Information Asset Owners

Handbook

2018

NPCC National Police Chiefs' Council

Authorised by the Police Information Assurance Board

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 targeted by ransomware.

The role of the Information Asset Owner (IAO) was created to provide a senior role responsible for ensuring specific information assets are handled and managed appropriately. An IAO is appointed by and reports to, the Senior Information Risk Owner (SIRO).

This handbook seeks to outline the overarching IAO requirements in relation to better understanding their role and remit.

The IAO will, on behalf of their relevant SIRO and their end users, be able to understand and address risks to the information and ensure it is fully used within the law.[1]

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 level. The IAO will support their relevant SIRO to ensure that information risks are treated as a priority for business outcomes and that information is utilised in the most effective way. 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.

[1] HMG Cabinet Office Security Policy Framework (HMG SPF)

The IAO role is an integral part of any information governance framework and so it is important for the IAO to support their relevant SIRO to set up and/or maintain a strong information governance structure appropriate to their operating environment.

As IAO, you manage information risk from a business not a technical perspective. It is important to remember that information management responsibilities extend further than digital data, but also includes building security, personnel (training and development) and paper records too. IAO are empowered to take some risk decisions within their own portfolio and within their risk tolerance.

Promoting security, policy and process

There is an expectation that the Data Controller, SIRO, IAO and all staff within their environment(s) are familiar with the requirements of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) as incorporated within the Data Protection Act 2018. This included familiarity and absolute compliance with the principles of data protection. The primary compliance responsibility falls to the relevant Data Controller (i.e. the Chief Constable or Chief Officer of an organisation) and their operational users when using IT systems and applications to process data held.

The IAO is expected to coordinate and support the active promotion of compliance with this and other relevant legislation / policy within their business area.

Where there is any type of suspected breach the IAO should ensure that any such incident is followed by a credible investigation to establish the facts.

In relation to Data breaches the IAO should consult with their relevant nominated Data Protection Officer (DPO) and relevant SIRO ASAP.

In relation to a security breaches the IAO should consult with their relevant Departmental Security officer (DSO) and relevant SIRO ASAP.

What is an Information Asset?

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected an exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles[1].

For example, a body of information held by a defined business area could be individual police forces or units within these. Assets include; information submitted to national databases; information available from other databases/application.

Information assets may contain personal or sensitive personal data [as defined by the General Data Protection Regulation Act (GDPR) and Law Enforcement Directive (LED)] or non-personal information that is critical to business. Existing force/organisation Data Controllers remain responsible for compliance with the GDPR / LED.

It should be noted that assets are not defined as specific templates, forms or report types, but refers to the actual information content. These formats are merely ways of recording a sharing information that may form part of the information assets subject to content, context and purpose.

Information Asset Risks to be managed

There are inherent risks to information assets on any database or IT system where user communities are drawn from different organisations, forces or units.

Overall an IAO will need to ensure:

- Confidentiality and protection of information is maintained to prevent inappropriate access to, or disclosure of, protectively marked or personal data directly or indirectly by unauthorised personnel (whether deliberate or accidental)

- Integrity of information is maintained to ensure accuracy and that any modification, use or change is legitimate

- Availability of information is managed to prevent intelligence failure and is considered for weeding/removal when no longer relevant

- Activity of staff acting in error or deliberately (the "Insider threat") is minimised, mitigated or prevented

- Information loss internally and externally is minimised and prevented, particularly during transfer or movement of information, or as a result of business change.

Consideration to better understanding Information Asset risks

The following generic questions[2] should be considered by IAO to assist to identify and manage information risk;

[2] Taken from the HMG SPF

What and why information is held?

It would be unrealistic to expect that an IAO will know each and every information or intelligence report retained. However, it is key expectation of the SIRO that an IAO can reasonably be expected to vouch that every operational unit and user within their area of responsibility understands their operational role and remit. IAO should challenge their business areas where this understanding is not apparent.

The role of the IAO includes ensuring the information in their charge is properly protected and its value to the organisation fully realised.

