Cabinet Office

Guidance on the DHR Mandatory Role: Information Asset Owner

March 2009

Making government work better

Guidance on the DHR Mandatory Role: Information Asset Owner

Audience: **This paper will be of particular interest to SIROs (on behalf of AO) and IAOs.**

Action: **Implement**

Timing: **Immediate**

Background

1. The Data Handling Review (DHR) stated that Government will implement the role of Information Asset Owner (IAO), specifically in relation to Personal information.

Guidance

2. This guidance sets out the nature and primary responsibilities of an IAO and proposes means of discharging these responsibilities based on Departments' experience.

3. This guidance discusses the role of an IAO in relation to Personal information. Some Departments have extended the role to cover a wider range of information assets, and this guidance does not prevent the possibility of such an interpretation.

Key to word usage in the 'Information Asset Owner Duties' section of this guidance

Must: Responsibilities/actions quoted or paraphrased from Mandatory Minimum Measures (HMG Infosec Standard No 6)

Should: Responsibilities/actions recommended in the previous April guidance, or new recommendations implied by or supportive of the Mandatory Minimum Measures (HMG Infosec Standard No 6)

Contacts Enquiries about content should be directed to:
datareview@cabinet-office.x.gsi.gov.uk

INFORMATION ASSET OWNER

The term 'information assets' is broad in scope and its definition is dependent on context. For the purposes of this guidance the term refers only to personal information stored or processed on government information systems, both information that is owned by government and that which is entrusted to it. The responsibilities described in this document should be read with this limited definition in mind. Departments may however apply this guidance against a wider definition of assets, e.g. for non-personal data or for information system components if they wish to do so.

The Mandatory Minimum Measures (now included in the Security Policy Framework (SPF) as HMG Infosec Standard No 6 (IS6) state that:

> *"(Information) Asset Owners (IAOs) must be senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process."*

The IAO in Context

Many IAO duties have long been carried out by staff with other titles, e.g. business or process managers, data guardians, information asset managers or internal governance units. There is no intention, requirement or recommendation that existing structures, terminology or mechanisms be changed to fit the template of a single IAO discharging all the duties described either in IS6 or in this guidance note.

It is appreciated that the 'assuring' and 'ensuring' aspects of the role(s) will not necessarily be carried out by the same individual. The person who gives assurance to the Department and/or to the Senior Information Risk Owner (SIRO) is not necessarily the one who ensures that relevant action is taken. The important point is that both aspects must be properly and demonstrably assigned, linked and carried out.

All the duties and requirements set out in IS6 (which are repeated and expanded upon in this guidance note) must be assigned so that:

- Each is discharged by a named post holder.
- The post holder is responsible and accountable for the duties in question.
- The post holder has the skills, resources and authority to discharge the responsibilities and 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 the SIRO has full visibility of the state of information asset management across his or her organisation.
- Assurance is available that all delegated duties are properly carried out.
- All relevant duties and responsibilities are demonstrably discharged.

The remainder of this guidance note is written on the basis of a single IAO discharging the responsibilities identified; however this should be read with the preceding observations in mind. Statements such as ‘an IAO will/should/must’ do not imply that one post holder is directly responsible for all activities. Distributing responsibilities to appropriate staff who do not carry the IAO title and across organisational units is appropriate as long as compliance with the principles set out above can be assured and demonstrated. Where an organisation has a Departmental Records Officer (DRO), an IAO is likely to liaise with the DRO to ensure that duties are properly co-ordinated. However, the specific mechanisms of how this relationship will or could operate will be up to the individual organisation.

An IAO is mostly responsible for the protection of computers and networks, but also manages other assets such as paper records and backup tapes. Critically, IAO responsibilities must also take into account organisational culture and behaviours.

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. This includes the necessity of being able 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 Duties

In order to meet the requirements of IS6 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. Contribute to the Department's plans to achieve and monitor the right culture, across the Department and throughout its delivery chain.
3. Take visible steps to support and participate in that plan.
4. Ensure compliance with the provisions of the Data Protection Act (DPA) in respect of IAO's personal information assets, in accordance with the Department's compliance mechanisms and policies.

