Information assurance

This page is from APP, the official source of professional practice for policing.

First published 25 March 2015 Updated 16 June 2020
Written by College of Policing
15 mins read

Some links are only available to authorised users who are logged on to College Learn. For further information contact **information.assurance@homeoffice.pnn.police.uk**.

The Candidate Control Set for Services (CCSS) can only be accessed by contacting **information.assurance@homeoffice.pnn.police.uk** directly.

Policing is an information-led activity, and information assurance (IA) is fundamental to how the police service manages many of the challenges faced in policing today. It is vital for maintaining public confidence and for the efficient, effective, safe and secure conduct of operations and services. Without robust IA governance and processes, there is a significant risk of compromise, potentially leading to the facilitation of crime, public safety issues, hindrance to investigations, financial loss, damage to organisational reputation and, consequently, a reduction in confidence from the public and partners.

IA provides the mechanism by which the police service identifies risk and satisfies itself, the public and partners that security arrangements are fit for purpose and that identified risks are managed effectively, collectively and proportionately. It underpins all areas of policing in support of the strategic policing requirement and other statutory responsibilities, for example the **Data Protection Act 2018** and the General Data Protection Regulation (GDPR).

Introduction

This authorised professional practice (APP) applies to police information whether it is locally owned or part of a national system, for which chief officers are joint data controllers. A data controller is a person (either alone or jointly, with other persons) who determines the purpose for which and the manner in which any personal data is, or is to be, processed.

Access to police systems, both local and national, is limited to police-vetted individuals. This approach is essential to meet legislative requirements, support operational policing, ensure successful prosecution, and protect the health and safety of police officers, staff and members of the public.

It is recognised that, in the best interests of public protection, the police must share information with many different partners, and indeed are encouraged to do so under the ‘dare to share’ principle. However, this is done with great care, limiting the amount shared considering the need to know, and most information is kept within the closed community.

A national police information system is:

- one that is provided for the police community as a whole and managed centrally
- used by at least 10 forces
- when the Home Office has a contractual relationship with the service provider and/or the service management of the system

National systems include those delivered:

- by or on behalf of the Home Office, such as the Police National Database, the Police National Computer, the Violent Offender and Sex Offender Register, and the national identification system (IDENT1)
- by other law enforcement agencies or through distributed components operated by forces, such as HOLMES
- to provide interconnectivity between law enforcement and other agencies, for example, through the Criminal Justice Extranet or Public Services Network
- to facilitate law enforcement agencies’ information sharing with external communities and connectivity, such as Criminal Justice Secure Mail

Each national system must be accredited in accordance with the **National Policing Information Risk Assurance Policy** and have an assigned national information risk assurer. Risk assurance ensures that risks are known, understood and managed in accordance with the risk appetite.

IA provides the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. The approach aims to:

- provide and promote IA advice to all police personnel
- embed IA culture as a core business process/activity in the police service at national and local levels, and which aligns across force/agency boundaries
- be clear on ownership and management of IA
- clearly define the information risk management framework and processes, so that individuals have a common understanding of the identification, assessment and treatment of risks
- develop IA standards and procedures so that they remain current and relevant to policing objectives and approaches

Governance

Governance is provided by:

- the national senior information risk owner (NSIRO) – the national policing lead for the Information Management Portfolio
- the Police Information Assurance Board (PIAB)
- national information asset owners (IAO)
- national information risk assurers

Structures at national level are governed by the following policies:

- national policing Community Security Policy (CSP) – this document can be accessed by contacting **information.assurance@homeoffice.pnn.police.uk**
- **National Policing Information Risk Assurance Policy**

Information risk management structure

The governance structure for IA includes forces, national systems, national policing, government departments and delivery partners. Force/agency senior information risk owners (SIROs) are responsible for information risk within their organisation and the NSIRO is responsible for information risk associated with the national capability.

Information risk management is owned by the NSIRO on behalf of the National Police Chiefs' Council (NPCC) and forms part of the SIRO's overall responsibility in the governance of risk.

