ico.
Information Commissioner's Office

Information Governance Roles and Responsibilities Guidance

Document name	Information Governance Roles and Responsibilities Guidance
Version number	2.1
Status	Published
Department or Team	Cyber Security and Information Management and Compliance
Relevant policies	N/A
Distribution	Internal
Author	Iman El Mehdawy, Group Manager, Information Management and Compliance
Reviewed by	Alan McGann, Head of Cyber Security and Information Management
Approved by	Michael Fitzgerald, Director of Digital, IT and Business Services
Date of sign off	20 January 2022
Review by	31 January 2024
Security classification	Official

Key messages

The main objective of this guidance is to provide:

- Guidance on the ICO's approach to managing its information through a network of individuals with management board oversight.

- An explanation of the key roles in this network along with their responsibilities.

Does this guidance relate to me?

This guidance relates to all ICO staff.

Table of contents

1. Introduction

1.1. This guidance sets out the ICO's approach to managing its information through a network of individuals with oversight from the Risk and Governance Board (RGB) and the Data Protection Officer (DPO).

1.2. It explains the key roles in this network, outlines their individual responsibilities and deliverables and highlights the further support available to help them with their roles from our internal compliance teams and through existing ICO policies, procedures, and appropriate training. It applies to all directorates at the ICO.

Back to Top

2. Accountability

2.1. Accountability means taking responsibility for what we do with our information. It’s essential we manage risks and protect the confidentiality, integrity, and availability of the information we hold.

2.2. We do this by assigning specific responsibilities for information governance (IG) to senior managers. We also appoint officers in each directorate to support decision makers.

2.3. This network of individuals allows us to embed good practice across the ICO in a consistent manner. Oversight is provided by the DPO and RGB, which provide an escalation process through to the SIRO who has overall responsibility for IG and sits at the most senior level of the ICO.

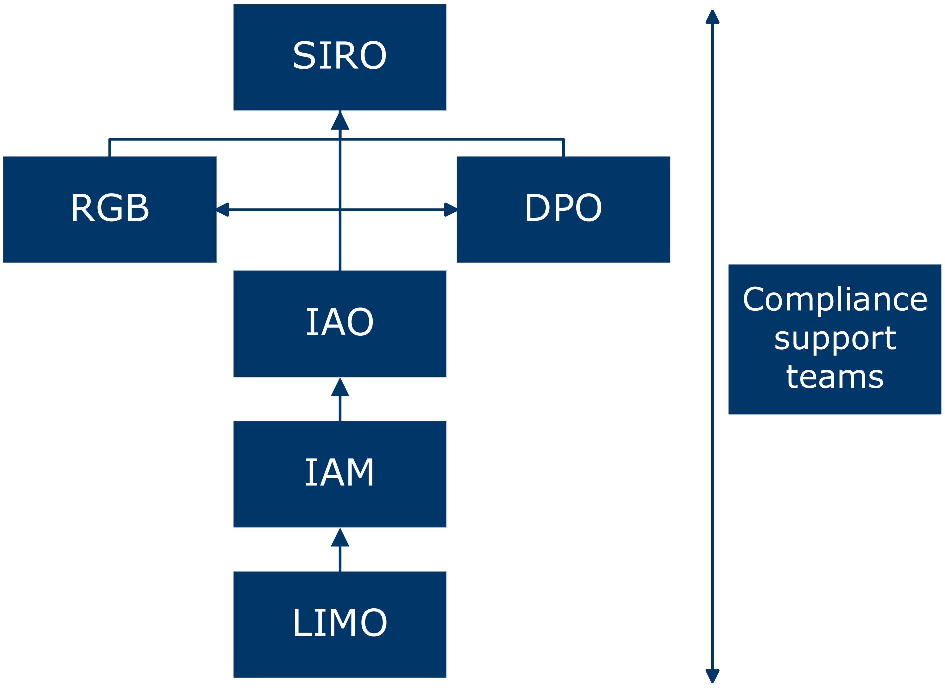
Back to Top

3. Our Information Risk Management Network

3.1. Our Information Risk Management Network (IRMN) aims to ensure that each information asset has a clearly defined asset owner and asset manager responsible for that asset on a day-to-day basis. There are a number of specific roles in the network.