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 that IAO's asset.
2. Maintain a log of access requests made.
3. Monitor as required with managers the allocation of users' rights 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.
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 Departmental Security Officers (DSOs) 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 DSOs an appropriate regime of Department-wide arrangements for the secure disposal of electronic or paper material, which has contained or carried personal data.

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

They must:

10. 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.
11. Ensure that a record is kept of individuals with access to, or involvement in the handling of, records containing protected personal data.

They should:

12. Understand the organisation's policy on use of the information.
13. Check that access provided is the minimum necessary to achieve the business purpose.
14. 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 protected personal information, electronic or otherwise.

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

D. Understand and address risks to the asset, and provide assurance to the SIRO.

They must:

15. Provide an annual written assessment to the SIRO about the security and use of the asset.

They should:

16. 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.
17. Make the case where necessary for new investment to protect the asset.
18. Ensure all risk decisions taken are demonstrably in accordance with departmental risk management policies established by the SIRO.

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

They must:

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

They should:

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

Annex to IAO Guidance

Data Protection Act Principles

Guidance on the Data Protection Act should be obtained from the Information Commissioner's Office (www.ico.gov.uk) and from departmental data controller staff. The eight principles identified in the Data Protection Act 1998 are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    a. At least one of the conditions in Schedule 2 is met; and
    b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one of more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country of territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix to IAO Guidance

IAO Case Studies

Introduction - use of the case studies

The following case studies provide examples of how a selection of organisations, with both homogeneous and heterogeneous record set, have implemented the IAO role. Please be aware that these case studies are not a template and are not intended to be prescriptive. Instead, they aim to provide organisations with ideas of the characteristics of the IAO role that have proved successful elsewhere.

Selection of case studies

A. Large umbrella department with a heterogeneous set of records
B. Large organisation with heterogeneous set of records
C. Small organisation with homogeneous set of records
D. Small organisation with homogeneous set of records for a service that is fully contracted out.
E. Small organisation with heterogeneous set of records

A. Large umbrella department (≈20,000 staff, 90% of whom are in Executive Agencies), which holds a heterogeneous set of records, including personal data on staff and 40million records for customer data.

Nature of the organisation: The organisation has around 20,000 staff, approx. 2000 of whom work for the central Department and 18,000 in the Executive Agencies. In the central Department personal information is predominantly held on employees (HR data), with sensitive personal records being held by the security division, who have carried out vetting on staff. Meanwhile, Agency personal data is predominantly customer related, though personal data on employees is still also held. There are around 1000 records (as assets) across the Department with an agency holding a database which contains over 40million individual records.

Seniority of IAO: There are around 250 IAOs in the whole department, who vary from PB4 (HEO with delegated authority) to SCS PB1 (Grade 5, Divisional Manager).

IAO's direct responsibilities:

1. Setting good practice examples for others, in the handling of data.
2. Maintaining their own Information Asset Table; this must be reviewed on a quarterly basis or whenever anything changes.
3. Assessing risks to the confidentiality, integrity and availability of their assets.
4. Recording the business impact levels on their asset table, and risks on their business risk registers, to be reviewed and reported on a quarterly basis
5. Ensuring the asset is fully used and is still required

Support available to IAOs: Provided by data handling and security advisors who manage and summarise the reports for the SIRO, as well as provide everyday assistance to staff on data handling issues. For IAOs in the central Department there is a central Data Handling Team (DHT) who are coordinating the implementation of the Cabinet Office review recommendations.

Responsibilities delegated from IAO to the support staff:

a. HR are responsible for implementing the training aspect.
b. The Information Management Directorate plays a key role in raising awareness about Data Protection Act (DPA) and data handling issues.

c. The DHT manages Department-wide policy on the use of removable media, which IAOs must refer to when considering requests to put their assets on such media.
d. DHT must be consulted on any data sharing activities involving a significant number of personal details, with appropriate clearance required from legal teams, the SIRO and Ministers.
e. DHT undertakes a consistency check on the business impact levels appearing across the Department and seeks to understand the risks to individual assets in order to judge which items to report to the SIRO/Board.
f. DHT make sure that correct teams are involved in clearing new data sharing arrangements by involving legal and data security experts as required.

