

Information Management Maturity Report 2023-24 Universities

STATE RECORDS
of South Australia



Government of South Australia
State Records

Table of Contents

Information Management Maturity Report – Universities	2
This report focusses on universities.	2
Survey.....	2
Information Management Standard	2
Definitions	2
Report structure	3
Response rate.....	3
General commentary.....	3
Principle 1 The value of information is known	4
Principle 2 Information assets are created and managed appropriate to risk.....	6
Principle 3 Ownership of information assets is assigned	9
Principle 4 Information assets can be relied upon.....	11
Principle 5 Information assets are available as required.....	13
Information Management Program and Plan	16
Attachment 1: Universities – survey results	18

OFFICIAL

Information Management Maturity Report – Universities

This report focusses on universities.

Survey

In 2023, under section 15 of the *State Records Act 1997* (SR Act), State Records conducted a survey of agencies¹ current information management practices compliance against the Information Management Standard (Standard).

Results are split into different sectors –

- » state government agencies (including boards and committees, minister’s offices and statutory authorities)
- » local government (including subsidiaries and regional subsidiaries)
- » universities

A 2023-24 South Australian (SA) baseline has been provided and includes all sectors results, enabling a comparison against every agency that responded to the survey across the state.

Information Management Standard

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

To comply with the Standard, agencies must satisfy the level 2 (operational) criteria for each behaviour (unless a valid reason can be demonstrated why maintaining a lower level is acceptable e.g. due to agency operational or regulatory requirements or level of risk identified). This will be referred to as the benchmark.

Definitions

Tool – the State Records Self-Assessment Tool (Tool) that enables agencies to assess information governance maturity and compliance against the Standard. The Tool offers a scalable, tiered approach to help identify areas of strength and weakness at each level of maturity and capability. It also generates automated reports that identify the areas agencies need to address as a priority. It has been designed to be used by agencies at any time to aid the improvement of their information management practices, not just when surveyed by State Records.

2023-24 Baseline – the whole of state combined survey result. Includes state government, local government, subsidiaries and regional subsidiaries, universities, boards and committees, minister’s offices and statutory authorities.

Benchmark – for the purposes of this report, the benchmark is the operational level 2 capability for behaviours (from the State Records Self-Assessment Tool (Tool)). To

¹ As defined under section 3(1) of the *State Records Act 1997*

comply with the Standard and reach the benchmark, agencies must score each behaviour at a level 2 capability (unless a valid reason can be demonstrated why maintaining a lower level is acceptable).

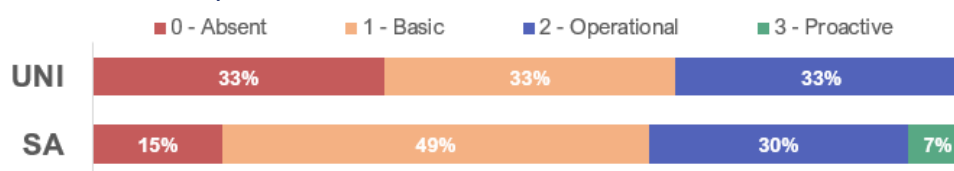
Principle – outlined in the Information Management Strategy, what agencies must follow to ensure their data and information can be relied upon and trusted. Each principle is underpinned by a set of behaviours that agencies must demonstrate to ensure their information management practices align with government expectations.

Behaviour – expected behaviours, under the principles in the Standard, required to effectively manage information, to achieve business objectives and to meet legislative and policy obligations.

Report structure

This report is divided up by principle, then by behaviour. The percentage of maturity ratings for each behaviour reported by universities (UNI) is displayed in a graph and measured against the 2023-24 SA baseline.

For example, the graph below shows that a third of universities rated at the benchmark for behaviour 1.1, compared to 30% of the whole state combined.



The principle graph combines each behaviour into one score and is followed by the behaviour graphs. Additional commentary highlighting points of interest rounds off each principle section.

Response rate

There was a 100% response rate to the survey for universities (all three universities responded).

General commentary

In recognising that one of the reasons for the survey was to establish a baseline to compare future surveys against, it was pleasing to see universities provided an honest account of current information management practices and disclosed there is room for improvement.

