

Information Governance

Guideline

Version: 1

Date Finalised: 21/04/2023

Date for Review: 21/12/2025

STATE RECORDS
of South Australia



Government of South Australia
State Records

Table of Contents

i. Introduction	2
ii. Information Management Program	4
1. Information Asset Audit	6
2. Value and Risk Assessment	9
3. Information Management Plan	18
3.1 Policy and Procedure	20
3.2 Resources, Roles and Responsibilities	23
3.3 Access and Release Schemes.....	28
3.4 Privacy Protection and Considerations.....	33
3.5 Security Controls.....	36
3.6 Disposal.....	42
3.7 Compliant Systems	50
4. Education.....	54
5. Self-assessment and Reporting	58
Glossary	60
Relevant Documents.....	62

i. Introduction

Purpose and scope

The Information Governance Guideline (Guideline) has been developed to support agencies in meeting their information keeping requirements under the State Records Act 1997 (SR Act).

It applies to all agencies as defined in section 3(1) of the SR Act, and to the information assets of those agencies.

In this Guideline, the term 'information asset' incorporates the definition of official record as defined by section 3(1) of the SR Act, and includes information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

This Guideline will assist with the development and implementation of an Information Management Program, as prescribed in the Information Management Standard (Standard). It will also provide direction on how to improve an existing Information Management Program. It expands upon the behaviours underpinning the Standard, offering guidance on the necessary structure and rigor to manage information assets now and into the future. It also offers advice to assist in compliance with other standards issued under section 14 of the SR Act, and other advice provided by State Records.

South Australian Information Management

The governance of information for South Australian State and Local Government agencies and Universities is established in the Information Management Strategy (Strategy) and the Standard.

The Strategy establishes the principles that must be followed to ensure information assets can be relied upon and trusted.

The Standard expands on these principles by outlining expected behaviours required to effectively manage information assets, to achieve business objectives and to meet legislative and policy obligations.

These expected behaviours can be achieved through the implementation of an Information Management Program (Program). You can assess your Program's compliance and current information management practices against the Standard using the Self-Assessment Tool (Tool) developed by State Records. The results of the Tool provide an indicative assessment of your agency's overall information governance maturity and capability, highlighting Program elements to focus on to ensure compliance with, and improvement against, the Standard.

Implementation of this Guideline

This Guideline does not need to be read in any particular order. You can choose to focus on priority information management areas already identified as needing improvement or carrying particular risk, such as ensuring business systems are compliant.

It can be applied to:

- » one or more components of information governance, such as security controls, privacy protection and considerations or disposal
- » any function or business process, including one that may span more than one business unit
- » single business units or the whole agency
- » any agency, regardless of size.

Sections 1-5 are in typical order of action but there is flexibility in how you might undertake them. For example:

- » some elements may already be in place and only require review
- » some elements can be undertaken simultaneously
- » risk or regulatory requirements may dictate a focus on one specific element.

This Guideline may be used by any staff responsible for defining and / or implementing information management processes or systems. This includes records and information managers, Information and Communication Technology (ICT) staff, or risk and compliance managers who are involved in advising or assisting in process or system implementation.

This Guideline is to be used in conjunction with the Standard and the Tool.

It should also be read in conjunction with the following Standards:

- » Appraisal
- » Contracting and Information Assets
- » Disposal
- » Managing Digital Records in Systems
- » Minimum Recordkeeping Metadata Requirements
- » Management and Storage of Temporary Value Information Assets
- » Transfer of Official Records.

These Standards can be found on [State Records Information Management Strategy and Standards webpage](#).

ii. Information Management Program

The Standard prescribes the required elements for a information management governance model, described here as a Program. The relevant components of the Program are outlined below:



Collectively, these elements will assist to develop a clear strategic direction for the management of information assets as well as foster a good information management culture with a view towards continuous improvement.

A Program should support broader strategic and corporate goals and objectives, carrying the same executive level commitment.

There are a number of steps to follow to develop and implement a Program:



1. Information Asset Audit

Undertake an information asset audit to identify what information assets your agency holds. The identified information assets must be linked back to the business activities and functions.



2. Value and Risk Assessment

Assess and value what information assets should be created to support your agency's business and regulatory requirements. To do this, consider legal and regulatory requirements, associated risks and business objectives. Identify and manage risks associated with not creating information assets to support requirements. This can be achieved by undertaking a value and risk assessment.



3. Information Management Plan

An Information Management Plan (Plan) provides practical direction for implementing a Program. The Plan should be based on the outcomes of the information asset audit and value and risk assessment and identify information priorities.



4. Education

Induct and train staff on the Program. A large part of the success of a Program relies on the commitment of staff to information management policies and procedures and an awareness of their information management responsibilities.

Educating staff in the value and management of information is key to fostering a culture of good information management (Principle 1 of the Standard).



5. Self-assessment and Reporting

Continue to formally assess and review the Program using the Tool. This assessment can also assist your agency to understand gaps in your Program and can be used as a first step in the review of the Program.

1. Information Asset Audit

Relationship to the Information Management Standard

To implement the principles and behaviours in the Standard, identify what information assets your agency holds (Behaviour 1.1) as well as how those information assets relate to business functions and activities (Behaviour 1.3).

This will ensure your agency is making and keeping full and accurate information assets appropriate to your business processes, regulatory environment and risk and accountability requirements (Behaviour 4.1).

Behaviour 1.1 be met by conducting an information asset audit.

1.1 What is an Information Asset Audit?

An information asset audit is a survey to identify what information assets exist and to evaluate how these assets support business requirements. This is different from appraisal which is the process of deciding what information assets should be made and kept, based on a value and risk assessment.

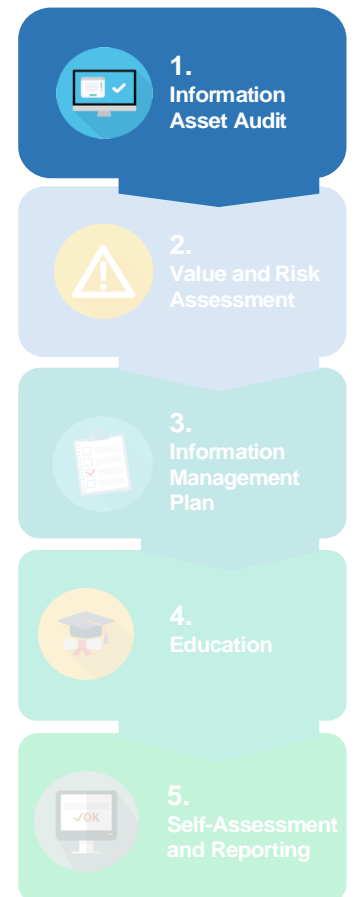
One of the purposes of conducting an information asset audit is to compile a comprehensive information asset register (asset register). An asset register identifies what information resources exist across your agency and provides stakeholders with an overview of the information assets under your agency's control.

1.2 Conducting an Information Asset Audit

Preparation

Before conducting an information asset audit:

- ✓ **Determine the scope of the audit**, for example prioritise core business functions, business-critical assets (such as assets which hold information vital to the survival of your agency, or without which your agency could not operate), high-profile work units, identified areas of risk or agency-wide.
- ✓ **Determine how it will be conducted**, such as through interviews and focus groups, business unit staff completing a questionnaire or business units completing a proforma asset register.
- ✓ **Determine how to identify an information asset**. An information asset is not usually a single item. It should be recognisable to the business users as an identifiable collection of data, where a collection is a set of like or related information. For example, personnel files, a contracts database, customer management data, a group of policies and procedures, or in the case of single items an asset register, complaints register or a password register.



Applications, such as an EDRMS, that collect, manage or store information are not legally considered information assets. However, the information they contain is. For information security purposes, applications might be treated as an information asset, as the software itself requires protection.

A single system may hold multiple types of information assets. For example, a single system in a Council may have modules for rates, accounting, property, etc., all of which are separate information assets.

- ✓ **Check relevant sources to locate existing information assets**, such as:
 - » previous information audits, including information security audits
 - » recordkeeping systems including registers of repositories for physical storage such as agency-run storage facilities, Approved Service Providers (ASP) or State Records
 - » information sharing agreements including Memoranda of Understanding (MOUs) and contracts
 - » approved operational Records Disposal Schedules (RDS)
 - » ICT technical environment lists and systems registers
 - » Cyber security information asset registers required by the South Australian Cyber Security Framework (SACSF)
 - » lists of information required to be reported externally and internally.
- ✓ **Prepare initial list of people / business units to approach**, such as staff who may be able to help identify and value information assets.

Conduct the Information Asset Audit

An information asset audit can be conducted by:

- » reviewing the documentation you obtained from your research of relevant sources
- » interviewing selected staff to obtain information asset profiles
- » sighting information assets and / or systems where required
- » acquiring any additional documentation relating to information assets and / or systems.

It is recommended the audit be conducted by a staff member / s with information management experience and corporate knowledge in consultation with other relevant areas, such as ICT and governance.

- ✓ **Record and collate data** into an asset register and analyse results. Create the asset register in a format such as a spreadsheet which enables data to be extracted for analysis, reporting or other purposes. Fields may include:
 - » type of record
 - » description
 - » business owner
 - » start date, and end date for legacy systems
 - » format (including copies)

- » location of the information (physical, digital, onsite, with a third party provider (within Australia or offshore))
 - » legislative or contractual context
 - » system context, including interdependencies or previous migrations
 - » disposal coverage
 - » business value and criticality (refer to Values and Risk Assessment)
 - » confidentiality, integrity and availability requirements
 - » risks.
- ✓ **Review and finalise the asset register.** This can be done by asking the nominated staff to review and validate the list relating to their business unit, or provide further information as required.

Note: Your agency may already have an existing register that references some or all of your agency's information assets, such as a Cyber Security Information Asset Register. Where a register already exists, it is recommended these registers be combined, if possible and appropriate, or at least be linked to one another.

- ✓ **Plan to review the asset register** both routinely and as more information assets are created, found or discontinued. A review should also be conducted when systems, software and media are upgraded or become obsolete.

1.3 Outcomes of an Information Asset Audit

The information asset audit will produce an asset register that will enable a clear understanding of what information assets are held. The asset register will form part of the value and risk assessment you will need to complete to inform the value of the information assets your agency holds.

2. Value and Risk Assessment

Relationship to the Information Management Standard

Information assets must be managed appropriately. To do this, it is vital to understand how your agency's information assets support the business objectives and operations, including compliance obligations (Behaviour 1.2). This helps determine their value. Linking information assets back to your agency's business functions and activities will enable this understanding (Behaviour 1.3).

In addition to the information assets identified through the audit, your agency also needs to analyse and document the information your agency needs to create to meet legal and operational obligations (Behaviour 2.1).

Further, all information assets created must be:

- » complete and accurate
- » appropriate to your agency's business processes, regulation environment and risk and accountability requirements.

A value and risk assessment can then be conducted to meet these behaviours in accordance with your agency's risk management framework.

Risks associated with not creating the required information must also be identified and managed (Behaviour 2.3).

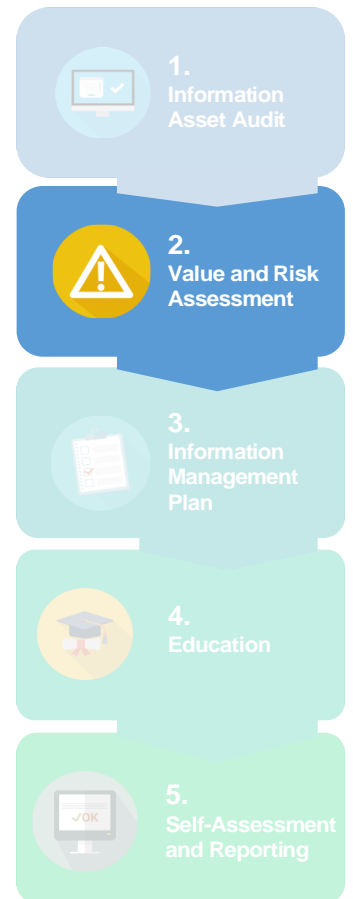
2.1 Why assess value and risk?

