Senior Information Risk Owners

Handbook

2018

NPCC National Police Chiefs' Council

Authorised by the Police Information Assurance Board

Foreword

Information is the lifeblood of policing and the way in which we handle information directly impacts upon our ability to effectively tackle crime and disorder and ultimately, it impacts upon our legitimacy with the public. Information or data is fundamental to every facet of policing activity, from criminal intelligence supporting pro-active operations, crime data supporting patrol strategy, information gathered in support of a reactive investigation, personal information shared with partners to safeguard the vulnerable all the way through to information that ensures our people are paid on time. There is no one activity that we execute that does not require data.

Our data and information is often sensitive personal data which can take many forms, from written documents in hard copy, photographic and biometric material through to data created and stored virtually. In whatever form it takes, as guardians of this data we must ensure that we make full use of it to protect and serve the public whilst also being able to provide assurance that it is sufficiently respected and protected and only deployed in accordance with the legislation that applies as well as the broader principles that underpin it.

In our policing family, defined roles have been set to ensure that this oversight and accountability is in place, to support Chief Constables and these are led by the Senior Information Risk Officer (SIRO). The role of SIRO is critical in risk management within a complex, challenging environment with issues ranging from the technical to the legislative.

I am delighted to introduce to both new and existing SIROs this handbook, which provides to you a consistent framework to consider in ensuring your Forces have the appropriate assurance structures, effectively trained staff and the fundamental considerations that should be addressed.

Nick Ephgrave QPM
Chief Constable
Surrey Police

Introduction

Information has never been more important to the essential working of policing. As the quantity, diversity and nature of police information changes, so will the threats and vulnerabilities it faces. The rise in cybercrime continues at pace and public sector bodies have already been seen to suffer at the hands of ransomware.

The role of the Senior Information Risk Owner (SIRO) was created to provide executive -level accountability and greater assurance that information risks are addressed. The SIRO ensures that information risks are treated as a priority for business outcomes. The SIRO also plays a vital role in getting their force to recognise the value of its information enabling them to use it effectively. By treating information as a business priority and not as an ICT or technical issue, we can ensure that risks are addressed, managed and capitalised upon. This in turn leads to improved decision making and policy development.

The community of police SIROs can create an outcome-focused and holistic strategy for managing and shaping the way policing uses its essential information.

As SIRO, you manage information risk from a business not a technical perspective. You focus on the strategic information risks related to the delivery of corporate objectives. This means you take a holistic approach to information risk across the supply chain and manage it in line with the force's risk appetite. It is important to remember that force's information management responsibilities extend further than digital data, covering building security, personnel (training and development) and paper records too.

In policing the SIRO is most usually the Deputy Chief Constable. Overall accountability rests with the Accounting Officer – the Chief Constable - but the SIRO is the delegated lead.

SIRO's Key Duties

The key responsibilities of a SIRO are to -

- Establish an information risk strategy which allows assets to be exploited and risks to be managed effectively;
- Identify business-critical information assets and set objectives, priorities and plans to maximise the use of information as a business asset;
- Establish and maintain an appropriate risk appetite with proportionate risk boundaries and tolerances;
- Establish an effective Information governance framework;
- Act as the champion for information risk within your force, being an exemplar for all staff and encouraging the Executive to do likewise;
- Build networks with peers and organisations that can provide essential support and knowledge exchange services;
- Ensure compliance with regulatory, statutory and force information security policies and standards;
- Ensure all staff are aware of the necessity for information assurance and of the risks affecting the force's corporate information; and
- Establish a reporting and learning culture to allow the force to understand where problems exist and develop strategies (policies, procedures and awareness campaigns) to prevent problems occurring in the future.

SIRO as the Strategic Lead for Information Assets

As the strategic lead the SIRO's role is to ensure information assets and risks within the force are managed as a business process rather than as a technical issue.