Given the small pool of universities in South Australia, it is difficult to identify trends in information management practices without identifying what scores were provided for each university.

Collectively, universities scored:

- » below the 2023-24 baseline for all the principles
- » at the benchmark for 10 out of the 33 behaviours (approximately 30%)
- » below the benchmark for the Information Management Plan and Program

See Attachment 1 for a table of consolidated results for universities.

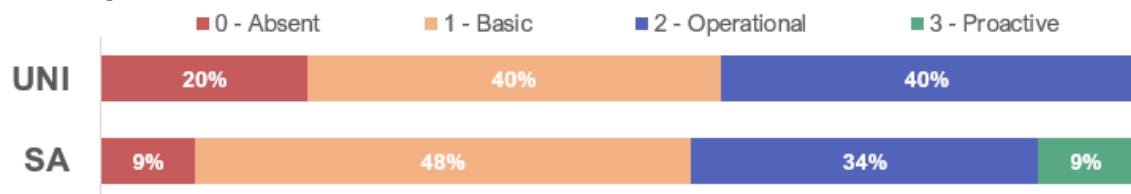
OFFICIAL

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.

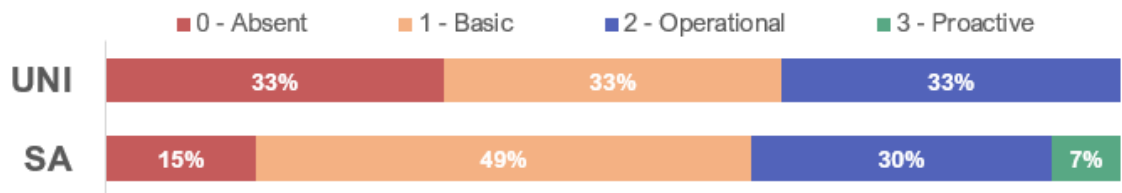
Principle Result



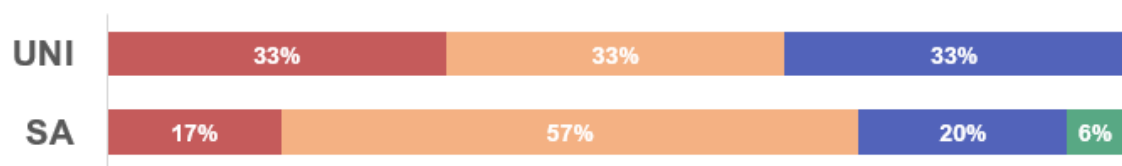
Universities are operating just below the 2023-24 baseline for principle 1.

Behaviours

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

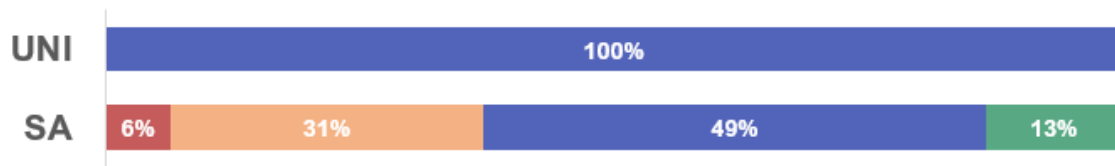


1.3 Ensure information assets are linked to business functions and activities



OFFICIAL

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



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



Principle 1 - Commentary

To achieve the benchmark for principle 1, universities need to:

- » complete an audit on hardcopy and digital information assets
- » create an information asset register that captures all assets
- » conduct a value and risk assessment
- » apply a business classification scheme (or similar) to all information assets in the information asset register
- » provide all new staff with a basic induction to information management and all information management staff with comprehensive information management training
- » have a clear strategic direction for the management of information assets

Under principle 1, universities are operating above the 2023-24 baseline for behaviours 1.2 and 1.4 and below the baseline for behaviours 1.1, 1.3 and 1.5.

For behaviour 1.3, no university is operating at the benchmark. This signifies for universities, some have a business classification scheme, or something similar applied and there is a general understanding of what information exists and how they are linked to business functions and activities.

