Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI1216
Policy Ownership	Corporate Services
Initial Publication	22/12/2016
Review Cycle	5 years from issue date
Reviewed	09/08/2022
Last Amended	09/08/2022
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 committed to effective and meaningful risk management as an integrated part of how we lead, direct and manage the Service.

The effective management of risk is a key element of good governance.

This instruction outlines how we will manage risk internally and with partners.

Keeping People Safe

Table of Contents

Table of Appendices

1. Introduction

In order to be successful in our mission of keeping people safe, the Police Service of Northern Ireland (PSNI) must proactively manage risk. Risk is inherent in everything we do to deliver high-quality services. Risk management is an essential part of governance and leadership, and fundamental to how the Police Service of Northern Ireland is directed, managed and controlled at all levels.

This Service Instruction, along with the Service Policy on Risk Management & Governance (SP16/16) provides a framework for staff and officers to manage risk. It is particularly relevant for risk owners and risk managers whose responsibilities are outlined in Appendix A. We have included key principles and advice from both The Orange Book (HMT) and the Good Practice in Risk Management (NIAO).

2. Key Principles

The Orange Book; Management of Risk - Principles and Concepts outlines five risk management principles.

A. Risk management shall be an essential part of **governance and leadership**, and fundamental to how the organisation is directed, managed and controlled at all levels.

B. Risk management shall be an **integral** part of all organisational activities to support decision-making in achieving objectives.

C. Risk management shall be **collaborative and informed** by the best available information and expertise.

D. Risk management processes shall be **structured** in a four step process as outlined in Section 6.

E. Risk management shall be **continually improved** through learning and experience.

3. Governance and Leadership

The Chief Constable is the Accounting Officer but delegates the responsibility for organisational governance, including the management of risk to the Chief Operating Officer (COO).

The Strategic Management Board (SMB):

- Owns, supports, promotes and accepts leadership responsibility for the adoption of risk management procedures and practice throughout the organisation; and

- Determines the organisational risk appetite.

The day-to-day management of risk will be undertaken by management with risk featuring as a standing agenda item at monthly management meetings at Departmental, Area and Branch level.

A Corporate Risk Report is provided to SMB monthly. This includes high level summaries of all corporate risks as well as information that supports executive management decision making. Decisions regarding material changes to corporate risks will be reported to the Audit and Risk Assurance Committee (ARAC) for information.

Corporate risks are subject to "deep dive" at ARAC with assurance provided to the Chief Constable on the adequacy and effectiveness of controls.

Twice yearly the Corporate Risk Manager will advise SMB and ARAC on the effectiveness and robustness of the risk management processes throughout the organisation.

4. Integration

The assessment and management of risks (both positive and negative) should be an embedded part of:

- Setting strategy and plans;
- Evaluating options and delivering programmes, projects or policy initiatives;
- Prioritising resources;
- Supporting efficient and effective operations;
- Managing performance; and
- Delivering improved outcomes.

Those responsible for setting strategy and policy, should use horizon scanning and scenario planning collectively and collaboratively to identify and consider the nature of emerging risks, threats and trends.

5. Collaboration and Information

Complicated and ambiguous risk scenarios are inherent given the dynamic and complex nature of policing. These risks require whole-system-thinking, aligned incentives, positive relationships and collaboration, alongside relevant technical knowledge, to support multi-disciplinary approaches to their effective management.

Effective relationships with partners, a mutual understanding of risk, and a proportionate approach to monitoring and reporting are critical. Where PSNI is the principal organisation in a partnership, consideration should be given to a Partnership Risk Register.

The Risk Management Processes (Section 6) should draw on the knowledge and views of experts and stakeholders. Those assessing and managing risks should consult with appropriate external and internal stakeholders to facilitate the; factual, timely, relevant, accurate and understandable exchange of information. Within the Police Service of Northern Ireland risks will on occasion require cross departmental co-operation and collaboration. Risk owners should secure commitment and co-operation from those effected departments. Where a risk requires action from more than one business area, the named risk owner will have overall responsibility for the management of the risk.

Communication should be continual and promote awareness and understanding of risks. Communication and consultation with relevant stakeholders will foster transparency and shared ownership and accountability.

6. Risk Management Process

Risk management with PSNI is a structured 4 step process and will include:

1. Risk identification and assessment
"To determine and prioritise how the risks should be managed"

A range of techniques for identifying specific risks that may potentially impact on one or more business objectives can be used. These may include; horizon scanning, audit/inspection findings and lessons learned reviews. Risks should be identified whether or not their sources are under the Service's direct control. Risks should then be assessed using the standardised matrix.

There are three risk ratings to be considered:

Rating	Refers to
Inherent Risk	The untreated risk and the impact and likelihood of it

	occurring before any action is taken to manage it.
Residual Risk	The treated risk and the impact and likelihood of it occurring after considering the key controls and additional actions in place
Tolerable Risk	The level of risk deemed acceptable according to our risk appetite.

2. Risk Treatment
"The selection, design and implementation of controls and actions that support achievement of intended outcomes and manage risks to an acceptable level."

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived against the costs, efforts or disadvantages of proposed actions. Effective risk treatment options or control measures should actively contribute to the reduction or management of the risk. Ineffective control measures will require additional actions to strengthen the assurance they provide.

3. Risk Monitoring "The design and operation of integrated, insightful and informative risk monitoring."

Monitoring should play a role before, during and after implementation of risk treatment. Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which control measures are operating as intended to provide reasonable assurance over the management of the risk.

The "three lines of defence" model sets out how these aspects should operate in an integrated way to manage risks, design and implement internal control and provide assurance through; ongoing, regular, periodic and ad-hoc monitoring and review. There should be no gaps in coverage and no unnecessary duplication of effort.