The IAO should be a suitably enabled senior member of staff with the position to influence operational decision making, the progression of information in support of the same and the behaviour of their staff when handling information and assets.

Some IAO responsibilities require IAO to take direct action and some simply to assure action is taken by others on their behalf. As such the IAO must be familiar with their component operational units across their related business areas they have responsibility for.

What information is added and what is removed?

The IAO should ensure that clarified and agreed working practices are in place stipulating the information flows and ensuring these can be supported by the relevant IT functionality.

Consideration should be given to how information is removed by users electronically from systems – the use of removable media on an IT platform remains a potential point of information risk. The importation and exportation of data electronically should be clearly defined and controlled.

How is information being managed?

Clarified and agreed working practices should stipulate information flows that are supported by the relevant IT functionality, coupled with staff access permissions being controlled will allow for a high degree of information oversight, insight and resilience. Wherever possible IAO should seek to adopt and incorporate consistent national practices.

Who has access to information?

For the IAO in any business area, standard default accesses limit the potential of overly compartmentalised (hidden) data being retained, enabling local oversight and quality control checks to be conducted.

Consideration should be given to the auditing and accountability of users accessing and amending information.

Why Staff have access?

All users with the remit of the IAO business area, should have access control imposed [to a reasonable extent] to prevent them from performing activities against information for which they do not have an agreed responsibility, or which falls outside of their operational requirements, i.e. the operational role performed is supported by the access allowed within specific IT applications.

Consideration should also be given to users receiving the necessary and suitable training to undertake the required activity.

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, via the SIRO, is consulted on all data breaches. There may also a requirement to notify other bodies such as NPIRMT and the IOPC. The SIRO, assisted by the IAO, 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.

Periodically, the SIRO (or IAO on their behalf) should run tests and scenarios to provide assurance to the executive on the force's ability to respond to incident. The SIRO and IAO 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.

IAO Key Duties

The key responsibilities of an IAO include:

- Assist and inform the SIRO to establish an information risk strategy which allows assets to be exploited and risks to be managed effectively;
- Identify business-critical information assets and assist to set objectives, priorities and plans to maximise the use of information as a business asset;
- Act as the champion for information risk within your business area, being an exemplar for all staff and encouraging other 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;
- Ensure staff utilise information and assets correctly and are appropriately training to do so;
- Maintain 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.
- Ensure information risks that affect business objectives are highlighted to the SIRO and / or chief officer group.
- The IAO 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.
- Chair regular IAO meetings form which risk/issues can be highlighted to the relevant SIRO
- Assist to ensure there are appropriate policies and procedures in place and mechanisms for monitoring and measuring compliance with them

- Ensuring all assets under their remit are assessed and correctly documented in an asset register
- Ensure any risk assessments are conducted in the context of the business which provides a clear, prioritised level of risk to inform the SIRO
- Ensure all necessary information is used to apply the most proportionate, appropriate and cost-effective risk control measures.
- Periodically, run tests and scenarios to provide assurance to the SIRO on the ability to respond to incident.
- Regularly review security incident statistics to identify consistent weaknesses and, if necessary, in conjunction with the SIRO support remedial action.

IAO first 90 days – *things to do*

The role and responsibilities for an IAO may often be new areas therefore the following sections, Appendix A (IAO Checklist) and Appendix B (Other reference points) are provided as guidance.

Role Familiarisation

When taking on the responsibilities of an IAO it is recommended that you;

- Engage with your SIRO
- Liaise with other IAO
- Liaise with your relevant Data Protection Officer (DPO)
- Meet the key people involved in the Information Assurance (IA)
- Confirm 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)
- Review the IA governance structure.
    - Review requirement to hold regular IAO meetings
        - A basic draft agenda should include;
        - Minutes, introductions etc.
        - Security/Breach incidents of note;
        - Legal/Home Office compliance – e.g. FOI, DP and PNC statistics
        - Accreditation issues
        - Risk / Issues
        - Papers for review and recommendations
        - Areas for IAO escalation to SIRO etc.

Training

It is recommended that IAO complete the Managed Learning Environment (MLE) e-learning package: Protecting Information. 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) provide 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 via MLE:

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.

