TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 40 The Role of an Information Asset Owner

Introduction

The Information Asset Owner (IAO) is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information you hold, how important it is, how sensitive it is, how accurate it is, how reliant you are on it, and who is responsible for it. It helps ensure that you can use the information you need to operate transparently and accountably.

This advice provides an overview of the role of the IAO in your agency. This document provides a good starting point for IAOs, giving practical guidance on:

- ***Identifying information assets***
- ***Managing information risks***
- ***IAO responsibilities***
- ***How to achieve them***
- ***Who can help you***
- ***How to know if you are doing your role well.***

Who is this Advice for?

This guidance is primarily aimed at Information Asset Owners. It may also be useful for Risk Managers, Project Managers when initiating projects, Information Managers and IT Managers to help them understand the support they may be called upon to provide.

Key Principles

Your role is about managing **information** not systems.

You are responsible for ensuring that information is protected appropriately and, where the information is shared, that the proper confidentiality, integrity and availability safeguards apply. But you are equally

responsible for ensuring that its value to the organisation is fully realised and that it is used appropriately. You will also need to ensure that information is managed appropriately following change (see Appendix B).

The role of the IAO is also to ensure that personal data is identified and securely handled. However, you also need to ensure you are managing the handling of other categories of sensitive or important information that your organisation relies on. This involves making sure that it can be used in the way you need, for as long as you need.

Your role is about providing assurance and making sure that action is taken. But that doesn't mean you have to do everything yourself - in fact much of the role is about understanding and where necessary coordinating the activities of others in your agency who have specialist areas of responsibility. Your IT, Security and IM functions are key contacts in supporting you in the role. However, if you delegate responsibility for ensuring actions are taken, you must make sure that this is properly co-ordinated and that there are clear reporting lines and that everyone understands their responsibilities. You can delegate responsibility to particular areas that can support you in your role but you retain accountability for proper information management and handling.

You will need to work with other IAOs in your agency to ensure your information is properly protected and the value to the organisation fully realised.

What is an Information Asset and what assets are you responsible for?

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

Your role within your agency will determine what information assets you are responsible for. **This should not just be a list of systems to manage, but should focus on the information that needs to be managed within those systems.** This could cover both sensitive personal data and non-personal information that is critical to business. It could be held in paper as well as electronic formats.

Information risks to manage

As an Information Asset Owner you will need to assure against:

- Inappropriate access to, or disclosure of, protectively marked or personal data by staff, contractors, volunteers and the public, whether accidental or deliberate
- Internal threat - staff, acting in error or deliberately, or external parties accessing your information illegally and exposing it/acting maliciously to defraud you or your customers
- Information loss - particularly during transfer or movement of information, or as a result of business change (government or internal restructure)
- Loss of access to information
- Loss of digital continuity - i.e. losing the ability to use your information in the way required when needed. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information - how long you need to use and keep it - is often different to the lifecycle of the IT system used to access and support it.
- Poor quality of information and poor quality assurance, for example, of data sets.
- Poor change management - business needs change, systems change, your information risk appetite may change, so you need to keep your policies and processes in step accordingly.

- Not maximising the public benefit from information (leading to a waste of public money and poor service delivery).

Your responsibilities

Your role is to ensure that the information in your charge is properly protected and its value to the organisation fully realised. This section of the Advice looks at what you are required to do to meet these responsibilities and how that might look in practice. Some of your responsibilities require you to take action, others simply to assure that action is being taken by others, such as your IT, IM and IA (Information Architecture) teams.

You have five responsibilities:

1. Lead and foster a culture that values, protects and uses information.

2. Know what information the asset holds, and what information is transferred in or out of it.

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

4. Understand and address risks to the asset and ensure any data loss incidents are appropriately managed.

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

You need to be able to answer the following questions:

- Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented and do others need that information?
- Have I assessed information risks to those assets?
- Do I have a plan for managing risks and identifying opportunities?
- Do my team(s) and other teams, volunteers, contractors, etc. understand their roles and responsibilities in managing those risks and opportunities?

Your IM, IT and information security staff are a great resource and can support you to provide much of that assurance. You need to discuss with them your business requirements so that they can include these into their operational IT, protective security and information management policies and plans.