100% of universities responded to behaviour 1.4 at the benchmark indicating all new staff are provided with basic induction for information management and comprehensive information management training is provided to information management staff.

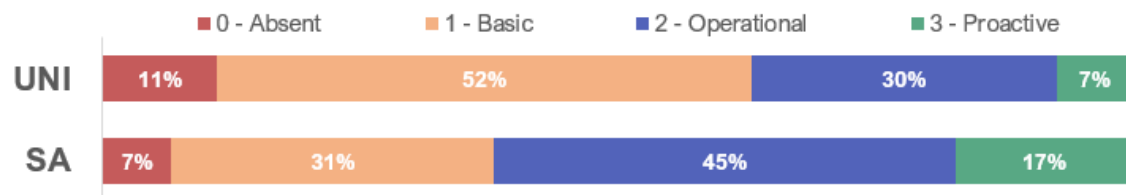
OFFICIAL

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.

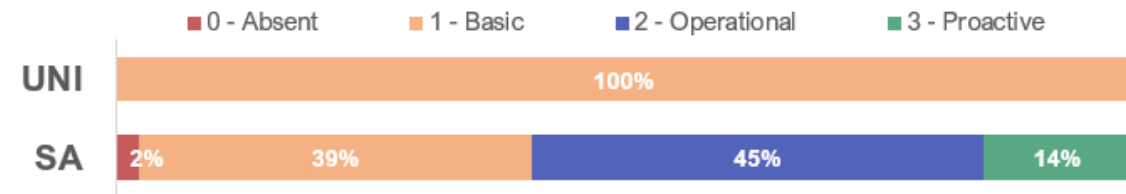
Principle Result



Universities are operating below the 2023-24 baseline for principle 2.

Behaviours

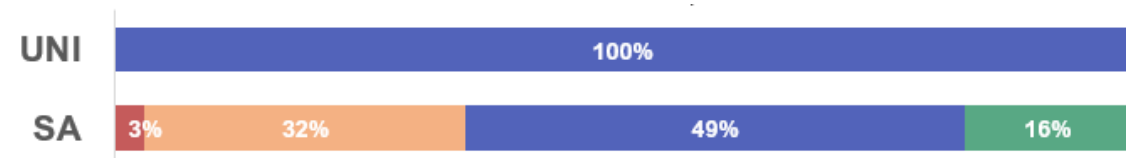
2.1 Analyse and document what information assets must be created and managed across the agency applicable to the regulatory environment in which they operate



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

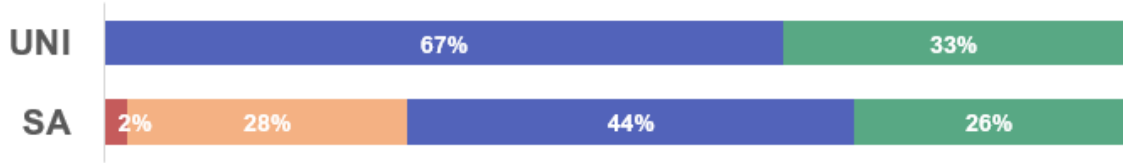


2.3 Assess the risks of not creating or managing information assets where there is a legal, evidential, or business need



OFFICIAL

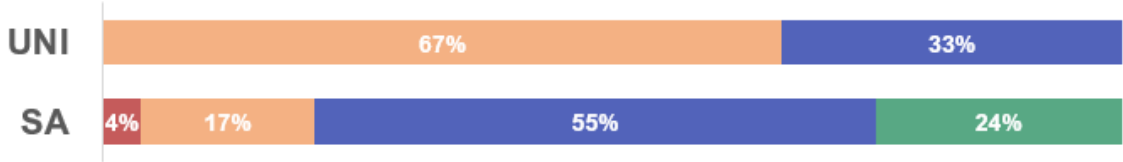
2.4 Manage information assets digitally unless there are specific reasons for keeping hardcopy information assets