4. Risk Reporting
"Timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities."

The information should support the risk owner to assess whether decisions are being made within its risk appetite to successfully achieve objectives, to review the adequacy and effectiveness of internal controls, and to decide whether any changes are required to; re-assess strategy and objectives, revisit or change policies, reprioritise resources, improve controls, and/or alter their risk appetite.

Principal risks should be subject to “deep dive” reviews with those responsible for the management of risks and with appropriate expertise present at an appropriate frequency depending on the nature of the risk and the performance reported.

7. Risk Registers

Within the Police Service of Northern Ireland, 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 its content will change frequently as risks are mitigated and new risks emerge.

Risk Register Ownership	
Corporate Risk Register	Contains strategic risks and is owned by the SMB
Departmental Risk Register (DRR)	Relates to activities within the control of a Department and owned by the ACC/ACO.
Branch Registers	Relate to activities within a branch and are owned by the Head of Branch.

Refer to Section 6 to see the process to follow when identifying and managing risks.

8. Escalation

It is important that risks are managed at the appropriate level within the organisation. During reviews, the risk owner should 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. Similarly, risks should be considered for de-escalation when the residual risk rating is at the tolerable level.

The escalation point to the Corporate Risk Register (CRR) is a residual risk rating of

16 or more. Escalation can be requested by the Risk Owner or the Corporate Risk Manager. Accordingly risks may appear on the Corporate Risk Register and Departmental Risk Register, however the primary management of the risk remains within the Department.

Should the PSNI, as an Arm's Length Body (ALB) of the Department of Justice (DoJ) believe a risk requires escalation higher than the CRR, it can be escalated to the DoJ's corporate risk register.

Department Risk Registers (DRR) identify risk to the Departmental effectiveness and efficiency. These should be reviewed monthly at the Departmental Management Meeting or other accountability meeting.

Branch/Area risk registers should also be maintained and discussed regularly at management meetings. Risks can be considered for escalation at these meetings.

Project/Programme Risk Registers are also supported. As before, risks on these registers can be escalated to DRR or CRR where appropriate.

Risk Registers will be maintained, reviewed and updated as necessary on a monthly basis.

9. Programme/Project Risk Management

All programmes and projects should be subject to comprehensive but proportionate risk management.

Section 5 Collaboration & Information is particularly important for programme/project managers. Programme/project managers 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. Project risks may be escalated up to and including the CRR.

10. Partnership Risk Management

There may be a different, but aligned, risk management process for partnerships with external organisations. The management of risks and the operation and oversight of internal control should be considered across this extended enterprise. This requires collaboration and cross-organisational working through a range of public sector, private sector and third-sector partnerships.

Effective relationships and partnership working between departments and arm's length bodies, a mutual understanding of risk, and a proportionate approach to monitoring and reporting are critical.

In relation to risk management the PSNI must meet two key responsibilities for each partnership[1] 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 risk register, with those risks relating to the PSNI managed and monitored by the appropriate PSNI lead officer through the risk management system.

If PSNI is in partnership with an external organisation then any procurement made on behalf of the partnership should, as a minimum, meet the Procurement Control Limit (PCLs) as set out in the PSNI's Procurement and Contract Management Guidance.

11. Continual Improvement

Risk management shall be continually improved through learning and experience. 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). 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?

[1] A partnership under this definition will have a formal agreement of roles (contract, funding agreement, SLA).

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

Lessons learned will be collated after formal reviews by Corporate Governance and shared across the organisation.

The Corporate Risk Manager will also undertake reviews of the robustness and effectiveness of the risk management process on a six monthly basis. Area Coordinators and Departmental Heads are required to assist in this process by signing a Statement of Risk Management Assurance on a half-yearly basis. As well as providing assurance that risk is being actively managed and reflected accurately in the Risk Registers.

Appendix A Roles and Responsibilities

Managing risk is the responsibility of **all staff**. However, there are roles within the process which are crucial to the successful management of risk.

Roles and Responsibilities	
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 Chief Operational Officer (COO) is responsible for the management and coordination of the organisation's risk policies and activities.
Board	The Strategic Management Board (SMB) owns, supports, promotes and accepts leadership responsibility for the adoption of risk management within PSNI. SMB has overall ownership of all the risks on the CRR.
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.
Governance	The Head of Corporate Governance has responsibility: • To support a risk management training programme for the service. • To ensure appropriate training for the corporate risk manager.
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.

Roles and Responsibilities	
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 COO has responsibility for coordinating and overseeing the risk management process and systems at all levels within the organisation. The Corporate Risk Manager is available to provide risk management advice to Gold Commanders.
Risk Managers	Area Coordinators/Heads of Departments and Branch Heads 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. Risk managers are available to provide risk management advice to Silver and Bronze Commanders.
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 support the Chief Constable, in his role as Accounting Officer, in relation to his responsibilities for governance, risk management and internal control. The ARAC also advises the Chief Constable on the "adequacy and effectiveness" of the risk management processes.

Appendix B Risk Assessment Matrix and Scoring Guide

1. The risk identification process can 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:

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

ii. 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.

Rating	Refers to
Inherent Risk	The untreated risk and the impact and likelihood of it occurring before any action is taken to manage it.
Residual Risk	The treated risk and the impact and likelihood of it occurring after considering the key controls and additional actions in place
Tolerable Risk	The level of risk deemed acceptable according to our risk appetite.

4. 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 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

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.

Appendix C Contact Us

Content Author

Corporate Governance

If you have any comment to make on the content of this Service Instruction please contact Corporate Governance.

Branch Email

zPlanningAndGovernance