By knowing what information assets are held it is possible to assess the value of those assets, the risks to them and any action that might be needed to manage and protect them. There will then be an understanding of how these information assets support business objectives, as well as your operations and compliance obligations.

Assessing value and risk relies on a good understanding of your agency's external and internal context. External and internal context can be determined through a business and regulatory analysis.

Examine:

- » external context including: regulatory requirements, political and societal influences, economic environment, technological and physical environment, and contractual relationships. **Note:** information assets that may not be of high value to your agency but may be to the State of South Australia and need to be permanently retained



- » internal context including: governance and organisational structure, policies, objectives and strategies, resources, capabilities or knowledge, decision-making processes, technological environment, standards and guidelines adopted by your agency, and contractual relationships.

This includes the business context in which the information assets are being created and used and any governance arrangements in place addressing the management (both administrative and regulatory), and registration of its information.

Understanding your agency's organisational, accountability and regulatory requirements means priorities can be determined based on objective data, which in turn enables planning of information related actions and justifiable allocation of resources.

2.2 How to determine the value of information

'Value' is the level to which something is held to be important, worthy, or useful. In relation to information assets, 'value' can mean a monetary amount but also includes the value the asset has in its business, legal, political or social context.

There are two angles from which to value an information asset under the SR Act:

- » its present importance to your agency, the government and the community, acknowledging this might change over time
- » its ongoing value to the State as an authoritative source of evidence, summary of substantive decisions or actions, or aesthetic or historical significance (which would be deemed to be permanent under the Appraisal Standard).

High value information assets are those that enable the performance of your agency's functions, to provide services and may be of permanent value either to your agency, government and / or wider society.

Information assets with an active business value, but not necessarily of permanent value, are critical in enabling your agency to:

- » undertake and continue your functions
- » make good decisions
- » service your clients / customers
- » maintain or enhance your reputation
- » respond to commissions, inquiries, audits, investigations and legal issues.

State Records' Appraisal Standard outlines the criteria for determining information assets of permanent value to the South Australian government.

Note: Regardless of the value of an information asset, it cannot be disposed of unless authorised under a current disposal schedule and any disposal action must be part of an authorised information management program and with the authority of the appropriate information management practitioner.

Deciding information assets to make or keep

The process of deciding what information assets should be made and kept, based on value and risk, is known as appraisal (refer to the Appraisal Standard). This is different from an information asset audit which records what information assets your agency has, not what it should be creating or keeping.

Appraisal is achieved by:

- » gathering information about the relevant business activity or process, including the people involved in the process (customers, clients, citizens, etc)
- » analysing the broader legislative, political and social context of the business
- » documenting the value and risk assessment to communicate and account for decisions.

Consider the following sources to help identify your agency's information needs:

- » legislation and regulations
- » business activities and functions (for example services provided to customers)
- » industry and State Records standards
- » government policies and procedures
- » audit reports (for example Auditor-General, other external or internal audit reports conducted on, and or by, your agency)
- » business impact assessments
- » Ombudsman reports
- » Royal Commission reports or relevant inquiries or reviews
- » MOUs
- » community and customer expectations.

These sources articulate specific information assets to be created, kept or provided. For example, under Regulation 425 of the *Work Health and Safety Regulations 2012*, your agency must create and maintain an asbestos register.

Where information requirements are not clear in legislation or regulations, it may be necessary to seek legal advice. For more information on appraisal refer to State Records' Appraisal Standard or *ISO TR 21946 Information and documentation – Appraisal for Managing Records*.

Note: your agency must identify and include, in any contracts with third party providers who provide services on behalf of the government, any legal requirements to create and keep information assets. Refer to the Contracting and information Assets Standard (Contracting Standard) on the State Records website for more information.

Business classification

Once your agency's information requirements (what it should be creating) have been identified, these should be linked back to business functions and activities (Behaviour 1.3). This can be documented using a classification scheme. A classification scheme applies a uniform hierarchical set of terms and conventions to classify, title and retrieve information assets.

Benefits of classification include:

- » consistency in the description of information assets
- » documenting the link between information assets and business activities and functions
- » documenting access and security decisions (for state government agencies these decisions must be made and documented in accordance with the South Australian Protective Security Framework (SAPSF) and SACSf)
- » improving the accuracy and ease of retrieval
- » assisting in sentencing and disposal of information assets.

Note: There may be information assets that you are unable to link to your current functions and activities, for example information assets of defunct or predecessor agencies. For the management of these records, please contact State Records.

Gap analysis

Once your agency's information requirements have been identified this can be compared against the information your agency already creates.

Gaps, as risks, can be added to an information assets risk assessment, to be managed and mitigated.

2.3 Value changes over time

The value of most information assets will change over time. How the value of an information asset changes over time will depend on several factors, including the potential use of an information asset beyond its original purpose, your agency's organisational, accountability and regulatory requirements and potential societal changes. For example:

- » high value information assets may decline as the risk for your agency and the community passes. For example, a contract is high value while it is active, then decreases in value after the contract has finished but it still holds some value in case of any recourse. It then becomes of low or no value once the time has expired for recourse. The value scale will depend on what the contract is for. Contracts for major building works would have a longer value over time in comparison with a short-term cleaning contract.
- » permanent value information assets, either to your agency or the State, may retain their high value indefinitely, even as their use changes. For example, school registers or hospital admissions are high value to particular agencies as evidence of the delivery of services. Over time, these registers offer evidence of family relocations and familial or societal health trends.
- » information assets of little or low value to the business may become high value to the community. For example, an agency visitor sign-in sheet needed for security or safety on a given day may become relevant in an Inquiry as evidence of who was on site on a particular time or date.
- » evidence needed for reporting diminishes once reports have been made. For example, accounting spreadsheets might have medium value for a finite period then reduce to low or no value once regulatory requirements have been met. They may be duplicated for future reporting cycles but are only for reference. If they were lost, the impact would be low.

2.4 How to assess level of risk

'Risk' is the effect of uncertainty. It is a deviation from the expected, which can be positive or negative.

Risks are analysed in terms of potential events, the likelihood of those events and the consequences of those events both internally and externally.

Note: All risks to your agency should be identified, assessed and managed according to your agency's risk management framework and risk management processes.

For more information on risk assessments refer to your agency's risk management policies or the *ISO TR 21946 Information and documentation – Appraisal for Managing Records*.

Types of risk

While there are many different types of risk to your agency, the two information-related risks are:

- » **business risk:** not having, or not being able to find, the information needed to meet your agency's obligations or the inappropriate disclosure of information through inadequate security or privacy management. For example, staff employment agreements are visible to a range of unauthorised staff within a corporate records management system, or documentation of a major tender process is not available to query a breach of contract. These risks can be mitigated by having an information asset register and knowing your agency's information requirements
- » **risk to the information assets themselves:** through inadvertent deletion, poor physical storage, incident / disaster, theft, ransomware or other cyber attacks, inadequate digital backup, or corruption.

Identification of potential events

Any risk event or circumstance that could affect business objectives and compliance obligations needs to be identified.

Initially this can be done based on past failures and successes, customer complaints, legal matters your agency has been involved in, reports, historical research or other events.

The causes and sources of the risk can also be discovered through questionnaires, interviews, review of complaints received, workshops, examples from other agencies or testing scenarios.

In assessing the level of risk to an information asset or assets, consider:

- » what is the impact or consequence on the business of information not existing, or being unable to be found when required?
- » what is the likelihood of the information being needed for any purpose?
- » does this likelihood diminish over time?
- » does the impact, effect and cost of remediation reduce over time?

- » what are the physical or digital risks to the information assets themselves?

Table 1 provides some examples of risks to information assets.

Table 1: Risk examples

Potential source of risk	Examples
Changes in the external environment	<ul style="list-style-type: none"> » regulatory » technological » physical environment (such as weather events (for example fire or floods), building damage, vermin) » external security threats (such as theft, cyber-attack) » stakeholder expectations
Changes in the internal environment	<ul style="list-style-type: none"> » organisational » technological » corporate capability and expertise » financial and material resourcing » internal security threats (such as fraud, inadvertent data breach, or sabotage)
Adequacy of the systems that manage information assets	<ul style="list-style-type: none"> » system design and documentation » system support » maintenance » sustainability » interoperability with related systems » backups of data and information » cyber security
Processes for managing the information assets	<ul style="list-style-type: none"> » definition of requirements » steps to create and capture relevant information assets » quality of metadata capture » managed access and use » maintained usability » management of migration » retention and / or disposal

Likelihood of the event

Once the potential event is known, consider the expected likelihood (probability or frequency) of that event occurring. For example, is a system outage a rare occurrence,

or does it happen regularly? Are physical security breaches increasing around the offsite storage or transport of hardcopy information?

Likelihood is usually quantified on a scale, ranging from ‘remote’ likelihood to ‘almost certain’.

Each risk should be assessed in terms of the likelihood of an event happening and the consequence if it does happen.

Potential consequences and impact

Poor information management results in:

- » loss of evidence of a business transition or decision because it was never created or retained
- » information assets being lost or damaged, destroyed, incomplete or inaccessible
- » unauthorised access, breaching security and privacy
- » altered information which is unable to be trusted.

These results might have an impact on business objectives and compliance requirements.

Table 2 expands on the potential consequences of poor information management.

Table 2: Potential consequences

Potential consequence	Examples of impact
Ethical	<ul style="list-style-type: none"> » corporate social responsibility at risk or damaged » loss of trust in government services » poor governance and compliance
Cultural	<ul style="list-style-type: none"> » change in community expectations and tone of engagement
Legal	<ul style="list-style-type: none"> » failure to comply with legislative obligations » breach of contractual obligations » failure to meet business objectives
Social	<ul style="list-style-type: none"> » labour issues » human rights issues » public health issues » political uncertainty
Reputational	<ul style="list-style-type: none"> » poor / unreasonable stakeholder expectations
Environmental	<ul style="list-style-type: none"> » pollution

Potential consequence	Examples of impact
Financial	<ul style="list-style-type: none"> » reduction in revenue » negative budgetary implications » reduction in assets » increase in debt

Note: Agencies must formally notify State Records of any lost or misplaced information assets as soon as possible after an incident has occurred. For more information refer to State Records website at <https://archives.sa.gov.au>.

Rating the risks

One example of a consequence / likelihood matrix is below using a five-point likelihood scale and a four-point consequence scale.

Placing a risk event in any of the squares determines its significance and therefore the urgency for action to address the risk.

For example, an external cyber infiltration event may result in information being lost or compromised. This could halt some operations and expose other systems to disruption. This event’s likelihood is ‘possible’ but has ‘high’ consequences. The risk therefore falls into a category of ‘high’ significance and urgency for action.

Like value, the level of risk can change over time, so a risk assessment should be revisited periodically to ensure that risk mitigation measures remain fit for purpose.

Table 3: Example four-point consequence scale

LIKELIHOOD				
Almost certain	Medium	High	Significant	Significant
Likely	Medium	High	High	Significant
Possible	Low	Medium	High	High
Unlikely	Low	Medium	Medium	High
Remote	Low	Low	Medium	Medium
	Low	Medium	High	Significant
	CONSEQUENCE OR IMPACT			

All risks should be recorded as part of your agency’s risk management program, whether in a separate information risk register or within a general agency-wide risk register or program.

2.5 Outcomes from assessing value and risk

Identifying information assets that are of high value and / or are at high risk enables priorities to be determined, strategies and plans to be developed and resources to be allocated accordingly.

Using a value-risk matrix can give an indication of where to assign priorities for risk treatment or mitigation.