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



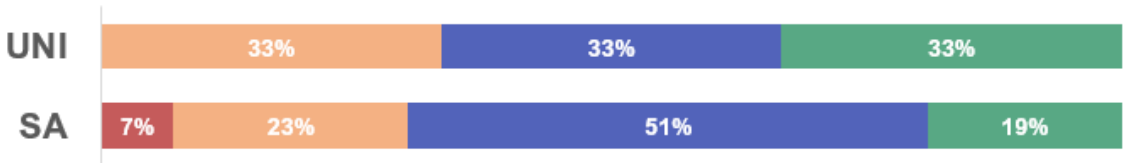
2.6 Manage and store information assets appropriately, to ensure they remain accessible for as long as required



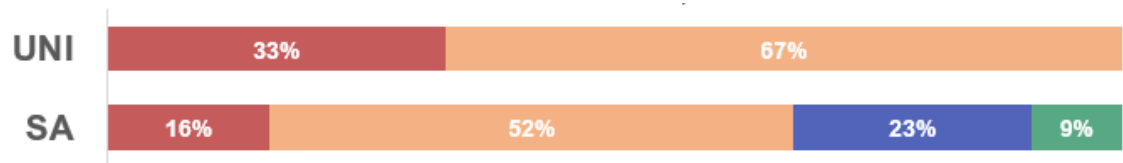
2.7 Only destroy information assets when no longer required, and in accordance with current, approved disposal determinations issued by State Records



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



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



OFFICIAL

Principle 2 - Commentary

To achieve the benchmark for principle 2, universities need to:

- » analyse and document requirements to create and manage information assets
- » have policies and procedures that outline the management of information assets
- » identify risks from not creating or managing information assets
- » move away from hybrid digital and hardcopy information assets and mostly digitally manage information assets
- » design/configure critical systems (including an EDRMS) according to information management standards and business requirements
- » manage and store information appropriately
- » plan and regularly implement destruction of information when no longer needed for legal, business or other purpose
- » report consistently on staff adherence to information management policies

Universities are operating below the 2023-24 baseline for most of the behaviours under this principle, except 2.3 and 2.4.

All universities scored at the basic level for behaviour 2.1 indicating some requirements to create and manage information in universities is analysed and documented.

Universities are assessing the risks of not creating or managing information where there is a legal, evidential, or business need well, with benchmark scores across all universities for behaviour 2.3.

Universities operate at or greater than the benchmark for behaviour 2.4 indicating universities have digitised systems for their information moving away from hybrid digital and hardcopy records.

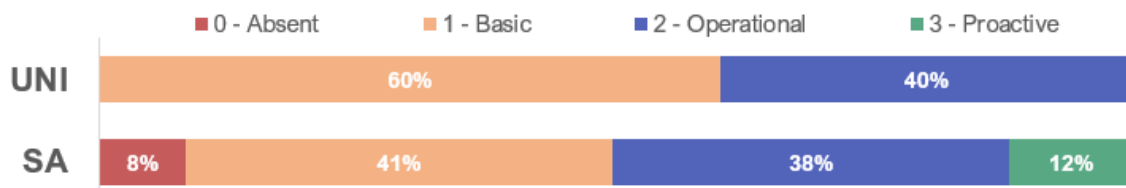
No university is at the benchmark level for behaviours 2.1, 2.5, 2.7 and 2.9.

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.

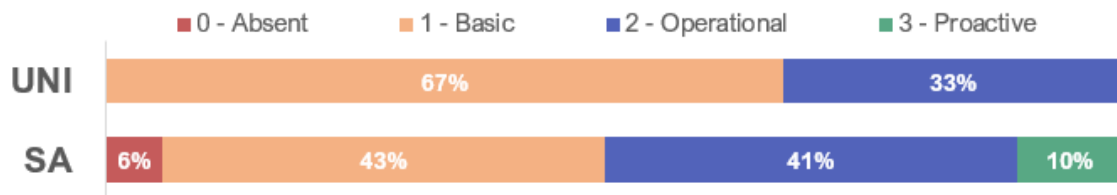
Principle Result



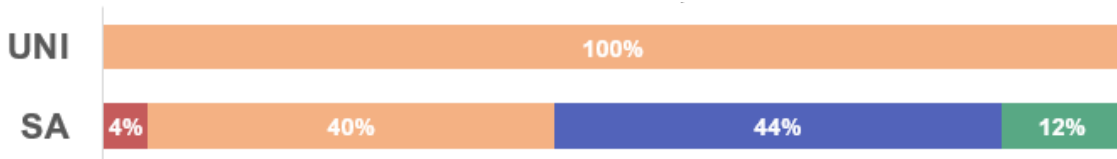
Universities are operating just below the 2023-24 baseline for principle 3.