Functions and responsibilities

National senior information risk owner

The NSIRO ensures that information risk ownership for national systems is formally retained by IAOs. The NSIRO:

- has responsibility for ensuring all national information systems are appropriately risk assessed and identified risks are managed in accordance with the **National Policing Information Risk Assurance Policy**
- ensures that a framework is in place to monitor and manage aggregated risks
- considers information risk escalation cases (REC) relating to national police information systems
- sets and endorses the national policing risk appetite statement
- represents Chief Constables' Council for all matters in relation to IA and is the final arbiter for all related matters

Senior information risk owner

The term SIRO is only used for the single individual within each organisation or collaborating organisation who has ownership of the corporate or collective information risks.

Each force/agency must have a SIRO. They are responsible for determining and setting their force risk appetite for their information assets that are not contained within or connected to national systems. SIROs must be aware of the need to act as a community of interest and of the need to manage risk collectively, considering the wider impact of any local decisions on national information, consulting the NSIRO when appropriate.

The SIRO:

- should ensure the information risk appetite is recorded and incorporated in the risk management processes, and communicated to their organisation
- is the final decision maker for accepting risks outside the level of acceptance, unless related to national information systems
- reviews annually and submits the police **Governance and Information Risk Return (GIRR)** and Candidate Control Set for Services (CCSS) and supporting documents to the National Policing Information Risk Management Team (NPIRMT)
- prepares and submits the protective security and risk management overview
- ensures that local governance meets the requirements of the **CSP**
- manages and implements national standards at a local level

For further information, see the **SIROs handbook**.

National Policing Information Risk Management Team

The NPIRMT provides a range of IA functions to the police community. This includes:

- maintaining the strategic national approach to IA (currently under review), associated policy and guidance
- supporting the chief constables in their role as joint data controllers under the GDPR as written into the Data Protection Act 2018
- ensuring that risks to police information held on national systems are managed through an accreditation framework and meet the expectations of the NSIRO
- ensuring that the security of connections (police service and non–police) to national information systems meets the national information risk appetite
- providing a central resource for all police security incident reporting, and investigating incidents relating to national systems
- auditing compliance with police service IA standards and policies of third-party suppliers and delivery partners to national policing
- approving supplier/service providers facilities to handle/process policing data

Police Information Assurance Board

The PIAB provides the strategic lead on the development, implementation and evaluation of IA within national policing. It is the authority under which the assessment and improvement of IA is undertaken and is custodian of the CSP on behalf of the community (CSP community of forces and agencies). It supports the framework for sharing information and promotes good practice in data management by forces/agencies and the wider community.

It is responsible for:

- acting as the information risk management governing body for all national policing systems and the accreditation process that governs the management and connection to them
- providing support to the police community on the use of new and existing information and communications technology (ICT) and data sharing, without compromising its IA responsibilities
- promoting a culture of responsible and compliant data sharing to ensure public safety and enhance operational effectiveness (jointly with the information sharing portfolio)

- considering and approving changes and developments to the IA strategic approach and national policing IA policies, guidance and procedures
- proposing the National Policing Risk Appetite Statement
- providing the authority for, and overseeing the delivery of, the police **GIRR** and CCSS
- reviewing data loss and security incidents and providing guidance to reduce the impact of incidents

Information asset owner

The term IAO is used for the corresponding function at project, programme or organisational unit level.

The NSIRO nominates an IAO for each national system, and force SIROs nominate an IAO for each local force system. The IAOs are accountable for the confidentiality, integrity and availability of their information asset, and are responsible for identifying and managing risk.

The IAO:

- identifies and assesses the information risks and decides whether they are acceptable, raising a REC when appropriate
- monitors and reports on risks allocated to them on an ongoing basis
- accepts information risks on behalf of the SIRO within agreed parameters
- is responsible for ensuring that the information systems assigned to them have up to date accreditation

Information security officer

The information security officer (ISO) is responsible for the development and implementation of information security policies and procedures within their force/agency in accordance with:

- the **Cabinet Office Security Policy Framework**
- Her Majesty's Government technical security standards, produced by the National Cyber Security Centre (the national technical authority for IA), and obtained via the NPIRMT
- the business needs of their force/agency

Additional responsibilities include:

- assuring and accrediting local information systems

- providing information security advice to the SIRO and the wider organisation
- providing an incident reporting service on behalf of the force
- facilitating information security awareness, education and training

The role of the ISO and the local information risk assurer may be combined. Should this occur, the impartiality of the information risk assurer function must be maintained.