1. Lead and foster a culture that values, protects and uses information.

What you need to do

- Actively contribute to your agency's plans to achieve and monitor the right information handling culture.
- Ensure the handling of your information assets complies with the *Personal Information Protection Act 2004* and your agency's Information Security compliance mechanisms and policies.
- Understand and document the business value of the information assets you are responsible for.

How you might do this

- Meet with other IAOs in your organisation to share ideas and talk to your Information Management Team.
- Make sure that people who use your information assets understand the rules and are aware of the consequences of non-compliance. Explore using line management responsibilities - appraisals and objectives setting - to monitor this
- Talk to your Senior Management about what you can do to contribute to departmental plans for cultural change
- Set up a 'lessons learned' log so if things go wrong you can learn from them and ensure that policies and practices are changed
- Talk to your agency's Information Security Officer to ensure appropriate physical, procedural and personnel security.

Get assurance from others

You can talk to your RTI officers to assure that how you're managing your information assets meets requirements.

You can also contact relevant teams to get the assurance that the way you need to use your information assets is reflected on IM, IT and protective security policies and practices.

2. Know what information the asset holds and what Information is transferred in or out of it

What you need to do

- Understand and address risks to your information assets
- Know who has access to your information assets and why and monitor use
- Understand whether a delivery partner or supplier has a dependency on your information to deliver a service
- Approve and minimise transfers
- Monitor the allocation of users' rights to transfer personal information to removable media
- Approve arrangements so that information put onto removable media is minimised and protected
- Make sure your information assets are fully used for the public good, including responding to access requests. This includes actively considering whether public protection or public services could be enhanced through greater access to the information assets that you are responsible for.

How you might do this

Document your understanding of your information assets (in an Information Asset Register). Refer *Advice 39 Developing an Information Asset Register.* Work with your IT and IM teams to document:

- What the assets are - what they cover, their content, what's sensitive and/or protectively marked and what personal data you're responsible for
- The value of your information assets to the business - now and in the future. How important are they and why? What would be the impact of losing or mishandling them? As part of this process you should consider the benefits of increasing access or of information re-use.

- Your usability requirements for those assets - who needs to be able to find them, how do you need to work with them to maintain the understanding and trust in that information? What authorised Records Retention and Disposal Schedules do you need to use?
- Keep a record of all staff and contractors with access to records containing personal data - or who handle records containing personal data. Ensure a process is in place to remove that access as soon as it is no longer required
- Manage agreements on the sharing of personal information between organisations
- Keep written records of the decisions you agree with IM, IT and security staff
- Talk to your senior executives about information security

Get assurance from others

Get assurance from your IT and IM teams that they are managing digital continuity - the ability to use your information assets in the way that you need, for as long as you need. TAHO has produced some advice on this topic (see the TAHO website).

Get assurance from your Agency Information Security Officer that personal and protectively marked information (in digital or paper format) is appropriately protected.

This should cover:

- Mandatory risk mitigation measures if use of removable media is unavoidable
- Alternatives to removable media for information transfer or storage
- Suitable security configurations on remote systems with approved access to the information assets you are responsible for
- The secure disposal of personal data and protectively marked information
- Exemptions from the requirement to encrypt material stored on removable media, together with approval of compensating risk management measures.

An Information Asset Register Template is available in *Advice 39 Developing an Information Asset Register*.

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

What you need to do

Agree in writing that relevant access control regimes allow business to be transacted with an acceptable level of risk – or require that an acceptable alternative approach be adopted. You need to agree who has access to your information assets:

- Ensure that you keep a record of individuals with access to, or who handle, records containing personal data
- Keep a log of access requests

How you might do this

- Make sure you understand your organisation's policy on the use of the information assets you are responsible for

- Document your agency's Risk Manager the level of access provided for each asset and when this will be reviewed
- Talk to your agency's Information Security Officer to ensure appropriate policies to protect physical, personnel/ confidential information are in place

Get assurance from others

You don't have to monitor access directly but you do need assurance that it is being done. Agree how to monitor usage with your managers and then ask them for records of usage checks and summary reports on what's been done, and the results.

Get assurance from your IT team that access rights to IT systems are limited to the appropriate people.