- Senior Information Risk Owner (SIRO)
- Risk and Governance Board (RGB)
- Data Protection Officer (DPO)
- Information Asset Owners (IAOs)
- Information Asset Managers (IAMs)

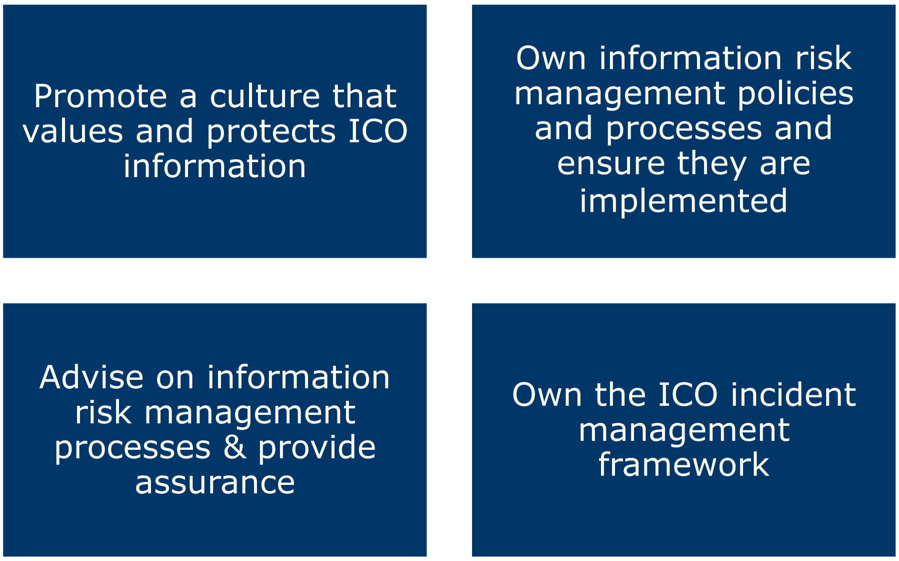
- Local Information Management Officers (LIMO)



Back to Top

4. Senior Information Risk Owner (SIRO)

4.1. The SIRO, who is the Deputy Chief Executive and Chief Operating Officer, plays the main role in the management and protection of the ICO's information assets. The main responsibilities of our SIRO are to:



Promote a culture that values and protects ICO information

Own information risk management policies and processes and ensure they are implemented

Advise on information risk management processes & provide assurance

Own the ICO incident management framework

4.1.1. Promote a culture that values and protects ICO information:

- Ensure the ICO has a plan to achieve and monitor the IG culture across the organisation and to take visible steps to support and participate in that plan.
- Ensure the ICO has designated staff with defined responsibilities including IAOs who understand their roles and are supported by appropriate information risk and governance policies.
- Ensure the ICO has a risk awareness and training programme of work that is appropriately communicated.
- Ensure that good IG assurance practice is shared within the ICO.

4.1.2. Own risk management policies and processes and ensure they are implemented:

- Act as the central point for information risk management at the ICO including resolution of any escalated risk issues raised by IAOs, the DPO, Auditors etc.
- Ensure the implementation of a risk management procedure and a risk policy and appetite statement that are appropriate for all

departments of the ICO in setting out how compliance will be monitored.

- Review all key information risks of the ICO on a quarterly basis and ensure that mitigation plans are robust.
- Ensure that information management policy, information risk management method and standards are documented, applied, and maintained consistently.
- Understand the information risks faced by the ICO and its business partners, ensuring that they are addressed, and that they inform decisions on outsourcing and data processing agreements.
- Ensure that information risk assessment and mitigating actions are subjected to an adequate level of independent scrutiny by external auditors.

4.1.3. Advise on information risk management and provide assurance:

- Ensure that regular updates are tabled at the ICO to brief, discuss, or report upon matters of IG, risk assurance and information risk culture affecting the organisation, including input to the annual IG reporting processes.
- Sign off an annual assessment of performance, including material from the IAOs and specialists, covering IG reporting requirements.