Table 4: Example value-risk matrix

VALUE				
High	Medium	Medium	High	Vital
Medium	Low	Medium	Medium	High
Low	Low	Low	Medium	Medium
	Low	Medium	High	Significant
				RISK

These priorities will form the foundation of the Information Management Plan by enabling your agency to:

- » identify and manage associated risks of not creating or managing information required for business activities and compliance
- » prioritise efforts or resourcing
- » help meet compliance with regulatory requirements for information assets (such as the SR Act, *Freedom of Information Act 1991* (FOI Act), *Public Sector (Data Sharing) Act 2016* (Data Sharing Act), open access directives, etc)
- » determine protection measures for information as required to maintain the security, confidentiality, privacy, integrity and availability of the information assets, including the assignment of physical, personnel, digital and information classification controls
- » develop business continuity programs and incident recovery plans
- » support the development of a disposal schedule
- » develop strategies and prioritise investment to ensure information assets remain in a usable and readable format for as long as required (for example through preservation or mitigation)
- » identify any 'silos' of information and decide what (if any) action to take. For example locating the information asset elsewhere, opening access to other areas of your agency, other areas of government or the public
- » identify where using existing information assets can be used to a greater extent, to reduce duplication of systems or effort
- » develop mechanisms for greater discoverability to support, for example, subpoena and other legal discovery processes.

3. Information Management Plan

Relationship to the Information Management Standard

As with any government asset, it is important that the management of information assets is planned at the agency-wide level. This is done through a Plan.

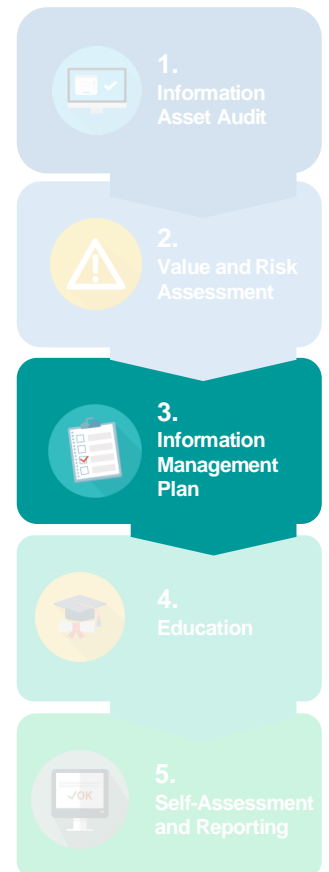
The Plan is a key element of the Program.

The Plan provides practical direction for implementing elements of the Program and meeting the [Information Management Policy](#).

The outcomes of both the information asset audit and the value and risk assessment form the foundation of the Plan. The Standard offers a range of behaviours to apply in your agency's context.

To develop the Plan, you will need to know which:

- » [policies and procedures](#) are required to support the information management priorities, as well as to manage information assets in general (Behaviour 2.2)
- » information resources your agency has or requires
- » information management [roles and responsibilities](#) are required
- » [access and discovery schemes](#) are applicable to your agency, through which information can be requested and / or shared, and how these are to be managed (Behaviours 5.7 and 5.8)
- » [privacy considerations](#) and controls your agency has, or requires, to ensure personal information is properly managed. This includes the collection, storage, access, correction, use and disclosure of personal information (Behaviour 5.6)
- » [security and business controls](#) your agency has, or requires, to ensure information remains accessible, available, managed and shared and can be relied upon for as long as it is needed (Behaviours 2.5, 4.5, 5.1 and 5.2)
- » [disposal program](#) your agency has, or requires, to ensure information assets are disposed of in an authorised and timely manner once all business, legal and accountability requirements have been met (Behaviours 2.7, 5.4, 5.5 and 5.9)
- » systems your agency has, or needs, to meet information management requirements to ensure the quality and authenticity of information and comply with the Managing Digital Records in Systems Standard and the Minimum Recordkeeping Metadata Requirements Standard (Behaviours 2.5, 2.6, 4.2, 4.3, 5.2 and 5.3).



Scope and content of the Plan

It is recommended that your agency has one Plan. However, detailed project plans can be developed for the various projects and initiatives outlined in the Plan.

The Plan can contain short and long-term actions.

At a minimum the Plan should cover:

- » Responsibilities
Outlining the overall responsibility for leading and monitoring implementation of the Plan and reporting on progress, as well as responsibilities for ensuring that specific actions are implemented and progress is reported
- » Tasks and Timeframes
The measurable tasks needed to achieve the objectives of the Program and the prioritised actions identified based on the value and risk analysis. These are likely to include:
 - policy and procedure development
 - access schemes
 - privacy measures
 - security measures
 - retention and disposal program
 - compliance of systems that hold information
 - education and training of staff
- » Resources
Defining what resources are needed to meet the actions, including funding, staffing and technical systems
- » Consultation
Identification of where consultation and interaction are required with other areas of your agency, such as ICT, security, business areas and senior management
- » Monitoring, assessment and reporting

Review the Plan

Progress against the Plan should be assessed and reported on a regular basis.

The Plan should be reviewed annually or as part of the self-assessment tool process to:

- » change or update the scope or timing on tasks as your agency's information governance maturity and capability improves and past Plan actions are completed
- » delete or add new tasks or projects
- » ensure it takes into account any changes in an external or internal context that affect the actions required under the Program and associated policies. For example a change in legislation might affect your agency's privacy or data security framework or data sharing arrangements
- » ensure it addresses any gaps in the Program and its overall compliance with the Standard.

3.1 Policy and Procedure

Relationship to the Information Management Standard

Information Management policies and procedures are the formal mechanisms outlining how information management priorities will be supported by your agency, including how information will be created and managed, appropriate to risk, specific to your agency's context (Behaviour 2.2).

Your agency should have a clear strategic vision of its own information management values and practices. This will assist in fostering an organisational culture that values and manages information as an asset and supports business objectives and activities (Behaviour 1.5).

All staff should be inducted and trained in information management policies and procedures (Behaviour 1.4). Staff adherence to the information management policies must be monitored and addressed as required (Behaviour 2.9).

Policies and procedures should be regularly reviewed to ensure they continue to support your agency's business and information requirements (Behaviour 2.8).

3.1.1 Information Management Policy

Develop the Information Management Policy (Policy) as a high-level set of requirements to be implemented according to the scale and complexity of your agency or business function, and the level of risk. It should contain objectives that reflect the principles and behaviours in the Standard as well as address your agency's information requirements (Behaviour 2.2).

An Information Management Policy:

- » takes an agency-wide approach. It applies to all functions where information assets are created, controlled, stored, preserved, retained, destroyed or transferred
- » is developed within the style and structure of your agency's policy framework
- » is broad and should remain applicable over time
- » should be short, concise and easily understood by the reader to communicate the guiding principles for creating and managing your agency's information assets
- » should be formally authorised by an appropriate senior manager and sent to staff, contractors and volunteers that create or access the information assets
- » should contain links to related policies



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

- » should be easily accessible
- » has a policy owner and is reviewed regularly and updated.

The Policy can be a single document, or the requirements can be built into one or more existing policies, such as Information or Cyber Security Policy, Information and Data Access Policy, Risk Management Policy etc.

Generally, your agency should have policies that cover:

- » roles and responsibilities relating to information assets including education and training
- » the management of information assets, including use, disclosure and storage on-and-offsite
- » information asset privacy
- » information asset security
- » the disposal of information assets.

All information management policies must comply with relevant Standards, including information and cyber security requirements.

3.1.2 Information Management Procedures

An Information Management Procedure:

- » provides step by step instructions to achieve the objectives in the Policy
- » includes a detailed description of activities, including what, how, when or who
- » should be regularly reviewed and updated to reflect any process changes or responses to regulatory changes and risk
- » is easily accessible
- » should be short, concise and easily understood. Lists, tables, checklists and drawings are useful ways of presenting guidance in a concise manner
- » should have a procedure 'owner' that is responsible for reviewing, updating and championing its use.

Procedures should be developed according to need. This will be dependent on the:

- » size and complexity of your agency and the functions it performs
- » level of regulatory compliance and risk, requiring rules-based controls
- » amount of detail required to provide the appropriate level of operational guidance.

A small agency might only need one or a few procedures covering the main aspects of information management practice. Whereas a large agency might need many procedures detailing information management practice for different functions of the agency.

Information management requirements can be one or more standalone procedural documents or can be built into other procedures. For example incident management planning for information assets can be included as part of a business continuity procedure and planning or as a standalone plan or procedure.

Your agency should also ensure it has processes in place for engaging with third party providers who will manage information assets on your agency's behalf, in particular those that are sensitive or contain personal information.

3.1.3 Review and adherence

Policies and procedures should be reviewed regularly to ensure they remain up-to-date, relevant and continue to support your agency's information requirements (Behaviour 2.8). Regular review ensures:

- » changes to regulatory or business requirements are incorporated and communicated to staff
- » policy gaps are identified and addressed
- » feedback received from stakeholders can be incorporated to improve current policies and services.

A large part of the success of the Program, and in turn fostering a culture that values information, relies on staff adherence to information management policies and procedures (Behaviours 1.5 and 2.9). It is important to educate and train staff (Behaviour 1.4) appropriately in:

- » the value of your agency's information assets
- » their information management responsibilities
- » the relevant information management and business systems
- » your agency's information management policies and procedures.

All relevant policies and procedures should be communicated to staff. Training should be provided where required. If appropriate, staff should provide an affirmation that they have read and understood the policies applicable to them.

3.2 Resources, Roles and Responsibilities

Relationship to the Information Management Standard

Sufficient allocation of resources, including budget, infrastructure and staff, is a vital element of a Program and Plan.

Staff allocated to perform information management related functions must be appropriately skilled and have the capability to manage information management assets in accordance with the Standard (Behaviours 1.4 and 3.1-3.6) and your agency's Plan.

Resource allocation needs to be done within your agency's specific context, such as legal and regulatory requirements, risk and business objectives.

Under Behaviour 1.5, agencies must “*foster an organisational culture that values and manages information as an asset and supports business objectives and activities*”. To foster such a culture, all staff must have a clear understanding and acceptance of their information management roles and responsibilities.

3.2.1 Resources

The scope of the Plan will define the type and quantity of resources needed to implement the tasks identified.

Relevant resources include:

- » financial – once-off and / or ongoing
- » staff – number and expertise
- » infrastructure – such as space, technology, materials, logistics such as transport, services.

All resource allocation will have a financial component, even in terms of using regular budget allocation. New initiatives may require additional funding. Depending on the nature, scope and components of the initiative a business case might be required. For example, if the initiative is to make one or more specific information systems compliant with relevant standards, there may be costs in engaging external specialists to undertake that work. Or, if a major disposal program for physical information assets is required, funding might be required for contract staff, materials transport and storage.



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

Determine resource needs by:

- » identifying all aspects of support needed to implement the required information management related tasks
- » assessing if resources are needed on a once-off, intermediate or ongoing basis, and how the resource mix might change. Funding might need to be secured as part of the regular budget allocation for specific areas (for example the records management function)
- » identifying what resources are already available and what resources need to be acquired from elsewhere
- » identifying costs as accurately as possible and, if applicable, how they might change over time
- » identifying possible options for resourcing, for example can someone with appropriate expertise be assigned from another area of your agency or from across the sector, can university students with relevant skills be engaged, can existing budget be reassigned from a lower priority task or can your agency share storage space with another agency?

If needed, prepare a business case or recommendations according to your agency's internal process. In aiming to meet the Standard you should clearly identify the business benefits and risk.

Short-term engagement of appropriate expertise is recommended, where required, for agencies that do not have a dedicated information management specialist.

Engagement of third party providers

It is common practice for government to engage third party parties to provide:

- » services on their behalf that involve the transfer or handling of government information assets or
- » direct services to your agency (for example with an ASP or a cloud service for storage).

Any contracts that involve the handling and / or storage of government information assets, in particular assets that contain personal information, must include obligations on the service provider to ensure your agency's information assets are managed in accordance with the SR Act and your agency's relevant privacy principles. The contract needs to clearly identify any ownership and custody arrangements of the information assets. The Contracting Standard sets out these obligations.

The Contracting Standard, accompanying guideline, and model contractual terms and conditions are all available from the State Records website at <https://archives.sa.gov.au>.

