| | |
|---|---|
| *Document Name* | **ACPO/ACPOS National Information Risk Appetite Statement** |
| *File Name* | ACPO_ACPOS National Information Risk Appetite v1_3.doc |
| *Authors* | Adam Clark and James McLelland |
| *Reviewer* | James McLelland (15/05/2012) |

| | |
|---|---|
| *Authorisation* | ACPO PIAB, ACPO IMBA, ACPOS IM |
| *Signed version held by* | NPIA Information Assurance Capability Team |



For additional copies, or to enquire about the content of the document, please contact the National Information Assurance team at the following e-mail address: information.assurance@npia.pnn.police.uk

# National Information Risk Appetite Statement

## Purpose of Document

The purpose of this document is to inform force/agency SIROs, National Information Asset Owners, National and force/agency Accreditors/Projects/programmes and other interested parties of the National Information Risk Appetite and its implications. This document should be read in conjunction with the BRG on Risk Appetite and for further detail the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document.

It has two distinct foci:

1. National Information Systems risk management and governance.
2. Force/agency risk management and governance, involving National Information Systems.

## Requirement

It provides a baseline for managing information risks for National Information Systems for example PND, PNC, ViSOR, Holmes, Ident1, etc…and National Police Infrastructures, e.g. CJX and xCJX, based on the need to protect information that is shared by various police forces, law enforcement agencies, government and voluntary bodies.

When addressing risk it is important the controls applied are pragmatic, appropriate and cost effective (PACE), and the National Information Risk Appetite will assist forces/agencies, National Projects/ Programmes and others to manage information risks by setting out delegation authority for accepting or escalating identified information risks regarding National Information Systems and the data they hold regardless of its business impact level or protective marking.

The National Information Risk Appetite forms part of the overall national IA governance for information risk management in the Police Service and is owned by the National SIRO (see the ACPO/ACPOS IA Governance guidance for further information).

## The National Information Risk Appetite

The National Information Risk Appetite has been set at **Cautious** for National Information Systems. This has been agreed and endorsed by the National SIRO, ACPO PIAB, ACPOS IARC, and ACPO IMBA.

The National Information Risk Appetite is reviewed on an annual basis or as required.

The National Information Risk Appetite reflects the need for the police service to protect and risk manage the information it handles, as compromise of its confidentiality, integrity and availability could impact police operations, personal or sensitive information and increases risks to the compliance or legal standing of the organisation.

In agreeing the National Information Risk Appetite the National SIRO, ACPO PIAB, ACPOS IARC and ACPO IMBA considered a number of categories of risks assessing the risk appetite for each (see Appendix A) in light of their understanding of the National Police Threat Model based on threat assessments promulgated by the CPNI, the CESG and SOCA.

The National Information Risk Appetite applies to all National Information Systems. It also applies to local force/agency systems, which are connected directly or indirectly to National Information Systems for example; force/agency e-mail services and force/agency networks that are connected to the CJX or xCJX, or use data from National Information Systems for example, through an interface to update or retrieve information from National Information Systems to local force/agency systems, such as PNC Phoenix or locally developed systems/applications.

The National SIRO must be informed of any residual risks which affect National Information Systems and is the final arbiter on those residual risks**,** as set out in the delegation matrix at Appendix B.

**Implications**

The level of the National Information Risk Appetite provides specific guidance for National and force/agency Accreditors, project owners and senior information risk owners.

- It indicates to National and force/agency Project Owners the extent to which they need to mitigate risks to information that are inherent in new systems.
- It informs National and force/agency Accreditors and force/agency Information Asset Owners (System Owners) when they are able to sign off a risk as being acceptable to the business, by virtue of it being within the risk appetite. If a risk is outside of the risk appetite then it will be escalated to the National or force/agency Senior Information Risk Owner (SIRO) depending on the level of the residual risk, for a decision on whether to accept it, invest in mitigating it, or avoid the risk.
- It guides the force/agency Senior Information Risk Owner (SIRO) in the organisation; to whom the information risks are escalated to and, in the types and levels of information risk they can accept on behalf of their organisation.
- It informs the force/agency SIRO and National Systems IAO when they are required to escalate residual risks (using the Risk Escalation Case process) to the National SIRO (see Delegation Matrix at Appendix B).