4.1.4. Own the ICO incident management framework:

- Ensure that the ICO has implemented an effective information incident management framework in line with the requirements of the data protection legislation.

Back to Top

5. Risk and Governance Board (RGB)

5.1. RGB provides an overview and scrutiny of information governance (IG) arrangements and considers escalated IG issues from the Senior Information Risk Owner (SIRO) for decisions. The Board is also tasked with assisting the Senior Leadership Team with management of risk including information risk by reviewing all matters concerning the development, maintenance, and implementation of the ICO's information risk and governance management framework, including monitoring, and reporting arrangements.

5.2. RGB has a permanent information governance working group tasked with:

- Supporting the work of the wider Information Risk Management Network in the continuous improvement of IG at the ICO.
- Establishing and implementing an Information Governance Strategy.
- Ensuring there is an effective accountability framework, with key roles, clear governance, and responsibilities, and with agreed outcomes.
- Developing an information risk appetite statement and maintaining an IG risk register ensuring risks are properly identified, effectively managed, and escalated accordingly.
- Acting on any issue or recommendation raised by the DPO.

- Providing the main point of reference and escalation for issues related to IG, providing recommendations to the SIRO for decision making where appropriate.

- Ensuring compliance with regulations through commissioning reports, audits and self-assessments on IG policies and operations.

- Providing assurance reports to RGB quarterly.

- Providing assurance that where there are changes in ICO processes or working practices, appropriate IG risk assessments are undertaken.

- Providing assurance that national developments in IG policies and legislation are recognised and acted upon.

- Ensuring the effective understanding and promotion of good IG within the ICO and across its partnerships.

- Supporting the reporting of progress to the Senior Leadership Team, Executive Team and Management Board as required.

Back to Top

6. Data Protection Officer (DPO)

6.1. The DPO has a responsibility to advise on and monitor our compliance with the DPA 2018 and UK GDPR and make recommendations to improve our practices. They work closely with several teams across the ICO.

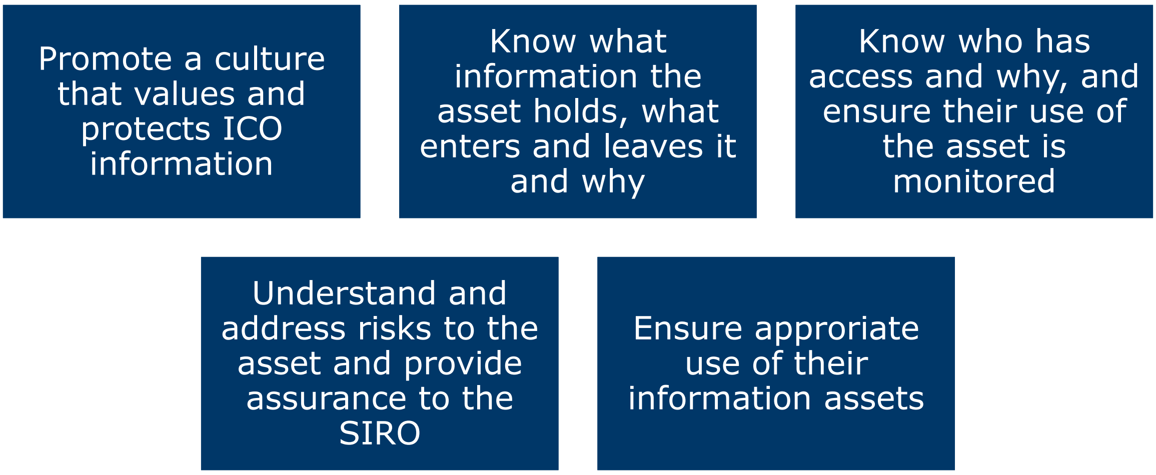
6.2. The DPO should:

