			I.e. Annually, Bi-annually, Quarterly, Monthly, Weekly, Daily.	
Multiple key controls may be added.										
ADDITIONAL ACTIONS TO MANAGE/MITIGATE THE RISK						**RESPONSIBLE OFFICER**		**START DATE**	**PLANNED END DATE**	
List other **actions, treatments and controls** which are being put in place to mitigate against the risk occurring. Actions should be **SMART**.						The individual responsible for completing the action.				
Multiple additional actions may be added.										

Appendix C Risk Assessment Matrix and Scoring Guide

1. Frequently the risk identification process will result in an unmanageable list of all the potential organisational 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.

3. 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.

4. Recommended Risk Rating responses can be found below.

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

Risk Matrix

Likelihood	**Almost Certain (5)**	5 (Low)	10 (Significant)	15 (Significant)	20 (High)	25 (High)
	Likely (4)	4 (Low)	8 (Significant)	12 (Significant)	16 (High)	20 (High)
	Possible (3)	3 (Low)	6 (Low)	9 (Significant)	12 (Significant)	15 (Significant)
	Unlikely (2)	2 (Very Low)	4 (Low)	6 (Low)	8 (Significant)	10 (Significant)
	Rare (1)	1 (Very Low)	2 (Very Low)	3 (Low)	4 (Low)	5 (Low)
		Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe (5)**
		Impact				

QUALITATIVE MEASURES OF RISK IMPACT

Impact	Score	Financial	Service Delivery	Litigation	Reputation	Injury
Insignificant	1	Potential or actual loss less than 5k	Negligible impact on Service Delivery or achievement of Departmental /Area Plans. No long term consequences.	Legal Challenge Minor out-of-court settlement.	Issue of no public concern.	Minor injury to individual.
Minor	2	Potential or actual loss 5k - £50k	Little impact on Service Delivery or achievement of Departmental /Area Plans. No long term consequences.	One-off settlement – no implications beyond the instant case.	Complaints from individuals. Minor impact on ability to engage with local communities.	Minor/Slight Injury to individual.
Moderate	3	Potential or actual loss £51k - £249k	Significant reduction in Service Delivery or Non-achievement of 1-2 targets on Departmental/Area Plans. Minimal long term consequences.	Moderate financial impact on limited range of cases.	Adverse local publicity. Significant impact on ability to engage with local communities.	Major/Significant Injury to an individual or several people.
Major	4	Potential or actual loss £250k - £499k	Serious reduction in Service Delivery or Non-achievement of a number of targets in Departmental/ Area Plans. Significant long term consequences.	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.
Severe	5	Potential or actual loss £500k or more	Major failure in Service Delivery or Non achievement of the majority of Departmental/Area Plans. Major long term consequences.	Serious and long term effects on the 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 MEASURE OF LIKELIHOOD			
DESCRIPTOR	**SCORE**	**PROBABILITY**	**DESCRIPTION**
ALMOST CERTAIN	5	1 in 10 chance	LIKELY TO OCCUR
LIKELY	4	1 in 100 chance	WILL PROBABLY OCCUR
POSSIBLE	3	1 in 1,000 chance	MAY OCCUR OCCASIONALLY
UNLIKELY	2	1 in 10,000 chance	DO NOT EXPECT TO HAPPEN
RARE	1	1 in 100,000 chance	DO NOT BELIEVE WILL EVER HAPPEN

RISK QUANTIFICATION MATRIX	
High	**16 - 25**
Significant	**8- 15**
Low	**3 - 6**
Very Low	**1 - 2**

Appendix D Risk Appetite

Risk management is high on the business agenda and we manage risks in a structured manner. Consideration and mitigation of risk is critical to the effectiveness of the system of internal control. The system of internal control is designed to maintain risk at a manageable level, based on risk appetite agreed by the SET to provide an acceptable level of assurance. Risk appetite will vary according to the perceived importance of the risks and their timing.

The PSNI's risk appetite categories are:

Averse	Avoidance of risk and uncertainty or for safe options that have a low degree of inherent risk and may only have limited potential for reward is a key objective.
Open	Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.

Appendix E Additional Guidance and Information

What is risk?

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'.

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.

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

What is Risk Management?

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. 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.

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.

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.

The **key benefits** of risk management are summarised below:

- Provides a framework for control;
- Encourages improved and better informed decision-making;
- Enables efficient allocation of resources;
- Affords increased certainty and fewer surprises;
- Protects and enhances image;

- Improves operational effectiveness/efficiency;
- Facilitates better service delivery;
- Enables more effective management of change;
- Minimises waste, fraud and poor value for money;
- Promotes more innovative approaches to the delivery of objectives;
- Improves strategic and operational planning.

Further Information

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

- Management of Risk (The Orange Book) – HM Treasury;
- Good Practice in Risk Management – NI Audit Office;
- Managing Risks with Delivery Partners – HM Treasury/OGC.

Appendix F Contact Us

Service Instruction Author

Corporate Risk Manager

Branch Email

PlanningAndGovernance@psni.pnn.police.uk