Legal advice is recommended where information assets will be stored and / or managed outside of Australia to ensure your agency continues to meet legal and compliance obligations specific to your agency. These obligations include, at minimum, those under the SR Act, the FOI Act, the SAPSF and SACSF, and relevant privacy principles. Provision of sensitive or classified information to a foreign entity is of a particular concern.

Agencies using ASP for secondary storage of temporary value information assets must comply with the Management and Storage of Temporary Value Information Assets Standard.

3.2.2 Roles and responsibilities

Principle 3 of the Standard is about information ownership or stewardship. Information stewardship is the careful, responsible and accountable management of information. The information is not owned personally by any individual but rather by your agency, however responsibility and accountability for the information may be assigned.

Good information stewardship

Ownership and accountability for information (Principle 3) must be managed consistently through a governance structure that:

- » formally assigns the responsibility of information assets (in writing) to the owners of the relevant business or function
- » ensures staff are aware of their information management responsibilities and have the necessary skills to fulfil them
- » documents and clearly defines in writing, through policy or other internal documents, the roles and responsibilities relating to the management of information assets
- » provides clear communication to assigned owners of their responsibilities in managing the information assets assigned to them
- » monitors and reports on staff adherence to its internal information management policies
- » has the support and commitment of the chief executive and senior management, including the allocation of proper resourcing.

Information stewardship might be the responsibility of several roles at different levels within your agency. An individual may be assigned more than one role, for example a senior manager or the Information Manager may also be the Policy owner. An Accredited FOI Officer may also be involved in coordinating data sharing agreements or privacy management. For small to medium agencies roles may be combined.

Fostering a good information management culture

In addition to good information stewardship, it is important for your agency to foster a good information management culture (Behaviour 1.5), that:

- » values and manages information as an asset
- » recognises how your agency's information assets support business objectives and activities.

To achieve a good information management culture, your agency must have a clear and well communicated strategic vision and understanding of the value of its own information assets and how they are to be managed. Your agency's strategic vision and direction should be developed in accordance with the Standard's principles with adequate training and resourcing provided to ensure the effective implementation of such policy. One of the key pillars to fostering an organisational culture that values and

manages information as an asset and supports business objectives and activities is having a robust Program.

Another key pillar is the championing and promotion of good information management principles and values by your agency’s chief executive and senior management. This includes ensuring the Program is effectively implemented through:

- » the allocation of adequate resources. This includes identifying future areas for improvement and development to be factored into budget objectives where current budget constraints apply
- » promoting sound information management practices, underpinned by the Standard, in its operational activities, including the implementation of supporting information management policies and procedures
- » providing information management training to staff and educating them on the importance of information management to create a shared understanding of your agency’s information management values.

Responsibilities

The level of responsibility for information management varies according to an individual’s role.

Typical levels of responsibility are listed in Table 5. The role title may be different depending on your agency, for example the Information Manager may be titled ‘Records Manager’.

Your agency must ensure all staff receive information management training and comply with your agency’s information management policies and procedures. All staff should be made aware of the roles and responsibilities in creating and capturing information assets in order to carry out business functions and activities effectively. Staff compliance should be monitored routinely.

Table 5: Roles and responsibilities

Role	Responsibility
Chief Executive (or principal officer)	<ul style="list-style-type: none"> » ensure your agency complies with legislative requirements for information management, including the SR Act and Standards issued under the SR Act » actively support and champion information management values and practices
Senior Managers	<ul style="list-style-type: none"> » understand regulatory requirements for information management and oversee compliance » approve and assign appropriate resources to support the implementation of the Plan » actively support and champion information management values and practices

Role	Responsibility
Information Manager	<ul style="list-style-type: none"> » participate in the development, acquisition and implementation of systems that keep information assets, in any format » liaise with others, such as ICT professionals, business area managers, FOI teams, privacy officers, cyber security specialists, and contracted service providers » develop controls for information assets » provide training and support » undertake information management compliance or capability assessments » intervene promptly and appropriately when made aware of inappropriate information management practices or adverse events » manage centralised hardcopy records systems and dedicated Electronic Document and Records Management Systems (EDRMS)
ICT / Information Custodian / Records officers and administrators	<ul style="list-style-type: none"> » ensure continuous and reliable operation of information systems, such as security, access control, backup and business continuity, including for hosted or cloud-based systems » administer hardcopy records systems and EDRMS
Business Unit Head	<ul style="list-style-type: none"> » be designated as the 'Business Owner' of specific information assets (for example the person or group that is ultimately responsible for an information asset) » be responsible for the creation and management of any information in their business unit » ensure that the Policy is appropriately implemented in their area and good information management behaviours are practiced
All staff	<ul style="list-style-type: none"> » adopt good information management practices by creating complete and accurate information assets wherever evidence of the conduct of business is required and storing them in compliant systems

3.3 Access and Release Schemes

Relationship to the Information Management Standard

Knowing the relevant access and release schemes (schemes) that apply to your agency will ensure it provides access to information where it is appropriate to do so or where authorised (Behaviour 5.7). This should be reflected in the Plan, policies and procedures.

Release of information outside of the schemes, wherever possible, is encouraged through proactive disclosure (Behaviour 5.8).

3.3.1 Access and releasing of information

Access and release of information can be done through a range of schemes, such as data sharing, FOI and legal discovery.

Such schemes can be used by:

- » members of the public to access certain types of government information
- » government agencies to share information with each other.

Each scheme has a different purpose and method of access or release. The schemes can be used to facilitate the flow of information within government (Data Sharing Act) or to the public (Government directives). They can also be legislative (FOI) or policy based (administrative release).

To develop the Program and Plan, all relevant schemes that are applicable to your agency need to be identified. This can be done as part of the business and regulatory analysis.

This will determine the access and release policies and procedures that may be needed (Behaviour 5.7). For example, the process to follow when dealing with an FOI application is mandated by the FOI Act, whereas the process for administrative release is determined internally by your agency.

Common requirements for accessing information

To provide responsible and open access to information to the public or other government agencies your agency needs to know:

- » any privacy, security or confidentiality constraints attached to the information sought



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

- » the systems (physical or digital) that are holding the information assets and any security classifications or other access restrictions that have been applied
- » any third-party property rights, such as copyright
- » that the information is accessible and available for release.

Other considerations include how and when to release the information and in what format.

The applicable schemes for your agency are determined by the regulatory and operational environment in which your agency operates. Some of the more common access and release schemes are listed below.

3.3.2 Relevant access schemes

Open data

Open data is the release and re-use of non-sensitive public sector data to the public. Government data sets are made freely available online. It is important when your agency is releasing open data that it uses established and existing definitions of information where possible (Behaviour 4.4).

Under the Government's Open Data Framework state government agencies can publish open data proactively or on request from another government agency.

For further information, refer to the [Open Data Toolkit and Open Data Process Guide](#), available from the Department of the Premier and Cabinet's website.

Freedom of information (FOI)

Under the FOI Act members of the public and Members of Parliament have a legally enforceable right to:

- » be given access to government information, subject to any exemptions in Schedule 1 of the FOI Act
- » amend their own personal information held by a government agency that is incorrect, incomplete, out-of-date or misleading.

The purpose of the FOI Act is to:

- » promote openness in government and the accountability of Ministers of the Crown and other government agencies
- » facilitate more effective participation by members of the public in the processes involved in the making and administration of laws and policies.

If your agency is subject to the FOI Act, having an up-to-date asset register will assist in the quick identification of information asset sources and locations that will need to be searched when progressing FOI applications.

All FOI applications must be:

- » processed in accordance with the FOI Act by trained and designated Accredited FOI officers

- » captured and managed within your agency's records management system. The original information asset must be retained in your agency's records management systems. The copies (including any redactions) provided to the FOI applicant should be saved in the relevant FOI case file.

FOI should be used as a last resort. Proactive disclosure or release through administrative schemes, where appropriate, is the preferred approach.

For more information on FOI refer to the [State Records website](#).

3.3.3 Relevant release schemes

Administrative release

Administrative release of information can be done proactively or in response to a request (Behaviour 5.8).

This is separate from information required to be released under legislation such as FOI, or for inspection as a public register, or other documents under agency-specific legislation. It does not include information specifically published for public dissemination such as publications.

To ensure consistency in decisions about, and processes for, the administrative release of information, a public access policy and / or procedure should be developed and published online by your agency.

For more information on administrative release refer to the [State Records website](#).

Government directives on release of information – applicable to State Government Agencies only

There are several government policies that require state government agencies to proactively disclose information to the public by online publication. Examples include the following Department of the Premier and Cabinet Circulars:

- » PC031 Disclosure of Cabinet Documents 10 Years or Older: allows a Cabinet document, over ten years but under 20, to be proactively disclosed to the public (subject to certain conditions)
- » PC035 Proactive Disclosure of Regularly Requested Information: agencies are required to release information that relates to various aspects of government expenditure, unless claimed exempt under FOI
- » PC045 Disclosure Logs for Non-personal Information Released through Freedom of Information: agencies are required to make non-personal information and documents available that have already been released under FOI.

Data Sharing Act

Under the Data Sharing Act, agencies can make information available to other public sector agencies or non-government organisations for specific purposes, subject to certain criteria and under specified protections (such as protocols around personal

information). This is done through data sharing agreements which outline how both parties will fulfil the legislated requirements.

The agency providing the information to another agency or organisation remains responsible for administering any other request by the public for that information.

Agencies can meet the requirements under the Data Sharing Act by implementing a comprehensive Program ensuring your agency has appropriate security and access controls in place.

Information Sharing Guidelines

The Information Sharing Guidelines provide the steps to be taken when sharing information relating to vulnerable people which might otherwise be subject to privacy restrictions.

Agencies that have interactions with vulnerable people should have a procedure which explains how to implement the Information Sharing Guidelines.

For more information on the Information Sharing Guidelines refer to the Department of the Premier and Cabinet's website.

3.3.4 Information sharing required by law

There are situations required by law where information must be shared irrespective of consent being given or not. For example, mandatory notifications under the *Children and Young People (Safety) Act 2017* or disclosures in the interests of public safety under the *Correctional Service Act 1982*.

Legal discovery is another process which requires mandatory production of documents for inspection as evidence relevant to the case under scrutiny. This could be a civil litigation matter or a commission of inquiry.

3.3.5 Public access to archives

When permanent value physical information assets are transferred to the State Records Archive, the SR Act requires your agency to, in consultation with the Director of State Records determine:

- » that public access to the information asset is not subject to any restrictions, or
- » conditions excluding or restricting public access to the information asset.

Often these determinations indicate that public access is restricted for a specified period, and open once their sensitivity had diminished.

State Records provides access to information assets that have been transferred to the Archive and are deemed open under an authorised access determination.

Where a request for access to a 'closed' information asset is received, your agency can either provide the information broadly through proactive disclosure, authorise State Records to provide access to the specific individual under certain conditions or require the requestor to make a request under the FOI Act as a last option.

State Records will contact your agency if it considers that sensitive information is not adequately protected, prompting a review of the access determination.

It is recommended that information assets of a non-personal and / or non-sensitive nature be open to public access on transfer to State Records.

In making a determination to restrict public access to your agency's information assets in State Records custody, it's important to consider:

- » the encouragement in the SR Act in favour of ready public access to information assets
- » the protection of personal information, confidentiality or cultural sensitivity
- » the continuing information security needs
- » ongoing commercial confidentiality requirements
- » legislative requirements.

State Records may impose additional restrictions based on the condition of fragile physical information assets.

3.3.6 Access to government owned information assets held by third parties

An obligation to access, or provide access to, information assets still exists where your agency has engaged a third party to provide:

- » business services on your agency's behalf that create or use information, or
- » a service to manage information assets (such as the electronic or physical storage of your agency's information assets through an ASP or cloud service).

Any contract entered into with a third party provider that results in distributed management or storage of information assets must include conditions that ensure your agency can still access those assets for a relevant purpose. This includes access required under the FOI Act, for legal discovery and any other administrative or legislated access requirements.

Further, it must include terms which address how information assets are to be returned to your agency upon completion or termination of the contract. They should seek to ensure:

- » the information assets remains accessible and in a useable format
- » in the case of digital information assets, they are transferred or migrated to a compliant system within your agency, and
- » the information assets are not retained by the third party any longer than necessary to perform the contracted services.

