National Police Information Security Risk Framework

ABSTRACT:
This framework is to ensure that all security risks are identified, assessed, and managed in accordance with best practice in order to facilitate improved governance. It is mandatory for all information systems that hold Police information, or which deliver an operational service to policing to undergo a risk assessment, as stipulated in the National Policing Community Security Policy.

The Security Risk Management Framework mutually supports the Police Cyber Assurance Framework (PCAF). The framework supports the requirements of the National Community Security Policy (NCSP).

ISSUED	April 2025
PLANNED REVIEW DATE	February 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This policy is due for review on the date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Introduction

1. UK policing faces threats to its national systems and the information assets they contain, ranging from highly resourced threat actors to individuals, including physical as well as cyber attack methods, malicious activity and accidents. The National Police Senior Information Risk Owner (NSIRO) is committed to ensuring that these threats do not result in unmanageable risks, and to use risk management to identify and manage risks at a national level.

Security risk management enhances UK policing's ability to manage uncertainty and drive improvement. It provides a comprehensive, systemic approach to help policing organisations identify threats, vulnerabilities, impact levels and the resultant risks, and then to ensure that those risks are managed effectively through life in a consistent, efficient and repeatable way. It also sets out the responsibility for accepting risks, via the delegated authority derived from the NSIRO, to nominated individuals and organisations. This document sets out the National Police Information Security Risk Management framework and provides the NSIRO's risk appetite statement.

Policy Alignment

2. It is mandatory for all information systems that hold Police information, or which deliver an operational service to policing to undergo a risk assessment, as stipulated in the National Policing Community Security Policy. The Security Risk Management Framework mutually supports the Police Cyber Assurance Framework (PCAF).

Aim

3. The aim of the National Police Information Security Risk Management Framework is to ensure that all security risks are identified, assessed and managed to facilitate improved governance.

Objectives

4. To support the aim of this framework, the following objectives have been set.

- Delivery of a risk management methodology which allows for a repeatable process at the national level,
- Providing improved risk information to key decision-making bodies, and
- Improved understanding of system risk across policing at a national level and potential risk aggregation.

Scope

5. The scope of the National Police Information Security Risk Management Framework covers:

- All information owned by policing held in national police systems, or by third parties,
- Any system providing an operational service to national policing,
- Supporting functions and facilities to the above, and
- Security Risk Management Governance.

