Cabinet Office

Guidance: Information Asset Owner Role

November ___

Version History

Document Version	Date Published	Summary Of Changes
1.0	March 2009	N/A
1.1	April 2013	Minor changes to format and branding.
1.2	October 2013	Updated following assimilation of IS6 into the SPF.
1.3	May 2018	Changes in data protection legislation reflected.
1.4	December 2023	Changes to: - align with Government Security: Roles and Responsibilities 2018 (removing reference to the mandation of positions such as Senior Information Risk Owners and Departmental Security Officers); - align the Role of the Information Asset Owner section with policy text included in Government Security Classifications Policy 2023; - remove out of date staff training and reference the new Security and Data Protection module on Government Campus; - update references to the Data Handling Review; - include reference to departments publishing a list of their IAOs; - update the executive summary; - remove out of date annexes; - make organisational responsibilities clearer under new subheading; and - change references to the Security Policy Framework to GOV007 Functional Standard Crown copyright page updated. Minor changes to formatting and branding.

Guidance: Information Asset Owner role

Executive Summary

The Information Asset Owner (IAO) plays a specialist role (as outlined in Government Security: Roles and Responsibilities) in securing information in many departments. The role was originally mandated across government as part of the 2008 Data Handling Review. This guidance sets out the nature and primary responsibilities of an IAO in managing the risks to personal information and business critical information held within a department.

This version of the guidance is issued as an interim update, intended to bring the guidance broadly up to date pending a wider review of the IAO role to be undertaken by the Cabinet Office during 2024.

Cabinet Office

2023

Role of the Information Asset Owner

1) Government Security: Roles and Responsibilities (issued in November 2018), outlines that Information Asset Owners are:

   "Named senior individuals responsible for each identified information asset (e.g. database or ICT system) at the appropriate business level within a Department/Agency."

2) Information asset owners must be senior/responsible individuals involved in running the relevant business, and must be trained on appointment. They need to: understand what information is held by their unit or directorate; address risks to their information; ensure that information is appropriately protected and marked; and, ensure information is used in compliance with all legal requirements, such as the Data Protection Act 2018 , UK GDPR, Freedom of Information/Environmental Information Regulations, the Public Records Act and the Inquiries Act. The IAO must provide written input to the senior board level risk owner annually on the security and use of the information asset.

Information Asset

3) An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and life cycles.

The IAO in Context

4) IAOs must formally review the risks to the confidentiality, integrity and availability of their information assets, including those in their delivery chain, at a minimum once a year or more frequently (quarterly or six monthly) as stated in the department's risk management policy, and implement proportionate responses. An IAO is mostly responsible for the protection of information held on ICT networks and also manages other hard copy information assets. IAO responsibilities must also take into account organisational culture and behaviours.

5) IAOs also have a responsibility to ensure compliance with data protection law within their business area.

Organisation Responsibilities

6) Departments with IAOs must ensure that:

- All staff with access to personal information successfully complete Security and Data Protection Training (available on Government Campus) on appointment and thereafter as appropriate according to the department's business needs and circumstances.
- The IAO has the skills, resources and authority to discharge their responsibilities and to take action on any deficiencies in the relevant processes.
- Appropriate mechanisms exist so that where duties are distributed across posts and organisational units, they are fully co-ordinated and visible to all relevant staff.
- Appropriate reporting chains exist to ensure that a senior board level risk owner (where relevant, or an equivalent role) has full visibility of the state of information asset management across their organisation.
- Assurance is available that all delegated duties are properly carried out.
- All relevant duties and responsibilities are demonstrably discharged.

7) Where an organisation has a Departmental Records Officer (DRO), an IAO is likely to liaise with the DRO to ensure that duties are properly coordinated. However, the specific mechanisms of how this relationship will or could operate will be up to the individual organisation.

8) Organisations may choose to publish a list of IAOs on their staff intranet. These organisations should ensure that this list is regularly updated.

9) Another essential aspect of Information Assurance (IA) is proper control over the integrity and availability of personal information. The information must be of sufficient quality to fulfil its business function and it must be available when needed, including to trace changes to personal information. Proper version control over information, including assets such as back-up or archive media and paper records, is essential. This ability to trace changes will allow errors, should they occur, to be corrected.