Transfer of permanent value information assets to the custody of State Records must be done in accordance with the SR Act and Transfer Standard.

See also 3.2.1 regarding engagement of third party providers.

3.4 Privacy Protection and Considerations

Relationship to the Information Management Standard

Personal information must only be collected, used, disclosed, stored and disposed of by your agency, in accordance with privacy principles (Behaviour 5.6).

Your agency's Plan, policies and procedures should clearly reflect how personal information will be collected and managed by your agency.

3.4.1 Information privacy protection

Information privacy refers to how an individual's personal information (for example name, address, date of birth, health information etc.) is handled.

Your agency must ensure that personal information is stored, accessed and used in accordance with established general privacy principles (Behaviour 5.6) such as:

- » being transparent - informing individuals why the personal information is being collected, such as if the collection is authorised or required by law and how the personal information will be used and disclosed, for example only for the purpose it was collected for, unless certain conditions are met (for example required for law enforcement purposes or authorised under law)
- » data minimisation - only information that is required for the stated purpose will be collected
- » security - making sure appropriate security measures are in place so that personal information is securely stored and managed according to the information's sensitivity
- » accessibility - informing individuals how their personal information can be accessed
- » correction - informing individuals how their personal information can be corrected if they believe it is incorrect, incomplete, out-of-date or misleading.

While the overarching policy varies for different sectors, most jurisdictions apply similar principles.

State government agencies must comply with the Department of Premier and Cabinet Circular [Information Privacy Principles Instruction \(IPPI or PC012\)](#) which regulates the way they manage, collect, use, disclose and store personal information. It also



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

regulates the practices of contracted service providers operating under agreement with a state government agency.

If your agency is not bound by the IPPI you will need to have your own privacy policy that describes the way your agency manages personal information.

Your agency must ensure personal information is disposed of in accordance with a current disposal schedule.

3.4.2 Assessing privacy requirements

Where a project is planned or a decision is made to go ahead with an initiative that involves the collection, use, disclosure or storage of personal information, a Privacy Impact Assessment (PIA) should be undertaken. A PIA is a systematic assessment that identifies the relevant privacy considerations and risks an initiative / project might have on the privacy of individuals and how those risks will be managed or eliminated. Importantly, a PIA should be undertaken in the initial stages of development of a project to have the best opportunity to mitigate privacy risks.

The purpose of completing a PIA is to identify and manage possible privacy risks or impacts and to understand how personal information flows in a particular project or initiative.

3.4.3 Privacy and Third Party Providers

If your agency contracts a third party provider to handle information assets that contain personal or sensitive information on your agency's behalf, the contract must include obligations on the third party provider to ensure the personal information is managed in line with your agency's relevant privacy principles.

Model terms and conditions have been developed by the Crown Solicitor's Office to assist agencies to meet their privacy obligations and are available on the State Records website.

Legal advice is recommended where information assets will be stored and / or managed outside of Australia to ensure your agency continues to meet legal and compliance obligations under the SR Act and relevant privacy principles.

Note: The Commonwealth *Privacy Act 1998* **does not apply** to a third party provider in respect of any work it performs under contract to a State or Territory Government agency. It only applies to Commonwealth Government agencies and the private sector. Many organisations have practices in place to comply with privacy and should therefore be able to adapt to adhere to local privacy principles.

3.4.4 Personal information privacy breaches

A privacy breach occurs when personal information that is not already publicly available, is lost or subjected to unauthorised access, modification, disclosure or misuse.

A breach may have happened because of accidental loss, internal errors, deliberate actions, theft of hardcopy information assets or the theft or misuse of electronic information assets.

Where a personal information privacy breach occurs, your agency must:

- » take immediate action / actions to contain the breach
- » identify any risks associated with the breach and mitigate where possible
- » report the breach to the relevant authority (if relevant)
- » notify relevant affected parties
- » implement remedial action to address the current breach as well as prevent further breaches occurring.

Staff should be advised of the process to be followed in the event of an information breach, including potential investigation and disciplinary actions.

As soon as possible after a breach has occurred, State government agencies must notify:

- » the Privacy Committee of South Australia, and
- » if relating to systems or cyber security incidents – the Department of Premier and Cabinet Cyber Security Watch Desk, and
- » if relating to tax file numbers – the Office of the Australian Information Commissioner.

For more information refer to the State Records website at <https://archives.sa.gov.au>.

3.4.5 Privacy requirements and proactive release of information

Section 3.3 outlines various schemes under which information can be accessed. In all cases, your agency needs to know what privacy requirements apply when releasing information under these schemes.

For example, when releasing information under the Information Sharing Guidelines, consent must be sought from the person to whom the information relates unless to do so would result in harm to their or others safety and wellbeing. Further privacy requirements include ensuring that the personal information (in any format) is stored securely and is shared in a secure way when required.

3.5 Security Controls

Relationship to the Information Management Standard

To ensure information assets remain accessible and reliable, appropriate informational, physical, cyber and digital security controls need to be implemented. These controls include:

- » ensuring all information assets are saved into systems in a timely manner that meets the relevant Standards¹ and whole of government security Frameworks² to ensure they are protected from compromise³ (Behaviour 4.2)
- » implementing information security classifications for all information assets applicable to the sensitivity of that information (Behaviour 5.1)
- » reviewing and amending access restrictions on information as sensitivity alters (Behaviour 5.2).

Any information assets that require protection, even at a low level, should be treated as sensitive. The actual level of sensitivity of an information asset is determined by the information’s assets level of confidentiality, security classification or the amount or type of personal information contained within it.

This will help ensure information assets are managed and stored appropriately and remain accessible for as long as required (Behaviour 2.6).

These controls should be reflected in the Plan and / or your agency’s information security policy. The Plan should also require all systems to be designed in accordance with relevant standards to ensure they support the effective management and disposal of information (Behaviour 2.5).

Relevant standards for security controls include the Minimum Recordkeeping Metadata Requirements Standard (Metadata Standard) and the Managing Records in Systems Standard (Systems Standard).


3. Information Management Plan

- 
3.1 Policy and Procedure
- 
3.2 Defined Resources, Roles and Responsibilities
- 
3.3 Access and Release Schemes
- 
3.4 Privacy Protection and Considerations
- 
3.5 Security Controls
- 
3.6 Disposal Determinations
- 
3.7 Compliant Systems

¹ Managing Digital Records in Systems Standard, Minimum Recordkeeping Metadata Standard, Contracting and Information Assets Standard and Management and Storage of Temporary Value Information Assets Standard.

² South Australian Protective Security Framework and South Australian Cyber security Framework.

³ Compromise includes, but is not limited to, loss, misuse, interference, unauthorised modification, unauthorised disclosure.

State government agencies will also need to comply with the SAPSF and the SACSF (as the relevant security Frameworks) in developing and implementing security controls.

Relevant security controls should also be included in any contract with third party providers who manage and / or store information assets on behalf of government to ensure these assets are managed in accordance with the SR Act and any other relevant legislation or policy. This includes ensuring security controls are implemented by the third party provider to ensure the agency's information assets are:

- » stored appropriate to their information classification in accordance with relevant government security standards (for example SAPSF and SACSF)
- » protected against unauthorised access
- » protected in the event of an incident (for example flood, power outage or ransomware cyber-attack)
- » handled appropriate to their format and protected from physical harm.

For more information on contracts with third parties refer to Contracting Standard and the Management and Storage of Temporary Value Information Assets Standard on the State Records website.

3.5.1 Security requirements

Your agency can use and implement several different controls to manage and monitor the security of information assets.

Information assets must be protected according to the impact misuse of such information could have on your agency's business activities and functions.

Information Classification

Information classifications must be applied to information assets (Behaviour 5.1), including emails. A classification is determined based on the sensitivity of the information in question.

Systems, where possible, need to be configured to automatically assign access and edit permissions to information assets based on their information classification. Refer to the Systems Standard for more information.

Your agency should also apply access restrictions or permissions to information assets. Access restrictions or permissions should be regularly reviewed and removed as soon as they no longer apply or once sensitivity changes, this includes updating the systems that hold the information assets to reflect any changes made (Behaviour 5.2). Systems, where possible, should be configured to review access restrictions or permissions automatically as information classifications change.

Note: State Government agencies need to ensure they apply information classifications in accordance with the SAPSF policy INFOSEC1: Protecting official information.

In addition to applying information classifications to the information assets, all cyber security risks must be managed in accordance with the SAPSF and SACSF when engaging third parties to access, store or otherwise handle information on behalf of your agency.

For further information on the SAPSF and how to apply the information classifications to your agency's information assets, refer to the [Department of the Premier and Cabinet's website](#).

Personnel Security

Staff should only be given permission to access information if they meet the relevant suitability checks to access and / or view that information, particularly for staff in positions of trust who might have access over and above the average staff member in order to administer systems.

This ensures that information assets can only be accessed by staff, including contractors, with the relevant associated security or classification level. For example, before allocating permission to a staff member for access of information on individual children within a system, the systems administrator must first verify they have a current and valid working with children clearance and national police clearance.

The greater the sensitivity of information, the higher level of assessment for suitability that will be required (such as a national security clearance).

Processes should be developed and maintained to ensure all staff remain suitable for the position they hold. Your agency's procedures for ongoing suitability assessment should be determined through risk assessments that consider:

- » the type of staff and employment (ongoing staff, temporary staff, security clearance holders etc.)
- » the staff member's level of access to sensitive or security classified information and resources
- » your agency's tolerance for security risks
- » any position specific risks
- » the individual's personal risk profile.

Note: State government agencies should refer to the SAPSF for more detailed requirements in relation to personnel security, including recruitment, maintaining staff suitability and staff separation.

Physical security

Information assets (both hardcopy or digital hardware) should be kept secure to protect from physical interference or damage (such as theft, corruption, changes to environmental conditions, tearing, vermin, etc) and from unauthorised access (such as having inappropriate security measures and uncontrolled access to storage areas). An indicative list of requirements is in Table 6 with examples of appropriate controls.

The type of storage facility depends on the information assets format and their physical and chemical properties, their required retention period and accessibility requirements.

Note: State government agencies should refer to the SAPSF for more detailed requirements for the physical security of information.

In addition to ensuring the storage facility has adequate physical security controls in place, they must also be fit for purpose for storing information assets. All information assets must be stored in a clean, environmentally and pest-controlled storage area that is well ventilated with a minimum of natural light. Information assets must be packed in suitable containers appropriate to their format and on shelves that are fit for purpose. For more information refer to the Management and Storage of Temporary Value Information Assets Standard on the State Records website.

Table 6: Requirements for physical security

Requirement for physical security	Examples of controls
Security arrangements for information assets stored onsite	<ul style="list-style-type: none"> » intellectual and physical controls (for example file movement locations) » secure and access-controlled server rooms » secure and access-controlled storerooms for hardcopy information » fire protection facilities » key management » building security, including compartmentalisation of access to sensitive or secure content » vermin and climate (temperature, humidity, air quality and lighting) controls
Security arrangements for information assets in use onsite	<ul style="list-style-type: none"> » clean desk policy and practice » locked facilities for confidential or sensitive information (this includes access controls) » ensure hardcopy information cannot be seen in public-facing areas » ensure computer screens (containing corporate-only information) cannot be seen in public-facing areas
Security arrangements for information assets stored or taken offsite	<ul style="list-style-type: none"> » secure transport and handling » use only State Records and / or ASP if using non-agency facilities » security is applied to offsite information assets taking into account the different risks of working outside your agency's premises

Requirement for physical security	Examples of controls
Information transmission	<ul style="list-style-type: none"> » information assets and equipment are managed securely when taken out of the office for official purposes, including home-based work
Ownership and custody arrangements	<ul style="list-style-type: none"> » government information assets are not sold, abandoned or donated to external parties » government information assets are not used for unofficial purposes without authorisation » appropriate controls are applied when transferring information assets to other government agencies in the event of structural change or archiving
Retention and disposal	<ul style="list-style-type: none"> » transfer permanent information assets to State Records according to applicable retention and disposal schedules and access determinations » non-current information assets are securely retained for the required periods according to applicable retention and disposal schedules » information assets are destroyed that are no longer required (as authorised under a current disposal schedule) using an appropriate method to ensure they are no longer accessible » appropriate sanitising or destruction of obsolete or damaged media so they are no longer useable, for example [through] full data erasure, crushing or disposal via an external specialist company

Digital security

There are additional controls that apply for information assets stored in a digital environment regarding the accessibility, sharing, storage and disposal of information.