- Ensure that both the ICO and the data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them.
- Give advice and recommendations to the ICO about the interpretation or application of the data protection rules and act as a point of escalation for data protection concerns.
- Ensure the creation of a register of processing activities within the ICO.
- Ensure data protection compliance within the ICO and help compliance with accountability obligations.
- Respond to queries from the regulator where it receives complaints about ICO processing.
- Ensure that complaints from data subjects are appropriately escalated and handled.
- Draw the ICO's attention to any failure to comply with the applicable data protection rules.
- Monitor completion rates for IG training.
- Receive assurance reports from key areas of the business on the progress of the ICO compliance with GDPR including security incidents and staff training.
- Have visibility and get involved in Data Protection Impact Assessments as required in line with the DPIA handling procedure.
- Ensure appropriate auditing of IG practices.

Back to Top

7. Information Asset Owners (IAOs)

7.1. Information Asset Owners at the ICO are the Directors. Their role is to understand what information is held within their directorate, how it is used, who has access and why, so that they can understand and address risks to the information. The main responsibilities of our IAOs are to:



Promote a culture that values and protects ICO information

Know what information the asset holds, what enters and leaves it and why

Know who has access and why, and ensure their use of the asset is monitored

Understand and address risks to the asset and provide assurance to the SIRO

Ensure approriate use of their information assets

7.1.1. Promote a culture that values and protects ICO information:

- Undertake training in information management and be familiar with the ICO’s IG policies and procedures.

- Ensure that their directorate’s plans reinforce and monitor the right culture in relation to information management and compliance across the directorate.

- Ensure compliance with the provisions of the UK GDPR in respect of the IAO's information assets, in accordance with the ICO's IG mechanisms and policies.

- Effectively plan IG activities with the ICO's compliance teams involving the Data Protection Officer, the SIRO and RGB as required.

- Provide IAMs and LIMOs with adequate time to carry out their responsibilities and ask to see evidence that assets are being appropriately managed.

7.1.2. Know what information the asset holds, what enters and leaves it and why:

- Keep their understanding of the asset and how it is being used by ensuring their directorate maintains a local information asset register.

- Ensure that registers of personal data held are compiled and maintained, including records of personal data processing mandated under Article 30 of the UK GDPR.

- Approve transfers while ensuring only the minimum amount of data required to achieve the business purpose is transferred.

- Negotiate, manage, and approve agreements on the sharing of personal data, confidential or sensitive information between ICO and third parties.

- Approve arrangements so that information put onto removable media, and information printed or taken away from the ICO offices, is minimised and protected and that written records are kept of their decisions to allow such activities.

- Ensure their staff follow the appropriate ICO policies for the protection of personal information, whether on digital systems or on paper.

- Approve the disposal mechanisms for paper or electronic records from their asset through consultation with the relevant compliance teams.

7.1.3. Know who has access and why, and ensure their use of the asset is monitored:

- Receive assurance from staff managing the directorate's information, e.g., SP site owners, that access provided to the directorate information is no more than the minimum necessary to achieve the business purpose.

- Understand the ICO's standards and policy on use of the information.

- Receive records of usage checks including storage capacity and adherence to retention and disposal schedule and assure themselves that they are being conducted.

7.1.4. Understand and address risks to the asset and provide assurance to the SIRO:

- Provide an annual written assessment to the SIRO about the security and use of the assets.

- Identify and, where appropriate, formally accept significant risks introduced when the directorate’s information is moved from one organisational unit, system element, medium or location to another.

- Ensure appropriate risk assessments such as DPIAs are completed in relation to their information assets. Integrate risk assessment outcomes and recommendations back into any work plan. Own and appropriately manage any residual risk.

- Make the case where necessary for new investment to protect the asset.

- Ensure all risk decisions taken are demonstrably in accordance with risk management policies and risk appetite agreed by the ICO.

- Take an active role in identifying and reporting new risks.

7.1.5. Ensure appropriate use of their information assets

- Ensure the timely search, retrieval, and response to access requests, including timely referrals to the Information Access team.

- Ensure that records selection methodology is appropriately applied, and that information of value is selected for permanent preservation for transfer to The National Archives.

- Consider annually whether better use of the information could be made including where it is decided that public access to information is in the public interest, proactively publish this information on the website making sure that appropriate checks and controls have been applied.