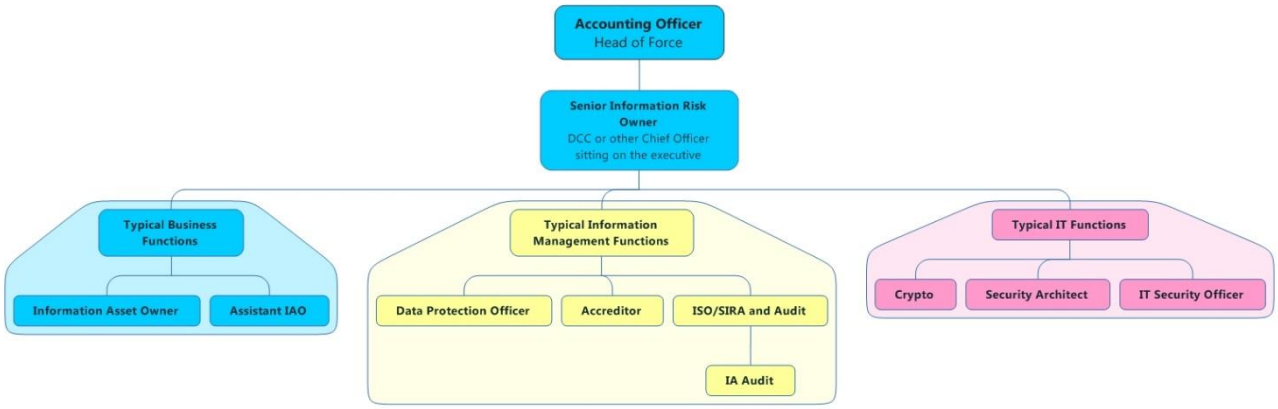
The force executive must consider all key risks associated with their business. The SIRO will ensure information risks which affect business objectives are highlighted to the chief officer group and addressed. They will also discuss the actions taken to develop the force's approach to its information assets, the outcomes and any lessons learned.

The SIRO is responsible for ensuring the Executive recognises the importance of information assets in delivering corporate objectives.

The SIRO role is an integral part of any force's information governance framework and so it is important for the SIRO to set up and/or maintain a strong information governance structure appropriate to their force.

In addition this role also has responsibility for understanding the risks associated with the management of police information. In particular, the quality and accuracy of data, the proportionality of retention and the ability for a force to comply with legislation and guidance.

Other Information Assurance Roles



As SIRO you will have a number of people in force to support you. Depending on the size of the force some people may be performing more than one of these roles.

- Information Asset Owner(s) (IAO). Each separate information asset (often but not always a computer system) should have a designated IAO. This is a senior role commonly at Chief Superintendent or equivalent position. So the C/S lead

for CJ would typically be the IAO for the force's case and custody system. The IAOs are empowered to take some risk decisions within their own portfolio and within their risk tolerance.

- Head of Information Management. Some forces have a senior leader heading an information management department. This department would normally include Data Protection, Civil Disclosure, DBS, Records Management as well as Information Security & Assurance.

- Force Accreditor – this person will lead on most of the Information Assurance work on your behalf. This is a relatively senior role, one that has a degree of delegated decision making within it. This person is responsible for the relationship between the force and the Home Office's national police information risk management team (NPIRMT). Where a force has a Head of IM – this role would often be combined into that.

- Information Security Officer (ISO) or Security & Information Risk Advisor (SIRA). This is the role that does most of the hands on assurance work within the force. It is important that this role is independent of IT. The person needs to have an understanding of IT matters but does not need to be an expert IT professional. As part of their assurance duties they should carry out audits of systems and physical controls.

- IT Security Officer (ITSO), not to be confused with the ISO. This role sits within IT and has responsibility for ensuring that the necessary technical controls are carried out. For example they would be expected to report on patching compliance.

- IT Security Architect. A person responsible for designing secure systems. In some forces these IT security roles may simply form part of a person's duties rather than being a specific post.

