NPIRMT

National Police Information
Risk Management Team

Information Management Business Area

National Policing Information Risk Escalation Policy

V1.0

January 2015

Introduction

1. This policy sets out the National Policing Information Risk Escalation Policy and describes the risk escalation case process.

2. This document will be held and maintained by the Police Information Assurance Board who will regularly review the Risk Escalation Policy and make recommendations to the National Police SIRO to ensure that the Police Service maintains the ability to exploit opportunities while sensibly managing exposure to risk.

3. Risk management is not only means mitigating risk, but also taking considered risks where the rewards are expected to be greater than any short-term losses. Effective governance results in business processes and capabilities that are designed, controlled and optimised to effectively and efficiently utilise information assets.

Scope

4. This document relates to the National Police Information Assets for which Chief Officers are Data Controllers[1] in common and extends to all systems, whether national or local, that access this information.

5. In conjunction with the National Policing Information Risk Appetite this document provides the framework for which all information risk decisions in relation to Nationally Connected Systems and National Police Information Systems should be made.

6. While not applying to segregated force systems, SIROs may find that the adopting the principles of this policy locally will support their information assurance maturity.

7. The National Policing Information Risk Appetite outlines the circumstances in which force SIROs should contact the relevant National Information Asset Owner and/or the National Police SIRO when variances between local and national risk appetites occur.

8. Where systems that contain police information are jointly accredited, these may be subject to different arrangements by agreement.

[1] a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Risk Escalation Case

Purpose

9. In the context of this policy a risk escalation case (“REC”) is used to formally escalate information risks related to Nationally Connected Systems or National Police Information Systems to the relevant National Information Asset Owner and/or the National Police SIRO who will either:

   a. Accept the risk on a permanent or temporary basis.
   b. Require the risk to be further mitigated.
   c. Not accept the risk.

10. RECs will usually be raised by Force SIROs, National Accreditors for the Police Service or National IAOs.

11. The circumstances where a REC is required are varied but include where:

    a. The level of residual risk is greater than a National Accreditor or National IAO is authorised to accept on behalf of the National SIRO. Levels of authority are set out in the risk delegation matrix below.
    b. The accreditor and risk owner do not agree the acceptance of residual risk.
    c. There is limited time to implement an agreed risk treatment plan and a temporary waiver or acceptance is sought.

12. A REC should not be used to avoid considering risk mitigation options or to bypass the accreditation process.

13. Residual risk level and risk appetite determine the level of authority required to accept the residual risks. For National Police Information Systems and Nationally Connected Systems this is set out in Table 1:

Residual Risk Level	Risk Appetite				
	Averse	Minimalist	Cautious	Open	Hungry
Very Low	National Accreditor	National Accreditor	National Accreditor	National Accreditor	National Accreditor
Low	National IAO	National Accreditor	National Accreditor	National Accreditor	National Accreditor
Medium	National SIRO	National IAO	National IAO	National Accreditor	National Accreditor
Medium-High	National SIRO	National SIRO	National SIRO	National IAO	National Accreditor
High	National SIRO	National SIRO	National SIRO	National SIRO	National IAO
Very High	National SIRO	National SIRO	National SIRO	National SIRO	National SIRO

Table 1: National Information Systems risk delegation matrix

Content

14. A REC will be written in clear business language so that often complex technical issues can be readily understood and balanced by the relevant National Information Asset Owner and/or the National Police SIRO. As a minimum It will set out:

    a. The business background (stakeholders, business need, benefits, costs, business impact etc).
    b. The threats to the Nationally Connected System or National Police Information System that area associated to the REC.
    c. The likelihood of these threats occurring.
    d. The risks associated with these threats.
    e. The mitigation options that have been considered.
    f. The mitigation options that have been implemented.
    g. The rationale for not implementing any mitigation options.
    h. The residual risks.
    i. Recommendations.
    j. Risk acceptance decision.

15. Where residual risks have already been accepted by the National Accreditor or National IAO this should be made clear in the REC. There is no requirement for the relevant National Information Asset Owner and/or the National Police SIRO to consider accepting these risks however it is essential that decisions are made is on the basis of all the available information.

Responsibilities

National Accreditor

16. The National Accreditor will:

    a. Highlight to a National IAO or project team when a REC is needed for a Nationally Connected System or a National Police Information System.
    b. Support the project team or national IAO in completing the REC, in particular in articulating the risks to the information system.
    c. Quality assure the REC prior to escalation to ensure that it is an accurate representation of the identified risk.

National Information Asset Owner

17. The National IAO will:

a. Identify when a REC is needed for a Nationally Connected System or a National Police Information System.
b. Take responsibility for authoring the REC.
c. Submit the REC to the National Police SIRO via the National Information Risk Manager.

Definitions

Force

18. This should be taken to mean all forces and agencies in the UK that are within the National Policing Community Security Policy.

