Information Management Advice 39 Developing an Information Asset Register

Introduction

The amount of information agencies create is continually increasing, and whether your agency is large or small, if you do not understand your information, you cannot fully protect and exploit it. This advice describes a practical process to enable you to understand, assess and document your information and make sure that it supports your business appropriately.

Developing an Information Asset Register (also called conducting an Information review or information inventory) is a useful tool for information managers. Information Asset Registers can be used for many objectives:

- ***to plan the implementation of information security across all information assets in an organisation;***
- ***to identify critical systems for disaster recovery and business continuity;***
- ***for risk analysis;***
- ***to inform digital preservation plans and***
- ***to identify information management strategy priorities.***

Developing this understanding will support you in effectively managing your information assets through change. This advice illustrates how to identify an information asset and provides a step by step process for carrying out an information review.

An information review is a process for identifying and evaluating the ability of your agency's core information assets to meet your business needs. An information asset is information in any format which supports a business process. An information review is the basis for an effective information governance regime.

Helping you manage digital continuity

Although this advice contributes to overall good information management, and can be used to meet a number of different objectives, one of the key objectives it supports is better management of your digital continuity.

Digital continuity is the ability to use your information in the way you need, for as long as you need. Managing digital continuity protects the information you need to do business. This enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, avoid and

reduce costs, and deliver better public services. If you lose information because you haven't managed your digital continuity properly, the consequences can be as serious as those of any other information loss.

Outcomes of an information review

The main outcomes of an information review are:

- Improved understanding of your agency's business
- Improved understanding of the information needs of the business. This includes identification of what information is captured, created or used, who uses it, how effectively it meets the needs of the business and the users, how long it is useful for, and who is responsible for the information assets remaining fit for purpose
- Identification of both strategic and operational opportunities and risks. These may include new opportunities, potential business benefits and efficiencies, information that is being underutilised or areas where insufficient or untrustworthy information is a barrier to efficient business practices or public trust
- Identification of the information assets custodian

Secondary benefits of an information review include:

- Identification of 'silos' of information – information closely held by one part of an organisation, but which has wider uses within an agency. By breaking down those silos and encouraging information to be freely shared within your organisation, the business benefits will be optimised
- Identification of additional information that can be made available to the public
- Assistance in developing information architecture for the agency
- Development of other information-based resources such as controlled document registers required by ISO 9001-based systems
- Although an information review does not include comprehensive or rigorous analysis, it may be useful in developing a records authority

Step 1 Plan your Information Review Project

Project Proposal

You may need to prepare a business case or project brief in accordance with your agency's policies and procedures, and the governance and management arrangements for the review will need to be agreed before commencing. Tasmanian Government Project Management Guidelines include a template for a project plan and this is available from the egovernment web site.[1]

Obtain Management Support

You will need a senior management sponsor or champion who understands the benefits of an information review and is prepared to support the project.

Ensure that the amount of effort in the review is appropriate to your agency. You may consider initially focussing on core business functions or identified areas of risk.

[1] http://www.dpac.tas.gov.au/divisions/egovernment/project_management

Define your Scope

The scope and steps in an information review will vary with the size and complexity of your agency and your information assets. It is important that an information review should:

- focus on the most important business activities and related information assets
- not restrict the scope to a particular format for information (for example, paper or digital)

It may be useful to take a staged approach to conducting the information review by establishing priorities or a sequence of business areas or business processes.

Step 2 Identifying Information Assets

What is an information asset?

In order to understand your information and how to manage and protect it, it is vital to first understand what we mean by the term 'information asset' and how this definition can simplify the process.

> 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 lifecycles.

The key concept here is to group your individual pieces of information into manageable portions; if you had to individually assess every individual file, database entry and piece of data you hold you would likely have a list of millions of items and an impossible task. By grouping items together you can make the task achievable.

An information asset is defined at a level of granularity that allows its constituent parts to be managed usefully as a single unit: too broad and you will not have enough detail, too fine and you will have thousands of assets.

Examples: Information asset
A database of contacts is a clear example of a single information asset. Each entry in the database does not need to be treated individually; the collection of pieces of data can therefore be considered one information asset. All the pieces of information within the asset will have similar risks associated with privacy and storage of personal information.
All files associated with a specific project may be considered a single information asset. This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All the individual items can be gathered together and treated the same as they have similar definable content, and the same value, business risk and lifecycle.
Depending on the size of your organisation, you may be able to treat all the content in your electronic document and records management system as a single asset – but this could be a risk as such a large asset containing varied types of content is likely to be hard to manage.
All the financial data for an organisation could be considered a single asset. There are very specific risks to the business if this information is mismanaged and you may also have an obligation to provide transparency of information, which could be problematic.