Information assets should only be accessible to those with appropriate permission and a need to know as defined by their security classification. Permission for users should be clearly defined and assigned in the systems used (refer to the Systems Standard), as well as align relevant security metadata to information assets (refer to Metadata Standard) (Behaviour 2.5).

When sharing digital information, staff should ensure they use:

- » appropriate email controls for sending information to others (internally or externally), including applying the appropriate information classification according to the sensitivity of the information
- » secure applications or methods for sharing information externally, in particular over public network infrastructure
- » encryption of sensitive material.

Digital information assets should be stored appropriately and securely (Behaviour 2.6). Having a robust ICT infrastructure ensures digital information assets remain secure and are not subject to unauthorised access, amendment or use. This can be achieved through mechanisms such as having secure logins, user authentication, encryption, supervision or surveillance of data. Other digital security controls include applying the principle of least privileged (a user only has access to specific information needed to complete the required task) or just-in-time access (access is granted for a limited to a predetermined period of time, on an as-needed basis). Incident recovery and business continuity regimes can also be built into the ICT infrastructure management plan.

Incident recovery planning is an important element of your agency's Program. Measures can be put in place that ensures that information assets continue to be accessible, managed, available and shared in the event of, and after, an incident. This is one security measure that aims to protect information assets against loss or irreparable damage (including corruption) because of an incident. Your agency must also ensure any third party provider engaged to manage or store your agency's information assets has an incident recovery plan that includes the recovery of information assets in place.

When disposing of digital information assets, they need to be cleared using an appropriate method that ensures they are no longer accessible or capable of being recreated or reinstated. Disposal of any information assets must be done in accordance with the SR Act.

3.6 Disposal

Relationship to the Information Management Standard

Information can only be destroyed if it is no longer required and in accordance with the SR Act.

The Standard requires agencies to dispose of information assets in a timely manner once all business, legal and accountability requirements have been met (Behaviour 2.7).

Your agency's chief executive or delegate is responsible for ensuring:

- » no information asset is destroyed unless in accordance with a current, approved disposal determination (Behaviour 5.5)
- » that information is not sold, abandoned or donated to external parties which would result in your agency, or the government, not having access to that information and without authorisation in the form of a disposal determination (Behaviour 5.9).

This includes identifying requirements for retaining information assets not covered by a disposal determination and seeking a disposal determination for these information assets if needed (Behaviour 5.4).

To ensure information remains accessible for as long as required and is not destroyed without authorisation, the Plan needs to be underpinned by a disposal program and approved disposal determinations in accordance with the SR Act and the Disposal Standard.

3.6.1 Disposal

Disposal is not simply destroying information assets, it is a range of processes associated with implementing records retention, destruction or transfer decisions of temporary value information assets [not including the transfer of permanent value information assets to State Records or between agencies] which are documented in disposal determinations (*ISO 15489.1 Information and documentation - Records management, Part 1: Concepts and principles* (2017)).

A permanent value information asset is an information asset that has archival value and will be retained permanently for research by the general community subject to appropriate access restrictions.

A temporary value information asset is an temporary information asset that does not have archival value and may be physically destroyed when a prescribed retention period has passed.



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

Information assets must only be disposed of in accordance with the requirements set out in the SR Act and the Disposal Standard. The Disposal Standard provides a set of mandatory principles and requirements to adhere to when disposing of government information.

Disposal includes:

- » destroying information assets
- » abandoning information assets
- » migrating information assets from one system or platform to another
- » transferring ownership or possession of information assets to a private entity (known as Transfer of Ownership and Custody Schedule or TOCS)
- » selling information assets.

Under the SR Act, disposal does not include transfer to State Records or to another government agency, although similar practices apply.

3.6.2 Disposal Program

A Disposal Program is a key element of your agency's overall Program. It should include:

- » development of an agency specific RDS if your agency does not already have one (Behaviour 5.4)
- » understanding of any other disposal schedules that might apply to your agency's information assets
- » a Disposal Plan for a backlog of information to be assessed for retention or disposal
- » a schedule for implementing regular (for example annual) retention and disposal actions such as transferring permanent information assets to State Records annually or twice a year, rather than in small ad hoc transfers
- » regular review of the currency of the disposal schedules applicable to your agency, including ensuring any current information assets are not subject to a disposal freeze. This assists in guaranteeing all information assets are covered by a disposal schedule
- » procedures for applying one or more disposal schedules (for example sentencing of information assets)
- » policy and guidance on the disposal of non-official records, called on Normal Administrative Practice
- » processes for applying retention periods, including documentation of decisions and quality checking by skilled and experience personnel (internal or contracted)
- » approval and documentation processes for the permanent retention and destruction of information assets
- » documentation and transfer of temporary information assets to an appropriate internal storage / ASP until they are due for destruction
- » documentation and transfer of permanent information assets to State Records when they meet the Transfer Standard (they are over 15 years old, no longer required for current administrative use by your agency and are openly

accessible or only restricted for no more than 15 years after transfer, unless otherwise agreed)

- » policy and guidance on the disposal (or retrieval if appropriate) of information assets created or maintained as part of a contract with a third party provider. This includes ensuring the proper documentation is maintained for information assets disposed of by the third party provider on behalf of your agency. (For more information refer to the [Contracting Standard](#)).

To develop a Disposal Plan your agency will need to know what information assets exist, including those in business systems, and whether those information assets are, or are not covered by a current disposal determination.

Destruction of hardcopy or digital information assets must be done securely. External specialist services are available for this. Physical disposal methods include pulping, burning, pulverisation, disintegration or shredding. Sanitisation is the process of erasing or overwriting information stored on digital media. Methods include clearing, purging, degaussing and destruction. The destruction and / or sanitisation methods needs to be chosen according to the format of the information assets and their security classification.

3.6.3 Disposal determinations

There are various disposal determinations (referred to as Disposal Schedules) that can be used to enable compliant retention and destruction of your agency's information assets (Behaviour 5.5). These determinations apply to information in any format and are required to be approved by the State Records Council in accordance with section 23 of the SR Act.

Disposal Schedules

Disposal schedules identify the minimum periods information assets must be kept for.

General Disposal Schedules (GDS)

These are developed to cover information assets common to all agencies or councils, or to a specific sector. For example:

- » GDS 30 – covers information assets common to all state government agencies. **Note:** GDS 30 cannot automatically be applied to temporary information assets more than 50 years old **and** previously unsentenced. For these information assets, a specific operational RDS (see below) will need to be developed in conjunction with State Records
- » GDS 40 – covers all information assets common to local government agencies.

Disposal freezes

A GDS may also be issued to freeze disposal of any information assets relating to a specific subject.

These are developed where specified information assets are required to be kept longer than the retention periods approved in their original applicable disposal determination to assist with anticipated legal or statutory requests for access to those information assets, such as for a Royal Commission.

Examples include:

- » GDS 38 – covers Records of Relevance to the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability
- » GDS 16 – covers Native Title Claims.

Records Disposal Schedules (RDS)

These are developed to cover information assets unique to your agency's core business and not covered by a GDS (Behaviour 5.4).

An RDS can also be developed to cover a specific set of agency information assets. For example:

- » to get approval to destroy administrative information assets created after the year 1900 and over 50 years old, which are not covered by a GDS
- » damaged information assets that cannot be recovered.

Lost or misplaced information assets on loan from State Records must be formally reported to State Records, as this is a form of unauthorised disposal.

Transfer of Ownership and Custody Schedules (TOCS)

These schedules are developed to cover the transfer and ownership of agency information assets to a non-government agency. For example, a TOCS will be required whenever an agency function is privatised, such as the sale of a government owned aged care facility to a private entity. It is not required for a lease or third-party provider contract.

A TOCS applies to specific categories of information assets created and controlled by your agency which are affected by sale or an administrative change and are required by the private entity to carry out the functions and related activities that have been transferred.

The TOCS prescribes, depending on the information assets in question, who is responsible for disposal and relevant retention periods.

Sentencing

Sentencing is the process of applying retention periods to digital or hardcopy information assets from an approved disposal schedule.

It is recommended sentencing occurs when the information asset is created because the retention period is based on the requirements for evidence of the activity or process generating the information asset. Sentencing can also occur prior to disposal.

Sentencing usually involves:

- » determining if the information asset has temporary value or is required to be retained permanently (if required permanently must be transferred to State Records in accordance with the Transfer Standard).
- » if temporary, identifying the earliest date when the information asset may be destroyed

- » recording the date for destruction or requirement to retain the information asset permanently, and the RDS or GDS reference, on the information asset itself or in a recordkeeping system such as an EDRMS.

Note: All pre 1901 information assets are permanent due to their rarity and must be transferred to State Records.

In addition to ensuring the information assets are sentenced against a current approved disposal schedule / s, they should also be reviewed to ensure they are not:

- » required for a longer retention following legislative changes
- » subject to a disposal freeze
- » required as evidence in legal proceedings
- » required for ongoing business use (Behaviour 5.5).

Reviewing applied retention periods must occur when previously sentenced information assets become due for destruction or transfer to State Records; these information assets need to be assessed to ensure the sentence applied is still current (for example, the GDS/RDS version and item number still applies). Where sentences are no longer current, resentencing should take place. It may also occur when a new disposal schedule is issued or an existing disposal schedule is reviewed or amended.

When a revised version of a disposal schedule is issued there will often be changes to existing retention periods. Some retention periods may be increased from temporary to permanent, while others may decrease. New classes may be added and / or class descriptions may change resulting in some classes being combined (or rolled up) into one class and other single classes being split into multiple new classes. Resentencing will confirm the current disposal schedule and item number for the information asset and what retention period applies.

Normal Administrative Practice (NAP)

NAP applies to destruction of **non-official information assets**.

Under NAP your agency may routinely destroy information of a transitory or ephemeral nature where it is obvious that no information of continuing value to your agency will be lost.

An information asset will be of 'continuing value' if it is required for administrative, business, fiscal, legal, evidential or historic purposes.

For the destruction of **official information assets** refer to [disposal determinations](#) and section 23 of the SR Act.

The NAP Test

Before an information asset can be destroyed using NAP, the following test must be applied:

1. Does the information asset offer evidence of your agency's business? For example is the information asset used to perform staff duties, such as printouts used to verify or monitor data?

If the information asset **does not** relate to your agency's work, it can be destroyed under NAP as it is not an official information asset.

2. If the information asset does relate to your agency's work, does it:

- » form part of your agency's business?
- » add value to an existing information asset?
- » show how a transaction was dealt with?
- » show how a decision was made?
- » show when and where an event happened?
- » indicate who was involved and what advice was given?
- » require someone to action it?
- » relate to a legal document or agreement?

If the answer is **yes** to any of the above questions, it **cannot** be destroyed under NAP as it is an official information asset.

If the answer to all of the above questions is no, the information asset can be destroyed under NAP.

Drafts and duplications

In addition to NAP, information assets that are not captured under the SR Act as an official information asset, such as drafts and duplications, can also be destroyed if they will not become an official information asset in the future (refer to section 3 of the SR Act).

Drafts and duplications must not be destroyed if they contain notes of significant decisions, discussions, reasons and actions or contain significant information that is not contained in the final version of the information asset.

Hybrid files

Hybrid files contain both digital and hardcopy information assets dealing with the same activity or function. Prior to the disposal of an information asset, it must first be established whether it is part of a hybrid file.

To efficiently dispose of hybrid files, both information assets need to be destroyed, preferably at the same time.