IAO methods to ensure delegated work is completed:

i. IAO liaises with DHT to ensure they are kept up to date with recent developments.
ii. Any exceptions to the removable media policy must go through the relevant IAO, the DHT and the Security Team before being put to central Department SIRO for decision. Outcomes are then reported back to IAO and kept on record by DHT.
iii. IAOs work collaboratively with DHT and ensure that any changes to risk assessments obtain IAO's approval.

Critical issues of Best Practice;

- Clear policy on use of removable media is critical, made clear to all - not just IAOs.
- The information asset tables also contains; the purpose for collection and sharing, as well as methods used for transferring and handling the data.
- Consideration is continuously given to whether efficiencies can be made by better use of the asset, through assessing the business processes and data flows as a whole.
- Every data sharing activity is cleared with legal and data security experts and supported by enforceable contracts. In the cases where the sharing of data is with other public sector organisations, detailed and specific memorandums of understanding are also provided.

B. Large organisation (>2500 staff), which holds a heterogeneous set of records, including staff recruitment and employment data

Nature of the organisation: Small Agency with around 2500 staff (a fifth of whom are contractors), which holds normal recruitment/employment related personal details on non-contractor staff, as well as customer details.

Seniority of IAO: One IAO in each of the business functions e.g. Finance, Human Resources (HR) etc. The seniority of the IAO is generally Corporate Director or Head of Function.

IAO's direct responsibilities:

1. Fostering a culture of value and protection of personal information in their business area.
2. Passing their IA training/knowledge onto key staff.
3. Approving, monitoring and minimising data transfers.
4. Liaising with other IAOs and organisations.
5. Reporting data breaches to the SIRO and Governance Officer.
6. Providing annual report to the SIRO about the security, use of and justification for continued requirement of the asset.
7. Ensure that a register of information assets is maintained and the security risks assessed, at least quarterly.

Support to IAOs: From the Governance Officer, as well as assistance from their business functional teams.

Responsibilities delegated from IAO to the support staff:

a. Training ALL Business function staff in the IAOs remit.
b. Ensuring compliance with the DPA provisions and the Government Protective Marking Scheme, with respect to personal information assets.
c. Logging requests for assets.
d. Keeping records of individuals with access to, or involvement in handling of, records containing personal data.
e. Logging data transfers by the business unit and any incoming requests for access to the asset in a national log, and producing an annual national report.
f. Reporting data breaches to the SIRO and Governance officer

g. Carrying out risk assessment to assets and presenting risk assessment proof to the IAO, at time intervals specified by the business unit[1].
h. A deputy ensures that quarterly reviews are carried out and collates returns for the IAO.

IAO methods to ensure delegated work is completed:

i. Centrally holding and monitoring a log of work that needs to be carried out/completed. This is then reported to Accounting Officer and Board.
ii. IAOs receive a summary report on a regular basis and review actions annually, when new posts are created.

Critical issues of Good Practice:

- Each IAO has the responsibility and the status to move changes forward.
- Each member of staff will be required to complete the basic training and this will be monitored until all staff have completed it.
- Staff need to understand their responsibilities as set out in the IA policy.
- Clear policy on use of removable media is critical, made clear to all not just IAOs.

[1] In practice, the risk assessments should always be examined by the most senior person with direct responsibility for the information asset.

C. Small organisation (>10 workforce), which holds a homogenous set of records, collecting around 60,000 personal data records annually and holding historic records from a decade ago.

Nature of the organisation: Small organisation with a workforce of seven, yet holds around 60,000 records annually, plus historical data of around 550,000 records (going back to 98/99). The organisation currently works with three different contractors and three other agencies.

Seniority of IAO: The IAO is a Professional Officer (TDA 5) or SCS.

IAO's direct responsibilities:

1. Liaising with other agencies on their data requirements and sharing.
2. Appointing and reviewing contracts to collect and manage data, ensuring that contracts contain the Data Handling Review (DHR) security clauses.
3. Regular review of business cases – establishing clear current and ongoing need for each data item
4. Establishing and monitoring user roles for data collection, management and publication systems

Support to IAOs: Provided from the rest of the team.

Responsibilities delegated from IAO to the support staff

a. Liaising with Information Technology and Telecommunications (ITT) providers
b. Ensuring systems are built to specification, i.e. that the asset meets the needs of the user, through regular review
c. Including data risks within the project risk assessment
d. Ensuring responsible management and review for data collection

IAO methods to ensure delegated work is completed: a formalised management and reporting structure including objective setting and annual appraisals.