Assessing whether something is an Information Asset

To assess whether something is an information asset, ask the following questions:

- Does it have a value to the organisation? Will it cost money to reacquire the information? Would there be legal, reputational or financial repercussions if you couldn't produce the information on request? Would it have an effect on operational efficiency if you could not access the information easily? Would there be consequences of not having this information?
- Is there a risk associated with the information? Is there a risk of losing the information? A risk that the information is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content? Do you understand what it is and what it is for? Does it include all the context associated with the information?
- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Agencies must also take into account that externally sourced information may also be an information asset. External reference material or information provided for context is not considered to be an information asset.

Examples of significant information assets could include:

- Data centres which host agency systems
- Applications used for the delivery of agency services online or through agency offices, or through downstream customer service organisations, etc.
- Applications containing information classified as PROTECTED; or
- Networks that allow:
    1. agency customers, or
    2. agency offices or downstream customer service organisations to access significant agency applications.

Examples of other information assets which may be used to compromise the security of significant information assets are:

- Systems/network management tools which can be used by systems administrators to look at server information, network traffic, application databases, etc.

Review Existing Resources

Your organisation may already have resources you can use to help in this process, for example documentation of previous information audits recorded in an information asset register (IAR), an approved disposal schedule and BCS, technical environment registers, configuration management databases or software asset lists.

By using the older information as a 'baseline' you can tailor your questions to suit. You should investigate these resources and re-use and adapt them wherever possible. However they may only be a very basic foundation to start from, and there will almost certainly be additional information you will need to gather.

Step 3 Design your Data Gathering Instrument

In order to identify an Information Asset you need to conduct an information review of the information your agency holds. An information review is the basis for an effective information governance regime and is a key action identified in the implementation of Information Security Policy.

An Information Review focuses on the value of information as a business asset, rather than on the technology used to capture or manage the information.

When conducting your information review you will gather data by holding focus groups, interviewing key stakeholders or surveying staff. You will need to talk to representatives from all sections of your organisation to ensure you have covered all aspects of your business.

In order to effectively record the information you gather you will need to design an information asset register (IAR) to record the information about each asset.

It is probably easiest to start with very broad definitions and then continue splitting the information grouping up until it is of a suitable size. Draft the questions carefully as responding to questions can be burdensome, and meaningful analysis of the responses can be challenging if questions are not framed with a clear purpose in mind.

If you are from a large agency then it will be necessary to gather your data from across the agency dividing it into its business groupings, for example divisions for each business area. You will need to determine:

- What are the core information assets created or used in each business area?
- Is the information used as input or output of a business process?
- Is the information used in a decision making process?
- Is the information used to evaluate a rule or condition?
- Is the information subject to a typical information lifecycle (plan, create, store, access, use and maintain)?
- Is the information received from an external agency or source and exchanged on a regular basis?

There are information assets which may be used to compromise the security of significant information assets. These must also be identified. A good question to ask is: ‘Could this asset be used to bypass normal security and compromise sensitive information, and what would the impact be?’ If the answer is 'Yes', then this information asset must also be included in the register so the risk to it can be assessed.

There are 5 key areas that you need to gather data about your agencies information assets:

- Asset Information
- People (users and custodians)
- Management
- Usability Requirements
- Technology Requirements

Asset Information

Information to collect includes:

- Asset Name
- Description
- Asset Status (actively used or legacy data)
- Personal Data – Does the asset contain information which will fall under the PIP Act?
- Sensitivity – is the asset protectively marked?
- Creation – original creation date of the asset (or the date it was transferred to the organisation), who created it or where was it transferred from?
- Date IAR Reviewed – the date the entry on the IAR was last reviewed or updated

People

Information to collect includes:

- Information Asset Owner - Who is responsible for maintaining the information asset (who is the custodian of the information)?
- Users - Who creates and uses the information asset?

Management

Information to collect includes:

- ***Business Risk*** - identify risks to the business from the asset, what would be the business impact of losing the asset? What would be the cost of replacing the asset?
- ***Business Value*** - What is the value, business criticality and importance of the information asset?
- ***Purpose*** - What is the business purpose served by the information asset?
- ***Risk to the asset*** – What are the risks to the asset?
- ***Retention Period*** – the period it needs to be kept for and why? These details may be in legislation, standards, policy of the agency
- ***Disposal Requirements*** – how must the asset be disposed of?

