Information Management Standard

Version: 1.3

Date Finalised: 12 04 2023

Date for Review: 12 12 2024

STATE RECORDS
of South Australia

Government of South Australia
State Records

Information Management Standard

The Standard

Authority

This Information Management Standard (Standard) is issued under section 14(1) of the *State Records Act 1997* (SR Act).

State government agencies must manage their information assets in accordance with the requirements set out in the SR Act and this Standard.

Scope

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

In this Standard, the term ‘information asset’ should be taken to incorporate the definition of official record as defined by section 3(1) of the SR Act. The term ‘information asset’ refers to information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

Executive Summary

The Standard establishes the principles and behaviours expected of agencies in managing government information assets to achieve their own business objectives and to meet requirements under their legislative and policy obligations.

The Standard is consistent with the concepts of International Standard ISO 15489 (2017).

Information Management

The appropriate management and control of information assets is crucial for the effective delivery of government functions and services. Good information management practices are the basis of good government; supporting evidence-based decision making, the development of policy and accountability.

Effective management of information assets supports innovation and the transformation of service delivery, enabling communities and individuals from across South Australia to transact with government and stay informed of government decisions.

Principles

The management of government information assets is based on five principles:

1. The value of information is known
2. Information assets are created and managed appropriate to risk
3. Ownership of information assets is assigned
4. Information assets can be relied upon
5. Information assets are available as required

Behaviours

Each principle is underpinned by a set of behaviours that agencies must demonstrate in order to ensure their information management practices align with government expectations.

The *Information Governance Guideline* and the *Self-Assessment Tool* have been developed to support agencies in achieving these behaviours.

Principle 1: The value of information is known

Information is treated as an asset of the agency; its value to enable business activities and functions, both current and future, is determined, understood and leveraged to improve business outcomes.

Behaviours

Agencies must:

1.1 identify and document what their information assets are, where they are stored and who is responsible for their management;

1.2 understand and document how their information assets support their business objectives and operations or their compliance obligations;

1.3 ensure information assets are linked to business functions and activities;

1.4 induct and train staff in the value of information and in their information management responsibilities; and

1.5 foster an organisational culture that values and manages information as an asset and supports business objectives and activities.

Principle 2: Information assets are created and managed appropriate to risk

Agencies understand what information needs to be created and kept to support business objectives, meet compliance obligations and mitigate risk.

Behaviours

Agencies must:

2.1 analyse and document what information assets must be created and managed across the agency applicable to the regulatory environment in which they operate;

2.2 develop and issue policies and procedures outlining how information assets will be managed;

2.3 assess the risks of not creating or managing information assets where there is a legal, evidential, or business need;

2.4 manage information assets digitally unless there are specific reasons for keeping hardcopy information assets;

2.5 design and implement systems according to relevant standards so that they support the effective management and disposal of information assets;

2.6 manage and store information assets appropriately, to ensure they remain accessible for as long as required;

2.7 only destroy information assets when no longer required, and in accordance with current, approved disposal determinations issued by State Records;

2.8 review and audit how well their information management policies and practices support their business; and

2.9 monitor, report and improve staff adherence to internal information management policies.

Principle 3: Ownership of information assets is assigned

Responsibility for the governance of information assets is assigned appropriately in order to ensure information assets are managed for the best outcomes of the agency, its customers and broader community.

Behaviours

Agencies must:

3.1 ensure ownership of information assets are assigned;

3.2 ensure that owners are aware of their responsibilities and accountabilities for managing the information assets;

3.3 ensure responsibilities for information assets management are delegated appropriately, in writing;

3.4 ensure that roles and responsibilities relating to the ownership and management of information assets are clearly defined in policy or other internal documents; and

3.5 ensure that ownership and accountability for information assets are managed consistently through a governance structure.

Principle 4: Information assets can be relied upon

Policies, practices and systems are implemented that ensure information assets can be relied upon as trusted and authentic evidence of decisions made and actions taken.

Behaviours

Agencies must:

4.1 create and keep full and accurate information assets appropriate to their business processes, regulatory environment and risk and accountability requirements;

4.2 ensure information assets are saved into systems in a timely manner that meet relevant Standards[1] and whole of government security Frameworks[2] to ensure they are protected from compromise[3];

4.3 record relevant details (metadata) in systems so that the business context of information can be readily understood;

4.4 use established and existing definitions for information assets where possible, so that there is consistency across the agency; and

4.5 implement practices and systems that ensure the quality and authenticity of information assets.

[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 (SAPSF) and South Australian Cyber Security Framework (SACSF).

[3] Compromise - includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure.

Principle 5: Information assets are available as required

Information assets are accessible for as long as needed and are shared appropriately (subject to access, security and privacy rules) within a protected and trusted environment.

Behaviours

Agencies must:

5.1 implement information security classifications and requirements that are applicable to the sensitivity of the information in accordance with whole of government policies and administrative directions;

5.2 review access restrictions on information and amend as sensitivity alters;

5.3 migrate digital information assets as systems, software and media are upgraded or become obsolete to ensure it remains accessible for as long as it is required;

5.4 identify requirements for retaining information assets not covered by general disposal schedules, and seek a disposal determination for these information assets;

5.5 ensure that no information asset is destroyed unless in accordance with current, approved disposal determinations;

5.6 collect, use, disclose, store, and dispose of personal information in accordance with the information privacy principles[4];

5.7 share information across government as appropriate or where authorised;

5.8 proactively publish information in line with government policy; and

5.9 not sell, abandon or donate information assets to external parties where such action would result in the agency not having access to that information and without authorisation in the form of a disposal determination.