Information Asset Owner Responsibilities

10) In order to help meet the requirements of the Government Functional Standard: GOV 007, IAOs will:

A. Lead and foster a culture that values, protects and uses information for the public good.

They must

1. Undertake and pass information management training on appointment and at least annually thereafter.

They should:

2. Act as a source of advice and expertise to their business unit.
3. 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.
4. Ensure compliance with the provisions of data protection legislation in respect of the IAO's personal information assets, in accordance with the department's compliance mechanisms and policies.
5. Work effectively with the department's Data Protection Officer.

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

They must:

1. Submit a request to the relevant IAO where they consider that public protection or public services could be enhanced through greater access to a particular asset.
2. Maintain a log of access requests made.
3. Monitor as required with managers permissions granted to transfer personal information to removable media.

They should:

4. Keep their understanding of the asset and how it is used up to date.
5. Ensure that registers of personal data held are compiled and maintained, including records of personal data processing mandated under Article 30 of the General Data Protection Regulation.
6. Approve and minimise transfers while achieving the business purpose.
7. Negotiate, manage and approve agreements on the sharing of personal information between organisations.
8. Approve arrangements so that information put onto removable media is minimised and protected. To do this IAOs should:

a) Agree with the Senior Security Advisor an appropriate regime for the physical protection of personal information, whether on ICT systems or on paper.
b) Keep written records of their decisions on at least the following:

- Unavoidable use of removable media.
- Application of mandatory risk mitigation measures if use of removable media is unavoidable.
- Use of alternatives to removable media for information transfer or storage.
- Suitability of security configurations on remote systems with approved access to the asset.
- Exemptions from the requirement to encrypt material stored on removable media together with approval of compensating risk management measures.

9. Approve the disposal mechanisms for paper or electronic records from their asset. To do this IAOs should:

   a) Agree with the Senior Security Advisor and/or Departmental Records Officer an appropriate regime of department-wide arrangements for the secure disposal of electronic or paper material, which has contained or carried personal data (in line with the security controls outlined in Government Security Classifications Policy, issued in 2023).

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

They must:

1. Agree in writing that relevant access control regimes permit the business to be transacted with an acceptable level of risk or, if agreement cannot be given, require that an acceptable alternative approach be adopted.

They should:

2. Understand the organisation’s policy on use of the information.
3. Check that access provided is the minimum necessary to achieve the business purpose.
4. Receive records of usage checks and assure themselves that they are being conducted. To do this IAOs should:

a) Establish with managers an appropriate regime for the monitoring of the use made of access to personal information, electronic or otherwise.

b) Establish with managers appropriate mechanisms for the IAOs to receive summary reports on the progress and results of such monitoring.

D. Understand and address risks to the asset, and provide assurance to a senior board level risk owner.

<u>They must</u>

1. Provide an annual written assessment to the relevant senior risk owner about the security and use of the asset.

<u>They should:</u>

2. Contribute to the department's risk assessment. To do this the IAOs should identify and, where appropriate, formally accept significant risks introduced when personal information is moved from one organisational unit, system element, medium or location to another.
3. Make the case where necessary for new investment to protect the asset.
4. Ensure all risk decisions taken are demonstrably in accordance with departmental risk management policies.

E. Ensure the asset is fully used for the public good, including responding to access requests.

<u>They must:</u>

1. Receive and log access requests from others. To do this IAOs ensure that a log of access requests is maintained.

<u>They should:</u>

2. Negotiate, manage and approve agreements on the sharing of personal information between organisations.
3. Consider annually whether better use of the information could be made.
4. Where it is decided that public access to information is in the public interest, reflect this in the departmental Freedom of Information Publication Scheme.
5. Ensure decisions on access are taken accordingly.

Any enquiries regarding this publication should be sent to us at governmentsecurity@cabinetoffice.gov.uk

This publication is available at www.gov.uk/government/publications

Printed on paper containing 75% recycled fibre content minimum.