Where a Force/agency network or system connects directly or indirectly to the CJX or xCJX it potentially offers a route, which could enable unauthorised or malicious access to or attacks on National Information Systems or the data they hold. The implication of this is those force/agency networks and systems are expected to adopt the National Information Risk Appetite when assessing risks and setting out delegation authority in their respective force/agency and this will form part of the approval to connect to those National Information Systems.

This statement does not restrict forces/agencies from taking decisions that may involve risks to the security of information. Rather it ensures that such decisions are properly assessed and have accountability at the appropriate level. Where residual risks[1] are identified through accreditation of local systems e.g. if the force/agency system connects to or uses data from a National Information System and the residual risk would need to be escalated to the force/agency SIRO (as determined by the appropriate delegation matrices, see Section 3.9.6 of the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document). If the residual risk is outside the delegated authority of the force/agency SIRO, as at Appendix B, then the force/Agency SIRO would need to escalate those risks to the National SIRO for a decision using a Risk Escalation Case. Further detail on this can be found in Section 4.3.5 of the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document.

Some individual force/agency systems, which connect directly or indirectly to National Information Systems may, with the approval of the National SIRO, qualify for Tolerance levels, which vary from the National Information Risk Appetite. For example when systems are delivering political or operational imperatives, or have become directly critical to police operations that need a more Open Tolerance to Risk. Conversely information systems, which handle information which is politically sensitive, or passes sensitive information to parties with questionable handling procedures, may have a more minimalist tolerance of risk. Section 3.10 of the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document deals with Tolerance for individual information systems.

Force/agency SIRO's should set and endorse a risk appetite for their force or agency. This can be viewed as an up-front decision on what level of risk is acceptable and conversely, what level of risk demands a balance of risks and reward at a more senior level than the Accreditor.

Guidance on how to set risk appetite can be found in section 3.9 of the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document.

[1] The term 'residual risk' implies that some countermeasures are in place, so that inherent risks may be mitigated in part or in full.

# Appendix A – Information Risk Appetite Assessment Table.

The following table was used to assess the National Information Risk Appetite following the process in Appendix C of the ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance document. The organisation's attitude to the different categories of risk was assessed, in the political and operational context. The pervasiveness of the risk through the organisation was also assessed. The **Risk Appetite** column uses the Categories of Risk Appetite definitions. The **Overall Appetite** is a simple aggregation of the Risk Appetite Column and could be considered the Information Risk Appetite for the whole organisation.

| Category | Sub-Category | Risk Appetite* | Justification | How Pervasive is this Risk in the business? |
|---|---|---|---|---|
| **Police Service Operations, covering: Public Order, Public Safety and Law Enforcement (Taken from HMG IS 1 (Part 1) Appendix A – Business Impact Level Table A2)** | **Impact on Life and Safety –** Protection of life and property: is there a risk to the life and property of individual/individuals? | **MINIMALIST** | The police are there to protect the lives of the public and any injury or loss of life or loss of or damage to property as a result of police actions or inactions would attract criticism. Therefore there is a low appetite for risks to safety of the public, and indeed to police officers and criminals. | Unique to certain operations |
| | **Impact on provision of Emergency Services –** Disruption to the emergency services | **CAUTIOUS** | The emergency service is a core service of the police and is subject to a level of expectation by the public. Disruption to emergency services, particularly as a result of failures by the police itself, would be severe enough to attract criticism. | Unique to certain operations |
| | **Impact on fighting Crime** – Hindrance to the ability to fight (prevent and detect) crime:<br>e.g. If critical data to an investigation is lost, either in real time or in slow time<br>e.g. if forensic data is modified rendering it uncertain or useless<br>e.g. if operational data is disclosed giving advance warning to criminals | **CAUTIOUS** | Breach or compromise of operations is to be avoided, particularly when time and effort has been invested in the operation. Tactical risks to operations may be weighed up with strategic benefits. | Pervasive |
| | **Impact on Judicial Proceedings –** Compromise of judicial proceedings<br>e.g. if evidence was tampered with<br>e.g. if evidence is lost<br>e.g. if evidence is disclosed at the wrong time | **MINIMALIST** | By the time judicial proceedings are launched there is a known suspect in mind and therefore failure to prosecute successfully could represent a failure of police, both to police staff and to the public. Hindrance or failure of judicial proceedings, resulting from a security breach by police, is to be avoided. | Pervasive |
| **Damage to police/ agency reputation and credibility** | | **CAUTIOUS** | Police is high profile in the national media and in the public eye. Mistakes and information security breaches could result in high profile scandals and criticisms, which damages the relationship with the public and with government, and effectively increases the scrutiny and potentially the bureaucracy of police work. | Pervasive |