Governance Structure

6. The diagram on the next page provides an overview of the national risk management governance model.

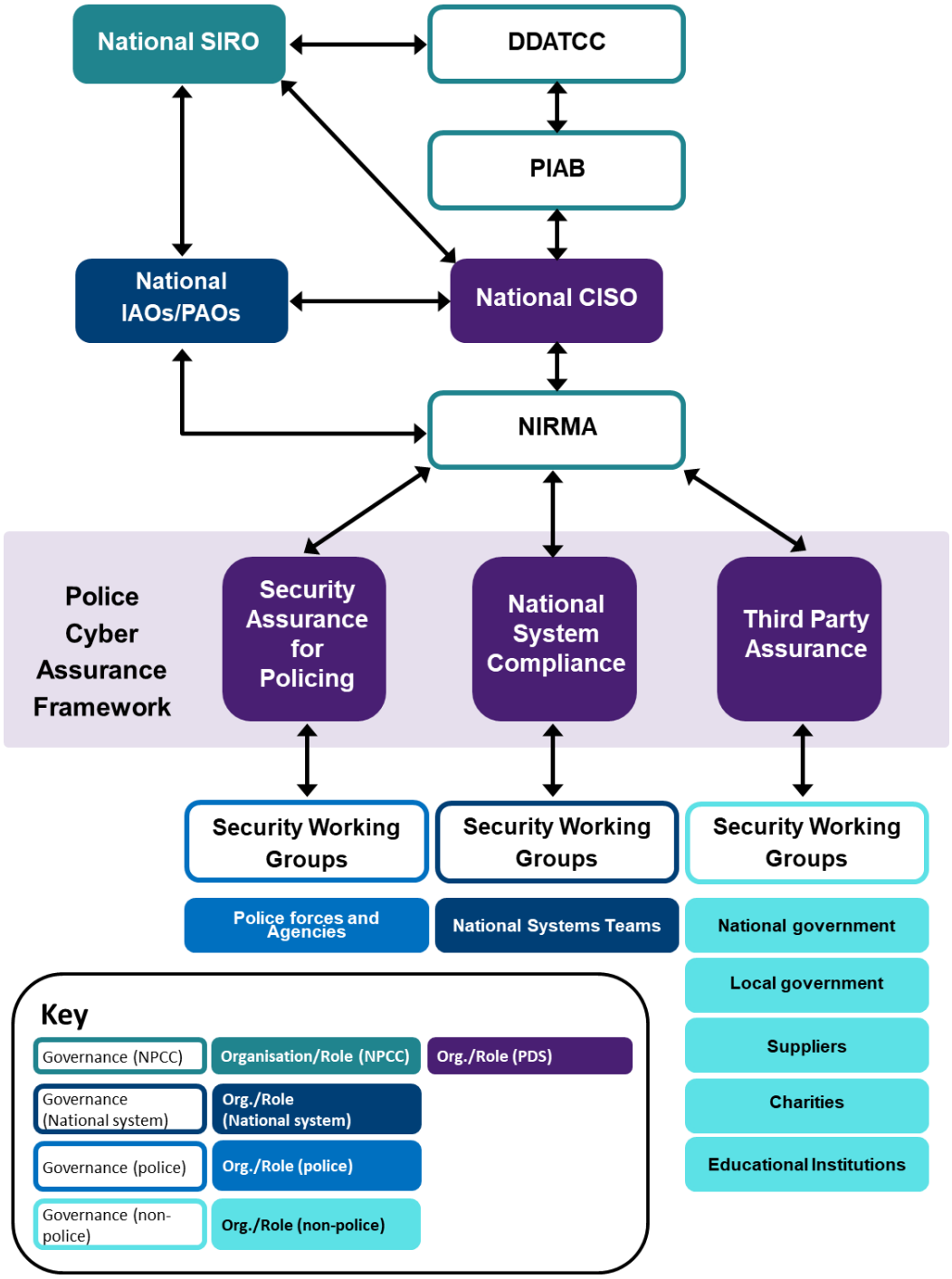

Figure 1- Risk Management Structure

7. The following bodies and individuals have key responsibilities in national risk management.

7.1 **Digital Data and Technology Coordination Committee (DDaTCC).** DDaTCC is responsible for ensuring that technology is used to deliver policing capability securely.

7.2 **Police Information Assurance Board (PIAB).** PIAB is responsible for providing guidance and direction to information assurance activities within policing at a national level and will consider national risks as part of its remit.

7.3 **National Information Risk Management Authority (NIRMA).** This forum provides a strategic overview of risk across policing on behalf of the PIAB Chair and PDS CISO and manages the Police National Information Security Risk Register.

7.4 **National Senior Information Risk Owner (NSIRO).** The NSIRO is the senior risk owner for national policing systems and data. The key duties and responsibilities of the NSIRO are captured in the SIRO Handbook, published by the NPCC.

7.5 **National Information Asset Owners (NIAOs).** NIAOs are the risk owners responsible for individual systems and/or data sets. The key duties and responsibilities of the NIAOs are captured in the IAO Handbook, published by the NPCC.

7.6 **National Platform Asset Owners (PAOs).** PAOs are the risk owners responsible for individual platforms.

7.7 **National Chief Information Security Officer (NCISO).** The NCISO is responsible for ensuring that the senior risk owners across policing are provided with appropriate advice on risk management.

7.8 **Security Working Groups (SWGs).** SWGs sit below the national risk management level and play a crucial role in escalating risks up to the national level, where they meet the criteria, and for the remediation of risks at a national and local level. It is a requirement for each national system to run a routine SWG.