4. Understand and address risks to the asset

What you need to do

- Ensure that significant correspondence about information risk handling is placed on the corporate recordkeeping system
- Contribute to the agencies 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
- Make the case where necessary for new investment to protect the asset
- Ensure all risk decisions taken are demonstrably in accordance with agency risk management policies and the agency's Information Security Framework
- Make decisions based on a risk assessment where users believe it is not possible to comply with policies or controls. Consult with others where necessary and ensure the decision and the reasons behind it are placed on the corporate recordkeeping system

How you might do this

- Make sure you are aware of the full range of risks – see section 'Information Risks to Manage' page 2.
- You defined your usability requirements in section 3 on page 5. Use this information to assess risks and opportunities:
- Understand how to maintain your digital continuity – identifying the management processes and technologies you need to satisfy your usability requirements
- Identify the technology that your information is dependent on to remain usable. Where are the assets held, and which search tools enable their discovery?
- Identify the risks to the information asset that could arise from changes, for example technology change (changing suppliers, systems and so on) and organisational change (e.g. sharing agreements, who has access to the information)
- Read your agency Information Risk Policy. This should indicate where losses of confidentiality, integrity and availability are likely to have the most critical impacts on your business, and where the greatest proportion of your mitigation should be focused
- Talk to your agency's Information Security Officer and Risk Manager about how the risk policy applies to the information assets you are responsible for.

Get assurance from others

Ensure your IM and IT teams carry out regular digital continuity risk assessments and that they work with you to ensure your continuity requirements are well defined. This will provide you with the assurance that your information assets can be used in the way that you need, for as long as you need.

Your IM and IT teams may also be able to give you some audit data on how your information assets are being used and protected.

Helpful hints

Look at the systems that your information assets are contained in. Here are some risk areas:

- **Databases:** is it easy to know who has access, or to identify what is personal data? Is the management of databases consistent? If your protocols for protecting personal data differ across databases, why is this?
- **Inappropriate access to shared drives:** who has access to information assets on shared drives and why? Do you know what sensitive personal data is held there? Do you have arrangements for protecting it?
- **EDRMS:** are access controls being applied properly and consistently to information assets in your EDRMS?
- **Search capability:** can you find the right information easily in the systems that hold it?
- **Email:** is your email protectively marked? Where are emails stored and how are they protected?

5. Ensure the asset is fully used including responding to access requests

What you need to do

Ensure you are able to use your information assets as appropriate:

- Regularly review whether you could make better use of the information assets you are responsible for
- Manage and approve agreements on sharing personal information between organisations and ensure appropriate access decisions are taken accordingly
- Log access requests from others

How you might do this

- Identify which of the datasets you are responsible for

Get assurance from others

You should get assurance from your RTI officer and managers that they are managing the digital continuity of the information assets you manage – so that you are assured that your information assets can be used in the way that you need for as long as you need. You should also receive and log access requests from others. To do this, you must ensure that a log of access requests is maintained.

Recommended Reading

Information Management *Advice 1 Government employees Responsibilities in Relation to State Records*

Information Management *Advice 32: Implementing Information Security for Information Managers*

Information Management *Advice 34: Implementing Information Security classification in EDRMS*

Information Management *Advice 39: Developing an Information Asset Register*

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

- This advice is largely based on National Archives of UK *The Role of the Information Asset Owner: a Practical Guide.*

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	April 2015	Christine Woods	Template	All
1.0	July 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: July 2013

Ross Latham
State Archivist

Appendix A: Personal Information Protection Principles

There are ten Personal Information Protection Principles contained in Schedule 1 of the Personal Information Protection Act 2004. The following provides a general overview of each.

Principle 1 – Collection

Personal information should only be collected if it is necessary for the organisation's functions or activities, such as providing a service to the individual. It should be collected lawfully and fairly, and preferably, only from the person to whom it relates. Generally, an individual should be made aware that their personal information is being collected and for what purpose it is being collected.

Principle 2 – Use and Disclosure

Personal information should only be used or disclosed for the purpose for which it was collected, or a related purpose that would reasonably be expected. Some important interests, such as protecting health and safety, welfare, or prevention and investigation of crimes, can justify use and disclosure without consent. Otherwise, unless the use or disclosure is required or allowed by law, obtain consent.

Principle 3 – Data Quality

Reasonable steps should be taken to ensure that the personal information held, used or disclosed is accurate, up-to-date, complete and relevant to your functions or activities.