| Category | Sub-Category | Risk Appetite* | Justification | How Pervasive is this Risk in the business? |
|---|---|---|---|---|
| **Undermined confidence in the government** | | **MINIMALIST** | As the police are seen as a high profile arm of national government, mistakes and breaches by police have the ability to undermine the government of the day, as government is essentially accountable. This is a similar, but heightened effect to that described above, in terms of the scrutiny and bureaucracy that it would attract. | Unique to certain operations |
| **Financial losses and penalties** | | **CAUTIOUS** | Budgets are tight and Value for money is required by the public. Financial losses could cause embarrassment as well as put other parts of the police service under strain. Well-informed risks can be taken but financial losses are to be minimised. | Unique to certain operations |
| **Legal and Compliance Obligations** | | **CAUTIOUS/ OPEN** | It is important for the police to maintain its compliance and legal standing to avoid criticism and to ensure that the effects of any mistakes can be minimised. A business or operational benefit may justify the breach in compliance, but it should be justified. | Pervasive |
| **Loss of private or personal data** | | **CAUTIOUS** | Loss of private data could place individuals at risk and therefore create more work to protect them after a breach. Police keep information about individuals who may be targeted for violence or persecution. Should an individual be harmed as a result of such a breach, then this would attract criticism. Furthermore this is politically sensitive and there is increased scrutiny on such breaches. | Pervasive |
| **OVERALL RISK APPETITE** | | **CAUTIOUS** | | |

***Categories of Risk Appetite**

The descriptions of the behaviours are as follows:

- **Averse (Risk Avoidance)**: Avoidance of risk and uncertainty is a key objective. Exceptional circumstances are required for any acceptance of risk.
- **Minimalist**: Preference for ultra safe options that have a low degree of inherent risk and only have a potential for limited business benefit.
- **Cautious**: Preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit.
- **Open**: Willing to consider all options and choose the one that is most likely to result in successful delivery minimizing residual risk as far as possible, while also providing an acceptable level of business benefit.
- **Hungry (High Risk, High Reward):** Eager to realise business benefits and to choose options to achieve this despite greater residual risk.

# Appendix B – **Information Risk Appetite National Systems Delegation Matrix**

| Residual Risk level | Risk appetite | | | | |
|---|---|---|---|---|---|
| | **Averse** | **Minimalist** | **Cautious** | **Open** | **Hungry** |
| **Very Low** | National SIRO | National IAO/Force SIRO | National/Force* Accreditor | National/Force* Accreditor | National/Force* Accreditor |
| **Low** | National SIRO | National SIRO | National IAO/Force* SIRO | National/Force* Accreditor | National/Force* Accreditor |
| **Medium** | National SIRO | National SIRO | National SIRO | National IAO/Force* SIRO | National/Force* Accreditor |
| **Medium-High** | National SIRO | National SIRO | National SIRO | National SIRO | National IAO/Force* SIRO |
| **High** | National SIRO | National SIRO | National SIRO | National SIRO | National SIRO |
| **Very High** | National SIRO | National SIRO | National SIRO | National SIRO | National SIRO |

* Where force is mentioned it includes agencies who are signatories to the ACPO/ACPOS Community Security Policy.

This delegation matrix is to be used where residual risks are in relation to National Information Systems.

This illustrates that:

1. A force/agency Accreditor can accept residual risks relating to National Information Systems that are Very Low, but must escalate to the force/agency SIRO any residual risks at Low. Residual risks at Medium or above cannot be accepted by the Force SIRO, but must be escalated to the National SIRO. (The National SIRO may delegate the handling of the risk to the National IAO) while retaining accountability for it.

2. A National Accreditor can accept residual risks relating to National Information Systems that are Very Low, but must escalate to the National System IAO any residual risks at Low. Residual risks at Medium or above cannot be accepted by the National System IAO, but must be escalated to the National SIRO. (The National SIRO may delegate the handling of the risk to the National IAO) while retaining accountability for it.