National Police Information System

A National Police Information system is:

- One, which is provided for the Police community as a whole and managed centrally[2], and
- It must be used by a number of forces (at least 10), and
- Police ICT Directorate and/or PNC Services of the Home Office have a contractual relationship with the service provider and/or the service management of the system.

Nationally Connected System

19. A system that is owned by a force, or jointly between forces, that is connected to national infrastructure (e.g. CJX, PSN etc) that is connected or has access to one or more National Information Systems including email.

Segregated Force System

20. A system that is owned by a force, or jointly between forces, and is either separate or securely segregated from a force's nationally connected corporate network and has no access to National Information Systems, associated national data or to national infrastructure, including email.

[2] Managed centrally makes the distinction that the system is not distributed (e.g. PNC which is hosted and administered centrally) or a distributed system, hosted and managed at individual force level (e.g. Holmes 2). A system in a cloud environment which is centrally administered is considered a centrally managed system.

Risk Appetite

21. The amount of risk that an organisation is prepared to accept or to be exposed to at any point in time. Risk appetite levels are set out in Table 2:

Risk Appetite	Description
Averse	Avoidance of risk and uncertainty is a key organisational objective.
Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk.
Cautious	Preference for safe delivery options that have a low degree of residual risk.
Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc).
Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

Table 2: Definition of risk appetite categories

Residual Risk

22. The risk that remains after risk treatment measures have been implemented. Residual risk levels are described in Table 3:

Residual Risk Level	Description
Very Low	Indicates maximum confidence. That risks throughout the life of the system have been identified to a high level of certainty and are being treated/managed effectively. Remaining risks are within the risk appetite. It is very unlikely the residual risks will require an escalation case
Low	Risks throughout the life of the system have been identified. Treatment plans and mitigations are in place to bring it within the risk appetite. Remaining risks are within the risk appetite. It is unlikely the residual risks will require an escalation case.
Medium	Current risks have been identified and treatment plans and mitigations are in place to bring it within the risk appetite. Risks throughout the system's life may not be fully identified or have detailed treatment plans. It is probable that residual risks will require an escalation case
Medium-High	Current risks have been identified and have treatment plans. Risks throughout the system's life may not be fully identified or have detailed treatment plans. Mitigations/controls may not be fully in place. Risks may not be within the risk appetite. Probable an escalation case will be necessary.
High	Current risks have not been identified and may not have treatment plans. Mitigations/controls may not be fully effective or in place. Risks will need an escalation case if they are outside the risk appetite

Very High	Risks have not been identified and/or do not have treatment plans. Mitigations/controls are not effective, in place or may not exist. Risks will need an escalation case if risks are considered outside the risk appetite

Table 3: Definition of residual risk levels

Risk Tolerance

23. Whereas risk appetite refers to risk at a corporate level, risk tolerance allows for variations in the amount of risk an organisation is prepared to tolerate for a particular project or business activity. It recognises that different types of risk within the overall appetite may have different thresholds. A risk tolerance case will allow SIROs to adjust risk appetite to allow for this in local systems.

24. Where Nationally Connected Systems or National Police Information Systems are concerned however the process for applying a risk tolerance will mirror that of a risk escalation case.

Appendix A - Risk Escalation Case Template

RISK CASE DECISION

This details the decision by the appropriate risk owner.

INTRODUCTION

It should include the authorship of the document and the list of stakeholders consulted. For Forces/Agencies, this list could include:

- The National and Force/Agency Accreditor
- The National and Force/Agency Information Asset Owner
- Information Risk Owner
- Project Owner

TERMINOLOGY

This section should describe any particular terminology used in the REC in simple English.

BUSINESS BACKGROUND

This section should clearly outline the business requirements, including:

- the business benefits of delivering the capability, including timescales as relevant; and
- the business impact of not delivering the capability.

THREATS

This section identifies the threats associated with this REC.

LIKELIHOOD

This section estimates the likelihood of threats materialising.

RISKS

The residual risks above the risk appetite should be documented in the REC and should be clearly explained, e.g.:

“There is a risk that if the network is compromised by external hacking, unauthorised access to intelligence data would result, leading to the following impacts:

compromise of investigation

damage reputation

etc”

MITIGATION

This details the mitigations in place to reduce the risks.

RESIDUAL RISKS

This section details the residual risks left once the mitigations have been implemented.

RECOMMENDATION

This section is where the author should make a recommendation for the preferred option, or a subset of options if a further decision is required. It should include clear justification for the decision and a concise explanation of why the options not chosen have been rejected.

In this section the National Accreditor should also comment on the recommendation from an accreditation and quality perspective. Any comments from the IAO would also be included in this section.

RISK ACCEPTANCE DECISION

Risks escalated in REC should either be accepted or mitigated (if not accepted by relevant National Information Asset Owner and/or the National Police SIRO). This section documents the decision that needs to be made by the risk owner.