Risk Management process and methodology

Setting the risk appetite

8. Risk appetite is the level of risk that an organisation is willing to accept while pursuing its objectives, and before any action is determined to be necessary to reduce the risk. Setting the correct risk appetite is important to ensure that the implementation of security controls is appropriate. Risk appetite is normally expressed as one of five levels:

- **Eager.** An organisation will take justified risks and will accept the possibility of failure in the pursuit of the potential benefits.
- **Open.** An organisation will take strongly justified risks (with appropriate mitigations) in the pursuit of potential benefits.
- **Cautious.** An organisation's preference is for safe delivery with limited tolerance for risks where there is a very strong operational benefit.
- **Minimal.** An organisation's approach is extremely conservative and will only look to accept risks if essential and there is a limited risk of failure.
- **Averse.** The organisation will always select the low-risk option and is not willing to trade risk against potential benefits.

9. Furthermore, a risk appetite must be set for the confidentiality, integrity and availability of the system or data under assessment, including proofs of concept. Applying a single summarised risk appetite across the CIA triad risks expending too much or too little resource in mitigating specific risks.

For national systems, the default risk appetite setting is:

	Default Risk Appetite	
	National Systems	**CNI**
Confidentiality	Minimal	Minimal
Integrity	Minimal	Averse

Availability	Minimal	Averse

A more cautious risk appetite may be applied to specific systems/data. Guidance on setting risk appetite is contained in Annex A.

10. Risk appetite must be reviewed annually in line with Business Impact Assessment.

Risk Appetite and Decision Making

11. Risk appetite setting influences decision making, with greater authority devolved for risks in environments with more open appetites. This is presented in the diagram below, with risk ownership/ acceptance levels aligned to risk appetite. The national risk management decision making delegation is highlighted for a Minimal risk appetite, representing the default for National Systems.

Risk Level	Risk Appetite				
	Eager	Open	Cautious	Minimal	Averse
Very Low	PDS	PDS	PDS	PDS	PDS
Low	PDS	PDS	PDS	PDS	NIAO/ F SIRO
Medium	NIAO/ FSIRO	NIAO/ FSIRO	NIAO/ FSIRO	NIAO/ FSIRO	NSIRO
High	NIAO/ FSIRO	NSIRO	NSIRO	NSIRO	NSIRO
Very High	NSIRO	NSIRO	NSIRO	NSIRO	NSIRO

Table 1 - National Risk Management Decision Making Delegation Matrix

- **National SIRO.** The National SIRO is the ultimate risk owner for policing and provides a decision on the most serious of risks at a national level.

- **National IAO/PAO.** A National IAO/PAO is responsible for approving and managing risks which fall solely within their area of responsibility, and which are within the risk levels

specified above depending on the risk appetite for the system or data concerned. If a risk level exceeds their remit (or involves a risk that spans the area of responsibility for multiple IAOs/PAOs) then it is escalated to the National SIRO. A register of all National IAOs and PAOs is held by PDS Cyber Services.

- **Force SIRO.** Force SIROs are responsible for the risks within their own forces until those risks exceed the set risk appetite. Where there is connectivity to national systems, the risk appetite for forces mirrors the national risk appetite, with the risk appetite set out above.

- **PDS Cyber Specialists and Compliance Specialists.** Cyber Specialists and Compliance Specialists operate on behalf of the NSIRO to ensure that risks are identified and managed in the development and operational phases respectively. They do not own risk but provide advice to risk owners on whether a risk is an acceptable one in line with the national risk appetite. They have delegated risk acceptance levels for risks as detailed above. For local systems, the role of the PDS specialists may be assumed by local information security teams.

Assessing a risk

12. Once the risk appetite has been identified, the risk(s) must be assessed. Direction on assessing national risks is contained in the National Police Information Security Risk Assessment Guidance document, which may also be used for guidance below national level.

13. PDS has developed a Police Security Risk Assessment methodology which will be used for undertaking risk assessments. Details on how to complete the Police Risk Assessment are provided in the National Police Information Security Risk Assessment Guidance.

Police National Information Security Risk Register

14. The national risk register is maintained by PDS, with access enabled for PIAB and NIRMA members. The risk register will contain all information security risks identified at a national level, including those that have been formally closed. The process for adding or managing risks onto this register is detailed in the National Police Information Security Risk Assessment Guidance.