For further information see:

- **IAO Handbook**
- **National Policing Information Risk Assurance Policy**

Information risk assurer

The information risk assurer acts as an impartial assessor of the risks to information systems. Their function is to ensure that systems are sufficiently secure to be placed into, and continue to function in, operational service. They accredit systems on behalf of the SIRO.

Within the police community, there are national information risk assurers and force information risk assurers.

National information risk assurers:

- review the level of residual risk of national police systems
- administer the CCSS for national police systems
- approve force connections to national services to ensure that they meet national standards for connectivity

Force information risk assurers:

- review the level of residual risk within a force
- accredit the local force network and request approval from a national information risk assurer for connection to national systems and networks
- may accredit regional or shared systems which do not qualify as national systems

The role of the information risk assurer and the ISO may be combined. Should this occur, the impartiality of the information risk assurer function must be maintained.

National policing Community Security Policy

For further information, see the community Security Policy – this document can be accessed by contacting **information.assurance@homeoffice.pnn.police.uk**.

is embodied in the national policing CSP. The CSP provides appropriate and consistent protection for the information assets of member organisations, whether national, collaborative or local assets. The Information Management and Operational Requirements Coordination Committee and PIAB have ownership of the national policing CSP.

Aims of the community security policy

The aims of the CSP are to:

- ensure compliance with statutory requirements and meet the expectations of the police service to manage information securely
- assure the Cabinet Office that police service elements of the critical national infrastructure and police service connections to government networks and services are appropriately protected

Community security policy compliance

Forces and organisations are required to show compliance with the CSP. Compliance provides assurance that risks to shared information are managed to a level acceptable to the whole community.

The NPIRMT monitors and reviews national policing CSP requirements. Compliance is provided through:

- submission of annual **GIRR** or CCSS returns
- evidence from force/system Risk Managed Accreditation Document Set (RMADS)/ Information Risk Assessment Report (IRAR) to support the **GIRR**/CCSS
- submission of the annual protective security risk management overview
- independent audits

For further information, see organisations that are **members of the CSP**.

Governance and Information Risk Return

Forces/agencies are required annually to provide a completed **GIRR** to the NPIRMT. These control set questions aligned with ISO 27001 are approved by the PIAB. The NPIRMT reviews and collates the force/agency returns and presents them to the PIAB on a rolling basis.

Compliance with the **GIRR** provides a level of assurance to the police community that information shared between connected organisations, and accessed on national networks and systems, will be appropriately protected and no additional risks will be introduced into the wider policing community.

Organisations connecting to national police information systems must seek approval from the national information risk assurer for the police service on an annual basis, providing evidence of compliance with the **GIRR**. Significant changes to ICT infrastructure should be notified in the form of an updated **GIRR** at the time of change. This is in the form of a template developed by the NPIRMT.

For further information, see **Governance and Information Risk Return**.

Cyber risk assurance of national systems

National policing has mandated the cyber risk assurance of police ICT services to manage risks to police information held in national information systems. This service for national information systems is provided by NPIRMT on behalf of the police service. National information systems require a CCSS to be completed annually, or when there is a significant change to a system.

For further information see:

- **Information Risk Assurance Policy**
- **Guidance for Achieving Accreditation for new ICT Projects**
- **Guidance for maintaining accreditation of national information systems**
- Candidate Control Set for Services

Management of information risk

Risk appetite

The SIRO must establish the risk appetite statement for the information assets under their control. This enables IAOs and cyber risk assurers to make effective risk management decisions and

defines the extent to which risks must be mitigated or escalated.