- Data Protection Officer (DPO). This post is responsible for the force's compliance with the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). Also known as parts 2 and 3 of the Data Protection Act 2018. It should be a senior position with access to the Executive. The post can be shared between forces or may form part of a person's duties. The post carries a fair degree of responsibility as described –

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

National Information Assurance & Regulatory bodies

There is a national governance framework in place to support forces and SIROs. Key components are:

- There is a national SIRO who will advise local SIROs and also makes some decisions on a national basis.
- The national SIRO chairs the Information Management Operational Requirements Co-ordination Committee (IMORCC) which oversees IA and IT activities at the national level. IMORCC has developed a national information strategy which SIRO's are advised to review.
- Police Information Assurance Board (PIAB) is a sub-group of IMORCC that is chaired by a nominated Chief Constable and meets quarterly. There is space on the board for a SIRO rep from each region (as agreed locally).
- Police Information Assurance Group and Forum (PIAF and PIAG). These are meetings and seminars that the ISO and other IA professionals should attend.
- The Information Commissioner's Office (ICO) is the independent regulatory body dealing with the GDPR & the Data Protection Act 2018, the Freedom of Information Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and the Environmental Information Regulations 2004.
- The National Cyber Security Centre (NCSC) is part of GCHQ and was set up to help protect the UK's critical services from cyber-attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisation.

SIRO's first 90 days

It is recommended that SIROs complete the Managed Learning Environment (MLE) e-learning package: Protecting Information (Level 3). When completing this module, you are required to pass a short assessment in order for it to be recorded as a pass. The MLE e-learning packages (1-hour each) will give you an understanding of why your role is important, the risks you need to consider and who can help you. Below is a summary of the Protecting Information modules available:

Level 2	Recommended for IAOs and Line Managers / Supervisors	Guide to Information Assets, roles and responsibilities of an IAO, information management culture, and processes for protecting information.
Level 3	Strongly recommended for all new IAOs and new SIROs	Guide to the responsibilities of the SIRO, IAO, and other information assurance roles. Also covers risk and threat, protecting assets.

The private company Advent-IM have designed a SIRO course for the police service. In addition the National Archives http://www.nationalarchives.gov.uk/information-management/ provide some free training sessions and other non-police specific material.

Additional advice can be provided by your information security team such as the head of Information Management or your ISO. All SIROs should be up to date with MoPI and Data Protection MLE packages and should encourage their teams to do the same.

When taking on the responsibilities of a SIRO it is recommended that you also –

- Meet the key stakeholders in Information Assurance - the DPO, Accreditor and ISO;
- Ask to see the force's risk appetite. This should be re-signed annually and each time a new SIRO is appointed;
- Read the national Information Management Strategy, available on Polka; and
- Review the IA governance structure. As a minimum the SIRO should chair a quarterly Information Board. A basic draft agenda is shown below.

Draft Agenda

- Minutes, introductions etc.
- Security/Breach incidents of note;
- Legal/Home Office compliance – FOI, DP and PNC statistics
- Status of annual accreditation process;
- Papers for decision – e.g. agreement of a new password policy
- IAO Updates as appropriate.

Risk Management

A key risk control tool is the Information Asset Register; this details the attributes and the asset's associated value. The value of an asset can be expressed in terms of monetary value, its role in supporting business objectives, its value to a potential attacker and the potential impact on the business if the asset were compromised or not available.

To address risks within the force the SIRO must ensure that:

- There are appropriate policies and procedures in place and mechanisms for monitoring and measuring compliance with them;
- The assets have assigned owners and assessed value which are documented in an asset register;
- Accuracy of the asset register is checked and maintained on a regular basis;
- Risk assessments are conducted in the context of the business which provides a clear, prioritised register of the risks; and
- All necessary information is used to apply the most proportionate, appropriate and cost-effective risk control measures.

Ultimately the SIRO is accountable for the residual risks to information assets, therefore it is essential that they understand the force's approach to risk management and, crucially, that they understand the outcomes of risk assessment activity and can set these within the context of the force's agreed risk appetite.

Availability of information

A key consideration for every force should be whether the right information is available to the right people, at the right time. For many forces, lack of availability is a key risk.

This is crucial to ensuring it can be used to meet business aims including meeting legal, regulatory and audit outcomes. This is about having the right systems, policies and

processes in place alongside a culture that recognises the benefits of good information management.