Principle 4 – Data Security

Reasonable steps should be taken:

- to protect the personal information held from misuse, loss, unauthorised access, modification or disclosure.
- to destroy or permanently de-identify personal information longer required. (This provision does not override any requirements of the State Archivist)

Principle 5 – Openness

An organisation must have a document, such as a privacy policy, that explains how personal information is handled.

Principle 6 - Access and Correction

An individual has a general right of access to, and right to correct information an organisation holds about him or her. The Act provides that relevant provisions of the Right to Information Act 2010 (RTI Act) apply when an individual requests access to, or an amendment of, personal information about them held by the organisation.

Principle 7 – Identifiers

Unique identifiers should only be assigned where they are necessary to carry out one or more functions effectively. They should not be shared or used for other identification purposes.

Principle 8 – Anonymity

Wherever it is lawful and practicable, an individual should be able to deal with an organisation anonymously.

Many transactions and services, such as the sale of publications or monitoring of web site usage, do not require the collection of personal information.

Principle 9 – Disclosure of information outside Tasmania

If people's information is passed to other organisations, first make sure equivalent privacy protection will continue to apply to it.

Principle 10 – Sensitive Information

Consent is usually required when collecting sensitive information, such as health status, ethnic background, religion, political views, sexual preference or criminal record.

Appendix B: Principles on the Transfer of Information Responsibilities

Making arrangements for the transfer of information, records and knowledge is a key part of any machinery of government change. However, all too often this aspect is not properly planned for, inadequately resourced and left until it is too late to do everything that needs to be done. Listed below are the eight basic principles that should be followed for a successful transfer.

Reinforce Senior Management Support

Ensure that senior management understand what needs to be done (including setting an appropriate budget) and the risks to the business if the transfer is not carried out successfully. Failure to transfer information and knowledge effectively between agencies can make it impossible to maintain business continuity and can result in the loss of vital information, loss of functionality of digital information, inability to be transparent and accountable and meet legal obligations, inefficiency and substantial additional costs.

Plan in Advance

Start planning for the transfer of information as soon as notification that the agency/function is to be abolished or transferred has been received. Identify desired outcomes – especially the usability of information (or digital continuity requirements after transfer) and test progress against these.

Clarify who is Responsible

Establish as early as possible who is going to do the work and form a team responsible for the transition of the information. Contact TAHO as early as possible in the process for advice. Ensure that transferring and receiving agencies and any contractors employed in information related activities (for example, an IT service partner) have a clear understanding of their separate and joint roles and responsibilities.

Decide what to Transfer

Decide what information needs to be transferred and to where, for example, information of continuing business or legal value will need to be identified and transferred to the agency that is inheriting responsibility for the function/s. Information of archival value may be transferred to TAHO. Refer to Advice 12 on transferring records to TAHO. Consider information/records in all forms, for example, paper files, information within an electronic records management or email system, websites, intranets, shared drives, databases and accompanying information such as finding aids, Information Asset Registers or retention/disposal information.

Make Provision for the Continuity of Digital Information

Define the usability requirements for information to be transferred, and test against them throughout the transfer process. The receiving agency needs to ensure the information can be found, opened, used, understood and trusted as required and will need to ensure it receives both files and necessary contextual metadata and has the technology to enable the usability requirements to be met.

Ensure Continued Compliance with Legislation and Information Security

Clarify responsibilities for Right to Information requests and related complaints and appeals and ensure that handover or guidance notes are prepared. Comply with rules on information security when transferring

information and records and conform to the Information Security Classification Policy Framework for protectively marked material. See DPAC Website. [1]

Capture Knowledge and Communicate to Staff and Stakeholders

Capture the knowledge of staff from the transferring agency, particularly if they are not transferring with the function and make as much information as possible about the changes available to staff in both organisations. Plan communication with customers and end-users.

Take Advantage of Opportunities for Savings and Increased Efficiency

Capitalise on opportunities to increase efficiency and make savings. For example, shared service options could be considered for storage/electronic systems, information that is not required could be deleted rather than transferred.

Further Reading

State Records Guideline 16 Managing inter-agency transfer of personnel records

State Records Guideline 10: Outsourcing of government business: recordkeeping issues

State Records Guideline 14: Privatisation of government business: recordkeeping issues

[1] http://www.egovernment.tas.gov.au/information_security_and_sharing