National level risks may be escalated from:

- Security Assessment for Policing (SyAP) risks,

- Third Party Assurance for Policing (TPAP) risks,

- National System Compliance risks,
- Cyber Delivery risks (where applicable, see point 15), or
- Risks relating to PCAF performance.

National Risk Criteria

15. To be considered suitable for insertion into the Police National Information Risk Register, a risk must

- Be directly related to a national police system and exceed that system's risk appetite, and/or
- Be a combination of multiple risks that collectively create a national level risk, and/or
- Relate to the performance of policing at a national level against the PCAF.

Risks must remain on local risk registers with a remediation plan documented, progressed and managed.

Project Risks

16. During the development of systems, risks will be assessed which will be managed as part of that project before it enters service. Project risks will not be recorded on the Police National Information Security Risk Register. Only if there is a live risk involving police data and/or the provision of operational services to policing (and exceeds the national risk appetite) will it be reported on the Police National Information Security Risk Register. Any risks relating to a system in development which cannot be mitigated to within the national risk appetite will be raised for risk owner decision prior to delivery into service.

Key Artefacts

17. The following artefacts support this framework:

- NMC Annual National Policing Threat Assessment,
- National Police Information Security Risk Assessment Guidance[1],

[1] See Guidance on National Standards Portal

- Information Security Risk Balance Case template[2], and
- National Police Information Risk Register.

[2] See Template on National Standards Portal

Annex A – Risk Appetite Guidance

Below are the suggested risk appetite levels for different types of cyber and information security asset. This list is not exhaustive.

Asset Category	Description	Confidentiality	Integrity	Availability
Police marketing and communications	Information generated, collected, stored and used for internal and external marketing and communications	Eager	Open	Open
Personal data	Personal data, as defined by UK GDPR, of all staff and citizens	Cautious	Cautious	Cautious
Special Category data	As defined by UK GDPR, for example • personal data revealing racial or ethnic origin, • personal data revealing political opinions, • personal data revealing religious or philosophical beliefs, • personal data revealing trade union membership, • genetic data, • biometric data (where used for identification purposes), • data concerning health	Minimal	Minimal	Minimal
Commercial/ procurement/ supplier	Information collected, stored and used throughout the procurement process	Cautious	Cautious	Cautious

Asset Category	Description	Confidentiality	Integrity	Availability
Police corporate information	Information generated, collected, stored and used by the corporate functions of forces, including security metrics, policies, etc	Cautious	Cautious	Cautious
Data delivering operational police effect	Data which supports policing operations which is not included in one of the specific category types covered, including evidential data and intelligence that is not personal data.	Minimal	Minimal	Minimal
OFFICIAL	Information which has been classified as OFFICIAL	Cautious	Cautious	Cautious
SECRET	Information which has been classified as SECRET	Averse	Cautious	Cautious
TOP SECRET	Information which has been classified as TOP SECRET	Averse	Cautious	Cautious
Data relating to staff in sensitive posts	Personal data, as defined by UK GDPR, that identifies personnel in certain sensitive roles, such as covert intelligence gathering	Minimal	Minimal	Minimal
Covert intelligence	Information generated, collected, stored and used during covert intelligence operational processes	Averse	Minimal	Minimal
Counter terrorism	Information generated, collected, stored and used in the course of counter terrorism operational processes	Averse	Minimal	Minimal
Test / Synthetic data	Data used for testing purposes	Open	Open	Open
Code / Configuration data	Information generated, collected, stored and related to system configuration.	Minimal	Minimal	Minimal

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	C Cope	Initial draft	09/06/22
0.2	C Cope	Revised version	10/08/22
0.3	C Cope	Incorporating peer review comments	19/12/22
0.4	C Cope	Updated following NIRMA review	08/02/23
0.5	C Cope	New branding	22/02/23
1.1	R Rees	New Template Minor changes as documented in accompanying change sheet.	18/02/25

Approvals

Version	Name	Role	Date
1.0	ACC P O'Doherty	Chairperson - Police Information Assurance Board	12/05/23
1.1	ACC P O'Doherty	Chairperson - Police Information Assurance Board	15/04/25

Document Owner

Name	Role
Christopher Cope	PDS National Head of Audit, Risk & Compliance