Integrity of Information

Through effective training and awareness building activities the integrity of information assets can be ensured. The SIRO's actions in creating a culture where training is provided, development encouraged and mistakes addressed is paramount to ensuring data is input, altered, maintained and removed from information assets in a correct manner.

Incident Management

Despite having taken steps to reduce risks security incidents will happen and they will vary in severity and impact. All data breaches should be recorded and serious breaches which are likely to result in a high risk of adversely affecting individuals' rights must be reported to the ICO within 72 hours. It is essential that the DPO is consulted on all data breaches. There is also a requirement to notify other bodies such as NPIRMT and the IOPC. The SIRO needs to support the formation of an effective incident management capability to limit the business impact from incidents and to prevent them from re-occurring.

The SIRO should empower the incident management staff to make decisions regarding the investigation and resolution of incidents. The SIRO should also ensure that the Executive provides the funding for their specialist training.

Periodically, the SIRO should run tests and scenarios to provide assurance to the executive on the force's ability to respond to incident. The SIRO should also review security incident statistics to identify consistent weaknesses and, if necessary, sponsor remedial action, such as a review of security policies and procedures or the creation of security education initiatives.

Procurement

Forces should have a joined-up process for the procurement of new systems and services. This process should include Information Management and ICT professionals working to establish the business, privacy and security requirements

To avoid unnecessary procurement a force needs to have a developed understanding of the information assets it holds, how they need to be used and how this is currently supported by ICT systems. An up to date and easily understandable Information Asset Register is a key tool in preventing these issues. The SIRO is responsible for ensuring the risk to information held by suppliers and 3rd parties is managed effectively. As part of the Security Policy Framework the Cabinet Office have produced a Supplier Assurance Framework which can assist in this process.
https://www.gov.uk/government/publications/government-supplier-assurance-framework

Information risk management checklist

The following checklist is not exhaustive and should only be treated as a guide for the reader to question themselves and their force.

Governance Checklist:	
1	I have governance processes and a framework in place to help me understand all important information assets, their value and their importance to the business and what the impact of their loss would be.
2	I have assigned appropriate roles and responsibilities within my information governance framework. The escalation path for decision-making is clearly defined, and appropriate personnel are empowered to make decisions on my behalf.
3	I have implemented appropriate and proportionate security controls as necessary to reduce risks to an acceptable level.
4	I have agreed the risk boundaries/tolerances with the Executive and keep them up to date with evolving threats.
5	I ensure that threats, vulnerabilities and risks to my force are regularly reassessed and re-evaluated.
Culture Checklist	
6	I am proactive and lead by example.
7	Staff are aware of their roles and responsibilities.
8	Staff receive regular training on current threats and risks and are aware of the steps to take to mitigate these.
9	The force has a culture where staff are aware of the consequences and impacts of information losses, data breaches or attacks and report them proactively.
10	The force has a culture where staff are aware of the risks to our information assets and proactively take steps to mitigate new risks as they arise.

Reference Links

College of Policing: Approved Professional Practice
https://www.app.college.police.uk/app-content/information-management/data-protection/audit/

Managing Information
Operational - https://www.mle.ncalt.pnn.police.uk/Course/Details/31147
Non-operational - https://www.mle.ncalt.pnn.police.uk/Course/Details/31146

Data Protection – Foundation
https://www.mle.ncalt.pnn.police.uk/Course/Details/21516

Data Protection Intermediate and Advanced delivered by NPCC.
Contact; National Police Freedom of Information and Data Protection Unit (NPFDU)
Introduction to Government Security Classification (GSC)
https://www.mle.ncalt.pnn.police.uk/Course/Details/23891

Freedom of Information
https://www.mle.ncalt.pnn.police.uk/Course/Details/21517

NCALT: Protecting Information 2
https://www.mle.ncalt.com/Course/Details/11060

NCALT: Protecting Information 3
https://www.mle.ncalt.com/Course/Details/11061

The Information Commissioner's Office (ICO)
https://ico.org.uk/

The National Cyber Security Centre
https://www.ncsc.gov.uk/