When transferring permanent information assets to State Records, State Records need to be advised if the information assets forms part of a hybrid file. Your agency must retain the electronic permanent value information asset, adding such metadata as required to reflect the transfer of the hardcopy permanent value information asset to State Records.

If transferring both the electronic and hardcopy temporary value information assets to an ASP, your agency should ensure that the hybrid nature of the files is reflected in the description.

Sale, abandonment and donation of government information assets

Staff need to understand they are creating government information assets which have value not only to their agency but to the government, community and the State. This can be achieved by having policies clarify that information assets must not be sold, given away to external parties or taken home by staff without proper authorisation (Behaviour 5.9).

Information assets no longer required must not be misused or accessed inappropriately. Controls should be in place to prevent the abandonment of information assets. All information assets, including the devices on which they are held, need to be securely, completely and lawfully destroyed once they are no longer required. Refer to your agency's ICT policy for more information. Your agency is responsible for ensuring the proper destruction of all information assets in your agency's custody and that it occurs in accordance with the SR Act and with any other government policies. Further, destruction must be documented, particularly if undertaken outside of your agency.

3.6.4 Other influences

Other situations or events might require information assets to be kept longer than the minimum retention periods. For example:

- » legal matters – information assets are to be kept longer than the minimum periods where your agency is aware of actual, or likely, legal or statutory requests for access to information, such as: legal discovery for an impending legal matter, a subpoena, a Royal Commission Notice to Produce or as a result of new legislation or regulations
- » FOI – where information assets are due for disposal but are subject to a current FOI application
- » high risk – information assets should be kept longer where they are identified as being of significant risk (for example, information assets potentially related to native title or COVID response)
- » machinery of government changes – information assets might need to be kept longer when functions, activities or processes change, within your agency or across government.

For digital information that must be kept long term or permanently, your agency is responsible for the information assets' ongoing custody. Use long term preservation formats, official systems and well managed migration processes to ensure your information assets remain in a readily accessible format (which includes content, structure and context) for the prescribed retention periods (Behaviour 5.3).

3.6.5 Accessibility

Information assets must remain accessible and in good condition (if digital, in a readable format) for as long as they are required. This includes when information assets need to be migrated from a physical to a digital format for preservation or conservation purposes, or digital information assets need to be migrated from one system, software or media format to another due to upgrades or the system becoming obsolete (Behaviour 5.3).

For example, if an information asset covered by a GDS has a retention period of 100 years it must remain accessible over the entire 100 year period and be capable of being relied on as trusted and authentic evidence of your agency's decisions made and actions taken. This means it must be capable of being retrieved by your agency in a readable format.

3.7 Compliant Systems

Relationship to the Information Management Standard

All information assets must be saved into systems in a timely manner that meet the relevant Standards⁴ and whole of government security Frameworks⁵ to ensure they are protected from compromise (Behaviour 4.2).

Your agency must design and implement all systems in accordance with Systems Standard and Metadata Standard to support the effective management and disposal of their information assets (Behaviour 2.5). This should be reflected in the Plan.

Having compliant systems will also help ensure the quality and authenticity of information assets (Behaviour 4.5) as well as ensuring they are managed and stored appropriately and remain accessible for as long as required (Behaviour 2.6).

For the purposes of the Standard:

- » quality refers to the integrity, reliability and accessibility of information assets to meet your agency's identified information requirements
- » integrity refers to information assets being intact, whole and uncorrupted
- » reliability refers to information assets being trustworthy
- » accessibility refers to information assets being available and locatable in a readable format
- » authenticity refers to the information assets being of undisputed origin, genuine and not a copy
- » compromise includes, but is not limited to, loss, misuse, interference, unauthorised modification, unauthorised disclosure.

For more information about relevant security Frameworks refer to section 3.5 Security Controls.



3. Information Management Plan



3.1 Policy and Procedure



3.2 Defined Resources, Roles and Responsibilities



3.3 Access and Release Schemes



3.4 Privacy Protection and Considerations



3.5 Security Controls



3.6 Disposal Determinations



3.7 Compliant Systems

⁴ Managing Digital Records in Systems Standard, Minimum Recordkeeping Metadata Standard, Contracting and Information Assets Standard and Management and Storage of Temporary Value Information Assets Standard.

⁵ South Australian Protective Security Framework and South Australian Cyber security Framework.

3.7.1 Characteristics of compliant systems

Compliant systems are format and technology neutral. Systems may be physical in nature (such as hardcopy filing systems) or digital (such as business information applications or dedicated EDRMS). The systems might be owned and managed by your agency or by others (such as in the cloud) but used by your agency.

Clear policies that outline each parties' responsibilities in relation to the management and use of your agency's information assets are required where systems are used that are outside the control of your agency. Refer to the Contracting Standard.

Management of digital and hardcopy information assets

Information assets created digitally should be managed digitally (Behaviour 2.4). They do not need to be printed for filing or information management purposes.

Information assets created physically can generally be scanned and managed digitally unless:

- » there are specific legal reasons to keep hardcopy information assets, such as property deeds
- » operational hardcopy information assets are routinely received, and it is not possible or feasible to scan them
- » existing systems do not have the required controls to manage digital images.

Note: Hardcopy information assets that have been digitised are not able to be destroyed without GDS 21 certification. Refer to [GDS 21 –Disposal of Hardcopy Source Records after Digitisation and the GDS 21 Guidance](#).

Where there is a legal, business or evidential need for keeping hybrid files, your agency must ensure that both the hardcopy and digital files are managed in the same manner. This means that both files should:

- » be appropriately linked to one another with the link documented in your agency's information asset register
- » have the same classification and sentence applied
- » have the same security classification applied
- » be disposed of at the same time and documented accordingly.

Specifying system requirements

All business systems, including EDRMS', should not only meet your agency's business requirements, but must ensure data quality and accessibility for as long as the information asset is required.

Business requirements usually identify the functions the systems should perform to support business objectives and operations. Technical (non-functional) requirements are also usually documented.

Business specific information management requirements are generally identified as part of your agency's value and risk analysis.

State Records has identified the **minimum** functional requirements that business systems must have regardless of the purpose of that system. These include:

- » being able to store digital information assets required as evidence of business activity as a record
- » ensuring information assets can be located and read
- » being able to apply access permissions to information content and metadata
- » ensuring information assets can only be deleted through an authorised process.

For a full list of the minimal functional requirements a system must have refer to the Systems Standard.

The Systems Standard is to be used / read in conjunction with the Metadata Standard as business systems need to hold the most up-to-date information while recording the relevant metadata to show the exact state of the data on which decisions were made at a particular point in time (Behaviour 4.3).

State Records endorses the use of the international standard *ISO 16175 Processes and Functional Requirements for Software for Managing Records* if your agency requires more detailed specifications than listed in the Systems Standard.

These documents can be provided to information system developers and project teams at the early stage of system development projects, or specific requirements from these documents can be added into business requirements documents.

Ensuring adequate controls

Compliant systems must have controls. Controls for information assets should include:

- » creation (where this occurs inside the system), capture and classification
- » access, retrieval and use (including security and personnel security requirements)
- » storage and preservation (including preservation of legibility)
- » control of changes (such as version control and audit trails)
- » retention and disposal.

Designating specific systems that are compliant as “official” information systems can be considered. These ‘official’ systems can be taken to hold the true and accurate information asset.

As these ‘official’ information systems are designated as the primary stores for agency information assets, such as EDRMS’, it enables:

- » design and implementation of consistent and understood controls (above) across systems
- » an agency-wide strategy for implementing retention and disposal of information assets
- » embedded staff routines of recording information and storing it in core systems.

For systems other than dedicated records systems processes can be implemented to provide the required controls. For example:

- » define and implement business rules for information management processes
- » configure the system to capture additional metadata where needed and / or enable metadata to be entered manually by a user
- » design a process for applying retention and disposal requirements
- » implement system security functions to prevent unauthorised access or modifications to any information, including metadata
- » design system capability to ingest information and / or associated metadata from other business applications
- » develop methods to migrate or export information and associated metadata, including security classifications, to another, or a replacement business application
- » develop and implement preservation and migration policies for information assets that require long-term retention.

The above processes may also be applicable to some dedicated records systems too.

The technology itself should be fit-for-purpose, operate on a continuous and reliable basis, and be protected by incident recovery and business continuity regimes.

3.7.2 Corrective action

When systems fail to perform for any reason, corrective action should be taken immediately. These actions might be as simple as configuring more automatic metadata capture to developing work-arounds (manual processes) for implementing retention and disposal actions, or restricting edit and delete permissions. They may also relate to increasing the education and training of staff in system use or good information management practice.

4. Education

Relationship to the Information Management Standard

Once the Plan has been developed, staff must be inducted and trained in the value of information and in their information management responsibilities and any relevant policies (Behaviour 1.4). Staff allocated to perform information management related functions must be appropriately skilled and have the capability to manage your agency's information assets.

However, all staff must have a basic understanding of information management.

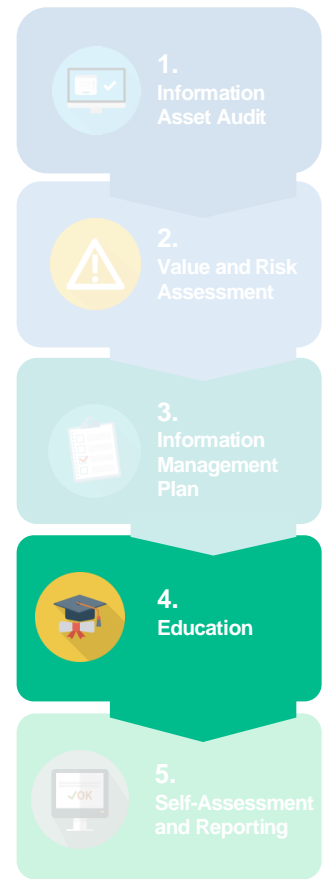
A large part of the success of your agency's Program relies on establishing the right culture and adherence to information management policies and procedures and awareness of their information management responsibilities (Behaviours 3.2 and 3.6).

Educating staff in the value of information and the management of information assets is key to fostering a culture of good information management (Behaviour 1.5).

4.1 Different messages for difference audiences

Before developing education or training tools, determine what information management messages your agency wants to convey, as these will differ depending on the audience. For example, the message to:

- » executive and senior management might emphasise that good information management supports achievement of business goals and objectives and mitigates business risk. It might also indicate management's ultimate responsibility for compliant information management across your agency, as well as meeting regulatory requirements, all of which contribute towards the fostering of an organisational culture that values and manages information as an asset and supports business objectives and activities
- » information technology professionals might focus on system and infrastructure reliability, security, design and acquisition of systems that are fit-for-purpose
- » business owners might focus on their responsibilities for overseeing the implementation of the Policy in their area and ensuring good information management behaviours are practiced
- » operational staff might focus on their individual and collective responsibility to create information arising from decisions and actions, managing it securely and storing it in the designated systems
- » to assist all staff in gaining basic information management training, State Records has an online course available, [Introduction to Information Management](#). It is recommended this training course be included as part of your agency's induction program and on its own internal training platform for easy



access to help ensure all staff have a basic understanding of their information management responsibilities.

Identify your agency's audiences, what their required competencies are and the key messages that need to be conveyed. Programs should be tailored appropriately according to the competence of each audience. It will also depend on whether your agency is introducing something new (such as software) or reinforcing previous training.

Audiences will vary in size and the frequency of messaging might be different for each. This will affect the style and content of the education or training programs.

4.2 Education content and delivery options

The aim is to build and maintain organisational capability to achieve your agency's information management objectives and compliance requirements.

Education and training needs to communicate the relevant messages in the right way. This includes:

- » what to communicate
- » how to communicate
- » when to communicate and how often
- » with whom to communicate
- » who should communicate it.

Education and training is critical for fostering a good information governance culture for the chief executive and senior management to promote and champion, creating awareness of the information management values that should be reflected in your agency's operational activities.