Critical issues of Good Practice:

- Clear business case to collect, manage and analyse personal data.
- Establish secure systems to hold data.

- Time-limited agreements with failsafe system i.e. data sharing will stop if the agreement has not been renewed.
- Ensure that any contracts/agreements contain the DHR security clauses.
- Ensure all systems have integrated audit trails.
- Service Level Agreements for contractors – with DHR security clauses.
- Effective project and contract management – with DHR security clauses.
- Carries out data access controls – user roles and permissions and password issue and management
- Clearly identifies individuals responsible for the data transfer.
- Undertakes data access review – who needs access to personal data and who can fulfil their requirements with anonymised data.
- Data sharing agreements/contracts – regularly reviewed, with DHR security clauses.
- Requiring contractors and agencies to have incident reporting arrangements in place.

D. Small organisation (>10 workforce), which holds a homogenous set of records and provides a fully contracted out service, collecting around 35,000 personal data records annually and holds historic records from a decade ago.

Nature of the organisation: The organisation works with one contractor to deliver a service and liaises with other agencies and its parent department. The organisation holds approx 35,000 personal data records annually, including historic data over ten years.

Seniority of IAO: The IAO is of Team Leader grade or SCS.

IAO's direct responsibilities:

1. All relationship management and compliance by the contractor, regarding data storage and management, including contract management which includes the DHR security clauses.
2. Regular risk assessments via the Programme and Project Management (PPM) system.
3. Ensuring that that the asset meets the needs of the user through regular review

Responsibilities delegated from IAO to the support staff

a. Monitoring contractor data management and handling,
b. Risk assessment and recording

IAO methods to ensure delegated work is completed:

i. PPM Reporting every month, includes a Project Risk Log for all team activities,
ii. Quarterly Tripartite meetings with key external contractors,
iii. Weekly project management calls with key contractors;
iv. Weekly team meetings to discuss project development and delivery issues,
v. Comprehensive, independent, regular audits of contractor systems to ensure that data is secure

Critical issues of Best Practice:

- Risk management systems are based upon regular team meetings and high quality information flows.
- Allocation of roles and responsibilities (own staff and contractor's staff)
- Ensure that only information which is required for the operation of the activity or for monitoring purposes is included.

F. Small organisation (≈200 staff), which holds a heterogonous set of records, including personal and financial information.

Nature of the organisation: The organisation, which has approx 200 staff, holds around 2 million records, which includes personal data, financial banking information, education and employment data. The organisation also holds statutory relationships with other agencies and contractors, including specified data exchanges in order to maintain personal information.

Seniority of IAO: There are 11 IAOs in the organisation; all of whom are members of the senior management team (one level below executive board).

IAO's direct responsibilities:

1. Constructing and maintaining information asset register
2. Managing access controls on data
3. Conducting quarterly risk assessments
4. Submitting quarterly and annual report to the SIRO
5. Raising awareness in teams

Support available to IAOs: Provided from a Data Governance Manager, who gives advice, guidance and support on policy, risk assessment and risk management, and business support staff (G7 to HEO, and occasionally an EO)

Responsibilities delegated from IAO to the support staff: Information gathering to support the IAO.

IAO methods to ensure delegated work is completed: Personally reviewing the information provided in meetings with those gathering it. On particular issues, they will take advice personally from the Data Governance Manager and seek to act upon it.

Critical issues of Best Practice

- IAOs invest sufficient time in managing information security, to ensure they provide effective assurance to SIROs i.e. realise they cannot delegate the whole thing. They need to get their "hands dirty".
- IAOs accept the corporate significance of the issue and share a common sense of proportionality and risk tolerance.

- IAOs understand the range of people, technical and contractor risks sufficiently in order to be able to identify risks. Risk naivety is one of the biggest risks!
- IAOs should be ensuring managers are protecting the IAOs assets by ensuring line managers are properly reviewing access controls.
- Data sharing must have business justification, legal requirement or data subject consent
- Minimise the amount of data shared
- Ensure security of data, especially whilst in transit
- Access control management depends on good administrative systems and reports regarding staff access