Back to Top

8. Information Asset Managers (IAMs)

8.1. Typically IAMs are the Heads of Departments. Their role is to support the IAOs with all aspects of their information management responsibilities and:

- Contribute to the department's plans to achieve and monitor the right culture, across the department and throughout its delivery chain, and take visible steps to support and participate in that plan.

- Support the department's compliance with the provisions of UK GDPR and data protection legislation in respect of the IAO's information assets, in accordance with the department's and the ICO's compliance mechanisms and policies.

- Provide the IAO with assurance that the department's IG is compliant with all the policies and procedures, and assist in completing compliance reports, ensure that risks to information are identified and appropriately mitigated and escalated.

Back to Top

9. Local Information Management Officers (LIMOs)

9.1. LIMOs act as local experts and advocates for good information management practices. Their key responsibilities are to:

- Promote information management guidance and policies within their team.

- Make themselves known to their colleagues and act as a model of best practice.

- Introduce new starters to any local IG practices in their area and tell them how to access help if they have queries.

- Be proactive in updating their colleagues on IG issues, current risks, or reminders about business-as-usual tasks by having a regular slot at departmental meetings to keep IG on the agenda.

- Engage with the LIMO forum sharing their experiences and challenges.

- Promote data protection compliance and accountability responsibilities in relation to the work of teams in their area.

- Update the Information Management and Compliance Service of any personnel changes in LIMO, IAM or IAO in their department

- Maintain the storage asset register and local information asset registers for their department.

- Ensure that any compliance questionnaires and annual reviews are responded to in a timely way and signed off by their IAO.

- Familiarise themselves with the Restore off site storage facility process and have oversight of any transfer of physical information from their area to our off-site facility.

- Maintain a log of physical information assets to track the movement of any assets removed from the office. Review the log regularly and be proactive in identifying any information that hasn't been logged in or out correctly. Ensure staff are aware of the log and how to use it.

- Provide assurance to the IAO that all the above activities are being completed in a timely manner.

Back to Top

10. Compliance Support Teams

10.1. Central support to the information risk management network is provided by several compliance support teams with responsibilities and appropriate skills to deliver the following functions:

Information Management, Information Security, Risk Management, Information Access, Facilities, IT, Legal, Procurement and HR.

10.2. The compliance teams produce the policies, procedures and standards and make them available to all staff in a central corporate repository. Each compliance team has a set of guidance, templates and published requirements that should be followed.

10.3. The information management team runs an IG compulsory training as part of staff induction covering the basic information access, security and information management requirements at the ICO. More specialised training is also available to certain staff requiring it to enable them to carry out their information governance responsibilities effectively. Training modules are available on the internal training system I-Learn.

10.4. The compliance teams also manage and summarise the reports for the SIRO, DPO and various oversight committees on information risks, security, compliance, and auditing.

10.5. All teams provide day to day assistance on IG issues via dedicated email inboxes publicised to the whole office on the intranet.

10.6. Directorates across the ICO assign administration duties to members of staff for the management of EDRM and other digital platforms. Those members of staff must follow all information management and security policies, procedures and guidance and escalate any problems to the IAO when appropriate.

Back to Top

11. Information Management Policies and Procedures

11.1. Further information to support ICO staff and the IRMN is available in our various policies and procedures, accessible in the Policies Hub on Iris.

11.2. All members of the IRMN should also familiarise themselves with the Business Continuity Plan, the Risk Register and the Risk Management Policy and Procedure.

Back to Top

Feedback on this document

If you have any feedback on this document, please fill in this feedback form.

Version history

Version	Changes made	Date	Made by
0.1	First Draft	18/01/2022	Iman El Mehdawy
1.0	Published	20/01/2022	Iman El Mehdawy
1.1	Content moved to new corporate template. Minor text and formatting changes.	07/10/2022	Steven Johnston
2.0	Review and minor typo change	10/02/2023	Iman El Mehdawy
2.1	Formatting changes to meet accessibility requirements.	27/06/2023	Ben Cudbertson

Back to Top