Insufficient guidance on legitimate, acceptable levels of risk may develop an overly cautious (risk-averse) culture, which results in a failure to seize important opportunities that maximise performance. Conversely, excessive risk may be accepted without regard to the potential impact. The alignment of risk exposure to risk appetite maximises business performance, through taking acceptable risks when developing and delivering services.

An information risk assurer or an IAO can only deviate from the risk appetite with the authority of the SIRO following an information REC. In relation to national systems or nationally connected systems, this authority needs to come from the NSIRO.

The level of risk appetite and, therefore, the severity of subsequent risk controls will vary for different information asset types. National policing has categorised its information assets as:

- police marketing and communications
- personal data
- public/citizen
- commercial/procurement/supplier
- police corporate information
- sensitive personal data
- national security commercial/procurement/supplier
- personal data – staff in sensitive posts
- national security corporate information
- covert intelligence
- counter terrorism

The national police information risk appetite applies to all national police information systems. It also applies to force/agency systems which are connected directly or indirectly to national police information systems.

For further information see:

- **HM Treasury ? Thinking about risk, managing your risk appetite: A practitioner’s guide**
- **HM Treasury ? Thinking about your risk, Setting and communicating your risk appetite**
- **National Information Risk Appetite Statement**

- national policing information risk appetite and **risk escalation** policies
- national policing information threat model (available from the NPIRMT on request)

Residual risk

Residual risk is the level of risk perceived to exist after security controls have been implemented to reduce the risk initially identified in the risk assessment. Residual risk is minimised through counter measures.

Risk escalation case

A REC escalates information risks that are deemed to be outside the level of acceptance by certain personnel involved in information risk management in an organisation. These information risks are escalated to the SIRO, who will decide on how to manage the notified information risk. The NPIRMT will manage cases where it is necessary for a REC to be raised for national information systems or nationally connected systems.

Detailed information on how to create a REC and the approval and consideration can be found in the **National Information Risk Appetite Statement** and national policing information risk appetite and risk escalation case guidance.

For further information see:

- **National Policing Information Risk Escalation Policy**
- Risk Escalation Case Template

Information security incidents – reporting and monitoring

Forces/agencies are required under the national policing CSP to provide the NPIRMT with quarterly statistical information on slow-time security incidents and to report fast-time incidents.

The slow-time quarterly reports are used to monitor and report on current threats/incidents faced by the policing community. The information is incorporated into the national policing information threat model. It includes the frequency, future likelihood of occurrence and any specific impacts this would

have on national policing.

The Police Warning, Advice and Reporting Point (PolWARP) procedure requires forces/agencies to report fast-time security incidents to the NPIRMT that may affect other members of the policing community. Appropriate action can then be taken to prevent widespread confidentiality, integrity or availability issues occurring. This information is also used to monitor and report on current threats to the police service and feeds into the national policing information threat model (available from the NPIRMT on request).

In order for forces/agencies to support this process, they are required to have their own local security incident procedures.

Police Warning, Advice and Reporting Point

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. PolWARP is supported by the Centre for the Protection of National Infrastructure and has been widely adopted by other government departments and local authorities throughout the country.

A security incident can also be described as any suspected failure in information security, namely:

- accidental or deliberate unauthorised destruction of information
- accidental or deliberate unauthorised modification of information
- accidental or deliberate unauthorised disclosure of information
- deliberate and unauthorised unavailability of the system
- unauthorised access to the system
- misuse of data and theft of assets containing information
- any contravention of the information security policy or security operating procedures
- any other event which affects security of information

Forces/agencies are expected to have their own local security incident procedures that include deciding whether the incident is likely to have immediate or serious repercussions for the rest of the community.

Where they assess the incident as having only local impact, it should be dealt with following their local procedures, and then reported to **PolWARP** as part of the regular return of security incidents.

Forces are required to:

- set up a PolWARP mailbox (**PolWARP@force.pnn.police.uk**)
- ensure adequate monitoring of the PolWARP facility
- have procedures in place to respond to any event.

For further information, see **Home Office (2013) Police Warning, Advice and Reporting Point (PolWARP) Procedures version 1.7** (available to **authorised users** logged on to College Learn).

Tags

Information management