Table 7 is a summary of options for different types of information management education and training and the means of delivering it. Responsibilities for delivery will vary according to the roles that exist in your agency and your agency's size and functions. Where the role 'Information Manager' is shown, in smaller agencies that task may be undertaken by another person or by an external specialist.

Table 7: Training and capability building in information management

Training	Audience	Delivery Mechanism
Induction	New staff, contractors and volunteers	<ul style="list-style-type: none"> » provided by the Information Manager as part of the existing induction program » content includes core principles and mandatory requirements » face-to-face briefing + one-page reference guide to resources available on your agency's intranet <p>and / or</p> <ul style="list-style-type: none"> » e-learning module (for example State Records Introduction to Information Management course), including a Q&A component and pass requirements
General awareness	<p>Management</p> <p>All staff, including contractors and volunteers</p>	<ul style="list-style-type: none"> » key messages according to audience and your agency » delivered by the Information Manager » targeted brief sessions at staff meetings, 'pop up' briefings in lunchrooms or similar – five-minute messages » regular short messages or bulletins on your agency's intranet » easily accessible suite of guidance documents on the intranet, for example the Policy, procedures, FAQ's » provision of a central contact for Information Management advice and support
Tailored	Staff with specific information management responsibilities, such as system administrator	<ul style="list-style-type: none"> » externally commissioned program for System Administrators » structured training program for staff with different information management responsibilities and on-the-job training and / or mentoring, for example educate ICT staff about retention, disposal and system compliance requirements (metadata) » contracted training or engagement of external expertise including knowledge transfer as part of the contract

Training	Audience	Delivery Mechanism
EDRMS	All staff, contractors and volunteers using the EDRMS	<ul style="list-style-type: none"> » initial comprehensive training on rollout » provided by: <ul style="list-style-type: none"> ○ external supplier of the system (where an external application is purchased) on a train-the-trainer basis ○ super-users for business unit training » other training and support provided by the Information Manager: <ul style="list-style-type: none"> ○ small classroom-style, hands-on training ○ quick (one-page) guides on specific, commonly used functions ○ one-on-one instruction for specific staff (such as senior managers) ○ simple user guidelines on the intranet, hyperlinked between topics ○ refresher – as needed » help desk for non-IT infrastructure queries and guidance on information management
Exit Interview	Separating staff (and contractors and volunteers where relevant)	<ul style="list-style-type: none"> » a standardised handover process for information management included as part of a staff exit procedure » staff member to provide overview of information used for their operations to the incoming incumbent or person conducting exit interview » ongoing requirements of the Code of Ethics to maintain the confidentiality of government information included

4.3 Review and monitoring

Regularly review and update your agency's information management education and training. This will ensure staff knowledge and skills are updated or developed as information management responsibilities and the value of your agency's information assets change.

Refresher courses should be provided on a regular basis.

Maintaining the ongoing education of staff is important, both as part of ongoing business and because of any changes to your agency's information management requirements.

Staff adherence to education and training should be monitored and non-compliance addressed (Behaviour 2.9). Provide additional education and training as required.

5. Self-assessment and Reporting

Relationship to the Information Management Standard

The last element of your agency's Program is to assess and review how well your information management policies and practices support your agency's business activities and functions (Behaviour 2.8) and complies with the Standard overall.

5.1 Self-assessment

The aims of self-assessment are to enable your agency to assess the maturity and capability of your Program and to identify gaps in complying with the behaviours mandated in the Standard.

This will:

- » allow action to be taken, where needed, to address gaps and act on poor practice or where high value or high-risk information assets are threatened
- » sustain good practice
- » allow continuous improvement to occur where the opportunity arises.

Your agency may choose to use the Self-Assessment Tool (Tool) as a first step in the review of an established Program to identify gaps for prioritisation. However, this Tool is the official tool that will be used by State Records as a survey mechanism under the SR Act.

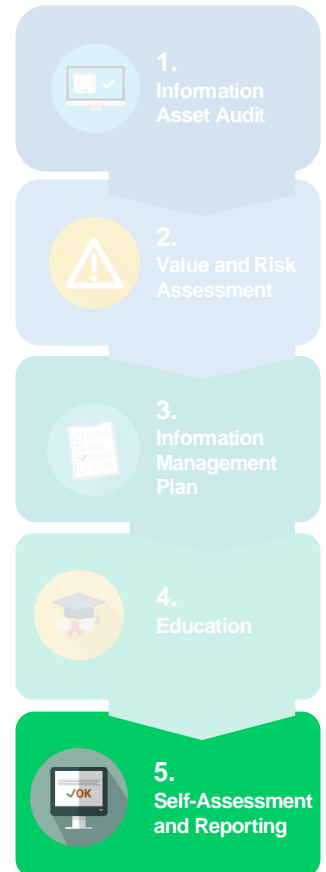
The Tool enables an assessment of your agency against the behaviours that underpin the five principles in the Standard. It is recommended to use the Tool on an annual basis to assess the Program's compliance against the Standard and your agency's overall information management governance maturity and capability.

The Tool is an excel spreadsheet which comprises four components:

- » instructions for use
- » detailed Assessment
- » capability Model
- » assessment Priorities.

The Tool developed by State Records is available on the State Records website - <https://archives.sa.gov.au/>.

Refer to the Tool instructions for more information on its use.



5.2 Self-assessment methodology

The methodology behind the Tool offers a scalable, tiered approach to help identify areas of strength and weakness at each level of requirement and to develop and implement actions to address weaknesses, improve outcomes and progress to the next level.

The four levels of maturity and capability your agency can assess your current information management practices (maturity and capability) against are:

- » absent (level 0)
- » basic (level 1)
- » operational (level 2)
- » proactive (level 3).

To comply with the Standard, your agency must satisfy at least the level 2 (operational) for each behaviour (under the principles of the Standard), unless a valid reason can be demonstrated why maintaining a lower level is acceptable. For example, due to agency operational or regulatory requirements, or level of risk identified.

Regardless of your agency's size, the Tool can be used by all, and can be applied to:

- » a whole agency
- » one or more business units
- » one or more business processes
- » all information formats, or one or more information assets such as hardcopy information assets or the content of business systems.

Improvement priorities may be determined based on the level of risk to a particular business area and the information assets supporting that area.

5.3 Outcomes of the Self-assessment Tool

Both the Capability Model and Assessment Priorities can be used by your agency's chief executive and senior management team to depict a high-level overview of the gaps in your agency's Program. The higher maturity and capability levels (level 2 - Operational and level 3 - Proactive) in the Detailed Assessment can also be used to help identify future actions required to improve your agency's compliance against individual behaviours.

The chief executive and senior management team can use the identified areas for improvement from the Capability Model report to feed back into their Program and Plan, improving overall compliance with the Standard and their information management maturity and capability.

Glossary

Agency – as defined in section 3(1) of the SR Act.

Approved service provider – service providers who have entered into the Deed of Agreement for State Records Storage Approved Service Providers List with State Records to provide storage, retrieval and destruction services.

Business and regulatory analysis – a systemic approach to assessing the internal and external environment of an agency to identify its operational, compliance and regulatory information requirements in this context, to determine what information assets it should be creating.

Compliant system – one that meets the minimal functional requirements as prescribed by the Managing Digital Records in Systems Standard and the Minimum Metadata Recordkeeping Standard in order to appropriately create and capture, use, manage, and dispose of information assets to ensure information assets can be relied upon as trusted and authentic evidence of decisions made and actions taken.

Compromise – includes, but is not limited to, loss, misuse, interference, unauthorised modification, unauthorised disclosure.

Disposal – under the SR Act disposal covers a range of processes associated with implementing records retention, destruction or transfer decisions (not including transfer to State Records) which are documented in disposal determinations.

Disposal Determination (commonly referred to as a disposal schedule) – a disposal determination is a legal document (for example a schedule or minute) that provides authorisation in accordance with the SR Act for information assets to be disposed of.

Disposal freeze – a disposal schedule that authorises specified information assets to be kept longer than the retention periods approved in their applicable disposal determination to assist with anticipated legal or statutory requests for access to those information assets, such as for a Royal Commission.

Disposal schedule – is the tool through which the disposal determination is implemented by identifying information assets as either temporary or permanent value. For information assets identified as being of temporary value, the disposal schedule further identifies how long the assets must be kept, at a minimum, before your agency can destroy them. Permanent information assets are to be transferred to State Records' custody in accordance with the Transfer Standard.

Good Information stewardship – the careful, responsible and accountable management of information.

Information asset – incorporates the definition of official record as defined by section 3(1) of the SR Act, and includes information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

Information asset audit – a survey to identify what information assets exist and to evaluate how these assets support an agency's business requirements.

Information asset register – a list that identifies what information resources are held and where they are located. It provides stakeholders with an overview of the information assets under your agency's control.

Information governance maturity and capability – the level of compliance of a agency's current Information Management Program and practices against the Information Management Standard.

Information Management Plan – practical direction, developed by an agency, for implementing elements of the Information Management Program and meeting the Information Management Policy.

Information Management Policies and Procedures – the means of conveying information management requirements expected of an agency. The procedures are the operational guidance for achieving the Policy.

Information Management Program – the overall set of elements, managed by an agency, to implement an information governance model which meets the Standard.

Information Management Standard – legal authority under the SR Act that expands on the principles of the Strategy by outlining expected behaviours required to effectively manage information assets, to achieve business objectives and to meet legislative and policy obligations.

Information Management Strategy – which establishes the principles that must be followed by agencies to ensure information assets can be relied upon and trusted.

Normal Administrative Practice – transitory (not permanent) or ephemeral information, only needed for a short period of time - a few hours or days.

Permanent value information asset – an information asset that has archival value and will be retained permanently for research by the general community subject to appropriate access restrictions.

Recordkeeping Metadata – recordkeeping metadata comprises of the details needed to identify, describe, manage and understand information assets so they act as authoritative evidence of business activity.

Temporary value information asset – a temporary information asset that does not have archival value and may be physically destroyed when a prescribed retention period has passed.

Third party provider or contracted service provider – a non-government party that has either entered into an agreement with an agency to provide goods or services required by the agency to meet business activities and functions, or information management functions and responsibilities to an agency. While the contractor may be an independent business entity that takes responsibility for risks, the management of information assets created, kept and used under agreement are often treated as if managed by the agency itself.

Relevant Documents

Legislation

- » *Freedom of Information Act 1991*
- » *Public Sector (Data Sharing) Act 2016*
- » *State Records Act 1997*

State Records Standards

- » Appraisal Standard
- » Contracting and Information Assets Standard
- » Disposal Standard
- » Management and Storage of Temporary Value Information Assets Standard
- » Managing Digital Records in Systems Standard
- » Minimum Recordkeeping Metadata Requirements Standard
- » Transfer of Official Records Standard

General Disposal Schedules

- » GDS 21 –Disposal of Hardcopy Source Records after Digitisation

Frameworks

- » Deed of Agreement for State Records Storage Approved Service Providers List with State Records
- » Open Data Framework
- » South Australian Cyber Security Framework
- » South Australian Protective Security Framework

Department of Premier and Cabinet Circulars

- » PC012 Information Privacy Principles Instruction
- » PC031 Disclosure of Cabinet Documents 10 Years or Older
- » PC035 Proactive Disclosure of Regularly Requested Information
- » PC045 Disclosure Logs for Non-personal Information Released through Freedom of Information

International Standards

- » ISO TR 21946 Information and documentation – Appraisal for Managing Records
- » ISO 15489.1 Information and documentation - Records management, Part 1: Concepts and principles
- » ISO 16175 Processes and Functional Requirements for Software for Managing Records

State Records Guidelines and Information Sheets

- » GDS 21 Guidance
- » Model Terms and Conditions - IPPs and Records Management Records

State Records courses

- » Introduction to Information Management

State Government Guidelines and Information Sheets

- » Information Sharing Guidelines
- » Open Data Toolkit
- » Open Data Process Guide

Need further assistance?

Contact

Tel (+61 8) 7322 7077

Email StateRecords@sa.gov.au

Web www.archives.sa.gov.au

Date approved	Approved by	Date for review	Version
21042023	Director, State Records of SA	21122025	Version 1