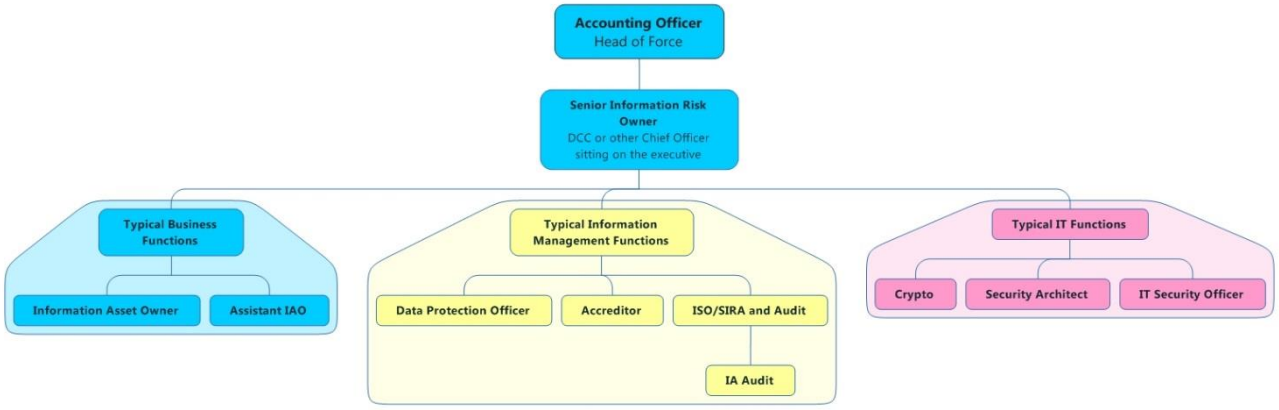
- All IAO should be up to date with MoPI and Data Protection MLE packages and should encourage their staff to also do so
- Additional advice can be provided by your local information security staff such as the head of Information Management or your ISO.

External Training Providers

- The commercial company Advent-IM have designed an IAO course for the police service [other companies also provide similar training].

- 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.

Other Information Assurance Roles



As an IAO there are a number of people/departments to support your role, these include;

- Senior Information Risk Owner(s) (SIRO) - The role of SIRO is a board level member with the responsibility for the accountability and assurance that information risks are suitably addressed. IAO are representatives of their relevant SIRO.

- 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 IT Accreditor – this person will lead on most of the Information Assurance requirements. This is a relatively senior role, one that has a degree of delegated decision making within it.

- 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) - 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 IT 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/

- Departmental Security Officer (DSO) - This post is usually responsible for the security elements and associated force's compliance

National Policing Information Assurance bodies

A national Information Assurance (IA) and Governance framework is in place to support forces, SIRO and IAOs. Key components are:-

- There is a national policing SIRO who will advise police and makes some national strategic decisions on behalf of general policing information assurance aspects.
    - The national police SIRO chairs the Information Management Operational Requirements Co-ordination Committee (IMORCC) that oversees IA and IT activities at a national policing level.
- IMORCC has developed a national information strategy which IAOs are encouraged to review.
- Police Information Assurance Board (PIAB) is a sub-group of IMORCC that is chaired by a nominated Chief Constable and meets quarterly.
    - Member include regional specific SIRO representation.
- Police Information Assurance Group and Forum (PIAG / PIAF).
    - These are meetings and seminars that regional/force IA professionals and feed into PIAB.

External National Information Assurance bodies

- 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 UKIC 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.

Appendix A

-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 SIRO and keep them up to date with evolving threats.
5	I ensure that threats, vulnerabilities and risks to my business area are regularly reassessed and re-evaluated.
6	Do I need to undertake incident testing scenario?
Culture Checklist	
7	I am proactive and lead by example.
8	Staff are aware of their roles and responsibilities.
9	Staff receive regular training on current threats and risks and are aware of the steps to take to mitigate these.
10	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.
11	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.
12	Has staff awareness and training been maintained

Appendix B - 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/