Usability Requirements

Once you have identified your information assets, you must determine how you need to use each of them. This covers everything from how you find it, through how you access it to what you do with it. You must also consider any surrounding or supporting information which is important.

For each of these issues you must consider what the requirements are at the moment, and how they might change over time. This will encompass the retention schedules imposed on your assets – how long do you need them for?

These questions also form the core of digital continuity – what usability you need to maintain for your information over time and through change. If you lose the ability to find, open, work with, understand and trust your information in the way that you need, you have lost its digital continuity.

Note it is possible that in defining these requirements you may want or need to re-define your information assets – this may well be an iterative process. If the contents of your asset have dramatically different requirements in any of these areas, you may need to further subdivide your assets.

Information to collect includes:

- ***Find*** - How will you find the information? The granularity and depth of the search required will depend on the type of asset; it may involve finding the asset itself, searching within the asset for files, or searching within those files to find specific pieces of data.
- ***Access*** - Who can access the information and how? These requirements cover not only the security issues around people gaining access to restricted or private information, but also the opportunities for sharing information internally and more widely. Is everything within the asset is protectively marked, only those with the right clearance should be able to open it?
- ***Work with*** - How do you need to be able to work with the information? What do you need to be able to do with the information?
  This is where you define the functionality that you require from your information assets, how you use them and what you need them to do. This area may overlap with the access requirements in that there may be different groups of users who need to access the assets in different ways.
- ***Understand*** - What do you need to be able to understand about the information? This is about understanding the content and context of your information asset. This additional information is not necessarily included within the asset itself but is vital to making the asset usable. The information may be stored digitally as metadata, but it may also be specific knowledge held by individuals, which may involve training or handover procedures if staff change.
- ***Trust*** - To what extent do you need to trust your information is what it claims to be? The level of trust required of an asset will vary considerably. The majority of your assets may well not require any additional validation – they speak for themselves. However for others you may have to prove they have not been tampered with, or to certify them as created on a specific date. These requirements are particularly important because they cover your legal requirements and there may be serious repercussions if they are not fully understood and implemented.

Technology Requirements

- ***Find*** – How will you enable people to find the information in the way you need it? This is both about the technology actually used to search for information and also the technology that is used to store the information.
- ***Access*** - What technologies, configurations and management processes need to be in place for to meet the access requirements?
- ***Work with*** – What hardware and software is required to be able to work with the information?
- ***Understand*** - What technology do you need to provide the 'context' you need to understand it, i.e. to be able to record the required metadata? What systems used to manage the information asset?
- ***Trust*** - What technology is needed to protect the information and to deliver the proof that is required (so that you can trust the information is what it claims to be)?

Appendix 1 includes a template for an information asset register.

The key purpose of the Information Asset Register (IAR) is to document the links between your organisation's information assets and its business requirements. The IAR should be structured so that it is very easy to see what is affected by changes to either of these areas.

In addition to details of how each asset supports your business there are a number of interesting and useful fields which can be recorded for each asset. How many of these you complete may depend on your purpose for developing the register.

The way that you build the IAR will depend on the scale of your objectives and the resources you have available. If you want to register hundreds of assets it may be worth creating or purchasing a software tool to record the information in a database. You should check with your IT team to see if they already have a tool available (for example they may already have a configuration management system which you could input into, or extract a report from). If you have a smaller number of assets, or limited resources, it may be viable to record the information in a spread sheet.

Step 4 Gather Data

Now that you have designed your template for IAR you can then use this tool for interviews, surveys or focus groups. How you gather information from business areas will depend upon the scope of the project i.e. what you want to use the information for and the size of your agency.

Information Custodianship – The Role of the Information Asset Owner

A part of the development of an information asset register is to identify a data custodian for each data asset. This is a critical step as this person will need to be involved in the development of any risk mitigation strategies put in place to protect the asset and any analysis of information held within the asset in order to apply information security classification.

Custodianship (also referred to as information asset custodianship, data custodianship or data stewardship) is a practice of assigning responsibility for data collections or information assets to a designated position or officer: the 'custodian'. The custodian is responsible for ensuring that the collection or asset is managed appropriately over its lifecycle, in accordance with rules set by the information owner. These responsibilities may relate to:

- ***Quality***, including ensuring that appropriate data and metadata is captured, and the quality and integrity of the data
- ***Access***, ensuring that the data is available internally and externally as appropriate, considering security, privacy and intellectual property/licensing considerations and interoperability requirements
- ***Accountability***, including ensuring compliance with any relevant legislation, standards and policies

The owner of the asset (the IAO) is responsible for making sure the asset is meeting its requirements, and that risks and opportunities are monitored. The owner need not be the creator, or even the primary user of the asset, but they must have a good understanding of what the business needs from the asset, and how the asset needs to be able to fulfil those requirements. The IAO is often a subject matter expert, or 'owner' of the relevant business process, for a particular information collection or asset.