Resourcing

Sufficient allocation of resources, including budget, infrastructure and staff, is a vital component of an agency's information management program. Staff allocated to perform information management related functions must be appropriately skilled and have the capability to manage their agency's information assets in accordance with this Standard.

[4] PC012 – Information Privacy Principles (IPPS) Instruction

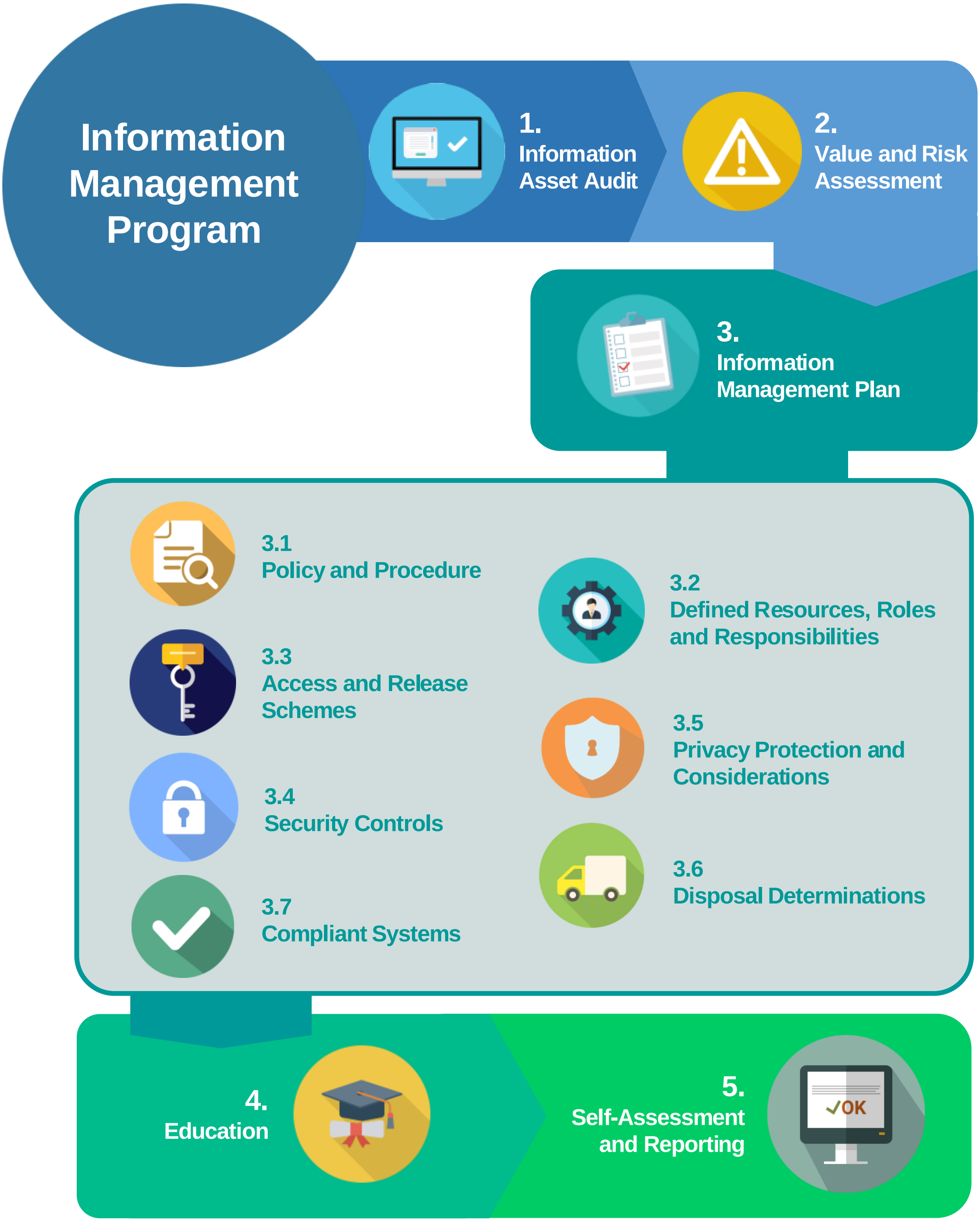
Planning

Like any organisational asset it is important that the management of an agency's information assets are considered and planned at an agency-wide level. An Information Management Plan (Plan) is a core element of an agency's Information Management Program (Program) and should be developed to support the agency's broader strategic and corporate goals and objectives.

The Plan provides practical direction and must be consistent with legislative and business requirements, and should be supported by a broader governance model (Program) incorporating policies, procedures, education and technology.

Progress against the Plan should be regularly assessed and reported on.

Prescribed Governance Model for Information Assets



Information Management Program

1. Information Asset Audit

2. Value and Risk Assessment

3. Information Management Plan

3.1 Policy and Procedure

3.2 Defined Resources, Roles and Responsibilities

3.3 Access and Release Schemes

3.4 Security Controls

3.5 Privacy Protection and Considerations

3.6 Disposal Determinations

3.7 Compliant Systems

4. Education

5. Self-Assessment and Reporting

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 are held. 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 an 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

A 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.

5. Self-assessment and Reporting

Continue to formally assess and review the Program using the Self-Assessment Tool (Tool). This assessment can also assist agencies to understand gaps in their Program and can be used as a first step in the review of the Program.

Refer to the Information Governance Guideline and the Tool for more information on the prescribed governance model and how your agency can comply with the behaviours listed in the Standard.

Version Control

Date approved	Approved by	Date for review	Version
18 June 2019	Attorney-General, SA	31 Dec 2021	1.1
28 June 2021	Director, State Records of SA	31 Dec 2023	1.2
21 April 2023	Director, State Records of SA	12 Dec 2024	1.3

Need further assistance?

State Records
Tel (+61 8) 7322 7081
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au