Classification of information assets

There are a range of classification schemes that can be applied to information assets. Classifications can increase accessibility and re-useability of information assets, and there may be several classification schemes that need to be applied depending on the intent of the classification scheme. Classification assists with identifying the scope, types, use and functions of an agency's information assets. Classification of information assets to a scheme should be done consistently throughout all business areas within an agency. Some common classification schemes include:

- Tasmanian Government Information Security Classification Framework
- TAHO Guidelines and Advice
- ANZLIC Metadata Standards

How to Group your Information

Information assets should be grouped and considered depending on their business needs not on their technology requirements. Each asset may contain individual items that need different technology solutions to address the same business need.

It may be that a piece of information could logically belong within two different assets, however this can lead to conflicts of ownership and control, so ideally each piece of information should only be included within in a single asset. However assets can reference other assets and care should be taken to manage these potentially complex relationships.

Assets can contain other assets – as you introduce more and more granularity, it may be useful to retain the sense of the high-level assets. Your organisation must define clear rules about how the management and retention schedules of these assets operate at these different levels.

The groupings of information within assets may change over time. For example, you may have an asset which contains all the items archived into long term storage, therefore other pieces of information will be added into this asset over time.

This can be a complicated process, but done properly can be of real, lasting benefit to your agency. There is no right or wrong way to group your assets. The key point to remember is that you are doing all of this within the scope defined by your objectives and if the list you produce is consistent and relevant, then it meets your objectives.

Step 5 Analyse Your Data

When analysing the data, develop a list of significant information assets. You should be able to identify your agency's information assets and the strengths and weaknesses of that information to support your business. Issues need to be prioritised against organisational performance and risk, as well as the likely cost and time to address the issues.

You should be able to identify information assets that are suitable for inclusion in an information asset register. This register can be used:

- as part of ongoing governance of information assets by identifying them, their purpose and who is responsible for them
- to identify important and valuable information assets required for business continuity
- Identify and analyse the risks to the significant information assets. The threats to each of the significant information assets then inform the identification, analysis, and evaluation of risks

Step 6 Report your Finding

When documenting the findings of the review you should not only complete the IAR for each asset , you should highlight the strengths and weaknesses of each information asset and which business processes the information supports.

Potential weaknesses of information assets include those that:

- have been identified as inadequate for the business purpose
- are a source of frustration for people using or managing them
- are unavailable to those with a legitimate need

- do not appear to serve a purpose, are underutilised, or
- appear to be duplicated.

These can be documented in a separate report for your senior management. Your report should outline the key issues identified and an overview of the significance and status of each. Recommendations for further projects or action should be based on the reporting framework that is in use in your agency.

The development and use of an information asset register will ensure that agency information is identified, defined and organised in a way that will facilitate access to and reuse of this information. Information asset registers will provide custodians with an overview of the information assets under their care. The register will help to avoid unnecessary duplication of information through collection or acquisition.

Depending on the extent of information already gathered, agencies may wish to extend existing agency registers, rather than duplicating information in a separate custodianship register. However, agencies should ensure that the ownership and custodianship details of an information asset are consistent across all registries which contain that information asset. Agencies should also consider any legacy information assets that require ongoing maintenance.

Step 7 Maintaining and updating the IAR

Business processes are always changing. You should regularly review the status of your core information assets and update your information asset register at least bi-annually. This will ensure the currency of the data gathered, as well as the being able to amend or update your recommendations to reflect any changes or developments in your agency's core business.

You should define a permanent owner of the IAR itself (as opposed to information assets described within it) and a maintenance schedule. This will assist in ensuring that the information assets identified in the register are appropriately recorded, stored and maintained, and are accurate and not unnecessarily duplicated.

Agencies should consider the overlaps between information custodianship processes and the agency's program management and project management methodologies, and business process improvement initiatives to ensure that the currency of information assets is maintained. For example, a project may need to update the agency's information asset register and their associated owners/custodians due to the implementation of business processes and systems which create or use new information assets.

When using IARs, it is important to realise they will have an effect beyond the confines of your own organisation. People doing work for your organisation will need to be aware of the IAR, the effect their work has on the IAR and how they will need to interact with the IAR. This could be external personnel working with your data or could be external personnel looking after some of your infrastructure, such as outsourced IT teams.

Step 8 Possible Next Steps

The IAR provides you with a comprehensive list of the assets that are important to your organisation within the scope of the objectives you have outlined for this investigation. It may be a list of a hundred assets covering your entire organisation, or it may be just a few assets that will be affected by a change you are planning for. Each entry on the register will have all the additional information about the asset that is required to understand how it should be managed so that it delivers the use that the business requires from it.

There are a number of ways you can use this register to identify risks, exploit opportunities and manage change. You should return to your original objectives and take the corresponding next steps.

Map to Technology Dependencies

For each information asset it is now possible to assess what technology is required to meet the relevant business needs. This will also allow you to understand the potential impact of change on your assets, and to make informed decisions about where to prioritise investment in ensuring the continued usability of your information. It should also highlight where savings can be made by not maintaining technical support unnecessarily. This should be done in conjunction with the IT department.

Understand your Information Management Requirements

Alongside having the right technical tools to support your information requirements, there are likely to be information management processes which need to support the delivery of the requirements. This may mean introducing, updating and enforcing metadata or security policies, or providing relevant training and guidance on how and where to store files.

Identify and Mitigate Risks

Information assets have risks associated with them, risks from losing the assets, having them fall into the wrong hands, getting corrupted or any number of other issues. By considering these risks you will hopefully be able to mitigate against them and form contingency plans. You may need to escalate these risks to appear on departmental or corporate risk registers.

Identify Opportunities for Disposal, Exploitation, Savings and Efficiencies

In assessing the business requirements for your information assets, you may have uncovered assets which are no longer actually required and action should be taken to dispose of these. You may also have found that some information assets are only needed very rarely and could therefore be moved to cheaper long-term storage which is less instantly accessible.

If you have identified assets that can, or should be shared, you can begin the process of allowing and promoting this access.

Manage change

Now that you have a comprehensive assessment of your current information assets and their requirements you are in a much better place to assess how any change may affect them. These changes could be to the assets themselves, how they are managed, the technology supporting them; or the business requirements driving them.

For specific changes you will be able to build impact and risk assessments allowing you to mitigating action and plan contingencies. You can also use this information to improve your change management process to make all future change planning better. It is important to remember that you must embed the management of the IAR itself within your change processes – if the IAR is not kept up to date through change it becomes redundant and misleading.

Further Advice

The method of conducting an information review outlined in this advice is one way of proceeding. There may be other methods more suitable to your circumstances. There is no agreed 'best practice' method, but the method should be scalable and should be adapted to meet the needs of your agency. 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

- National Archives of Australia Conducting an Information Review
- Victorian Government Information Security Management Framework Guideline
- Public Records Brief - Custody and Ownership of Public Records and Information Asset Custodianship Queensland State Archives
- Queensland government chief information officeIS44 implementation advice
- The National Archives of UK Information Assets and Business Requirements

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	May 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

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

Issued: May 2013

Ross Latham
State Archivist

Attachment 1: Information Asset Register Template

Information Asset Register (IAR)	
Asset Information	
Asset Name	A simple way to identify the asset
Description	Brief description of what the asset is Detail on what the components of the asset are
Asset Status	Is this asset being actively updated? Has the asset been closed, what date was it closed?
Personal Data	Does the asset contain information which fall under The Personal Information Protection Act?
Sensitivity	Is the asset protectively marked?
Creation	Original creation date of asset, or date it was transferred into the organisation. Who created it, or who was it transferred from?
Date IAR reviewed	The date this entry on the IAR was last reviewed or updated
People	
IAO	Who is the Information Asset Owner?
Users	Who are the departments and third parties who use or access the asset?
Management	
Business Risk	Risks to the business FROM the asset? What would be the business impact of losing the asset? What would be the cost of replacing the information?
Business value	What is the value of the asset to the business, both the financial value and the use it delivers to the business?
Risk to the asset	What are the risks to the asset?
Retention period	The period it needs to be kept for and why
Disposal requirements	How must the asset be disposed of?
Usability requirements	
Find	How will you find the information? The granularity and depth of the search required will depend on the type of asset; it may involve finding the asset itself , searching within the asset for files, or searching within those files to find specific pieces of data
Access	Who can access the information and how? These requirements cover not only the security issues around people gaining access to restricted or private information, but also the opportunities for sharing information internally and more widely.