Behaviours

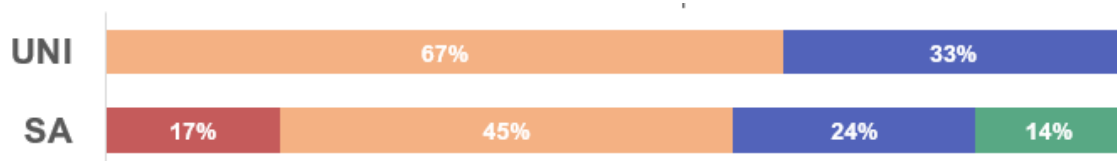
3.1 Ensure ownership of information assets are assigned



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

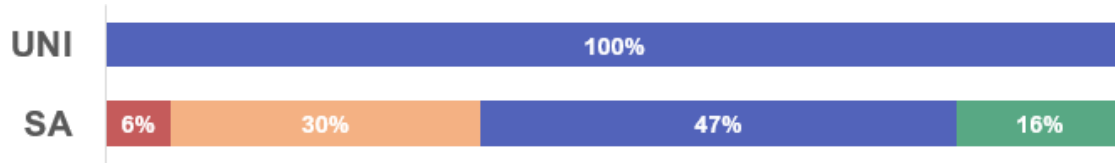


3.3 Ensure responsibilities for information assets management are delegated appropriately, in writing



OFFICIAL

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.



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



Principle 3 – Commentary

To achieve the benchmark for principle 3, universities need to:

- » assign owners to all information assets who are responsible for their management
- » formally delegate information management responsibilities in writing
- » formally document information roles and responsibilities in policies, position descriptions and governance documents
- » consistently implement accountability structures

For principle 3, universities are operating below the 2023-24 baseline for all behaviours except behaviours 3.4.

For the behaviours under this principle, universities mainly scored at the basic level. This could indicate that responsibilities relating to information management could be improved.

All universities scored basic for behaviour 3.2 indicating owners may not be aware of their responsibilities and accountabilities for managing information.

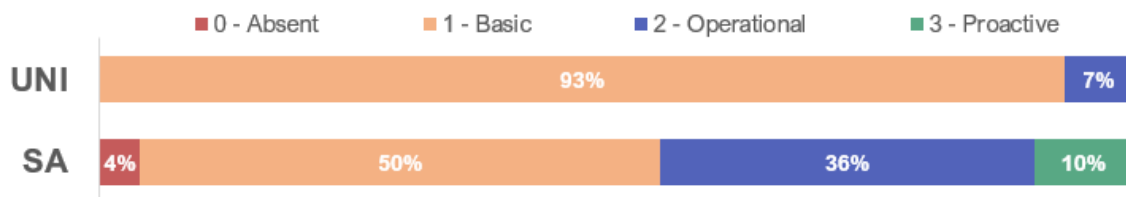
From the scores provided for behaviour 3.4 (benchmark for all universities), universities ensure that roles and responsibilities relating to the ownership and management of information are clearly defined in policy or other internal documents.

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.

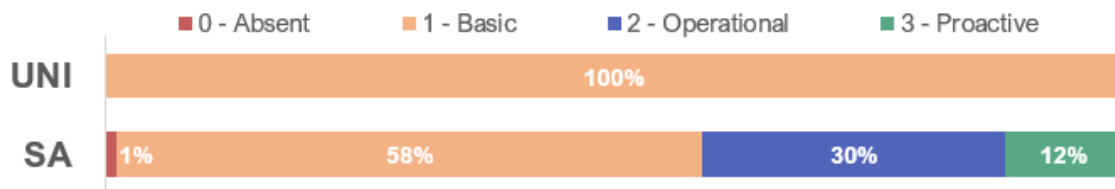
Principle Result



Universities are operating below the 2023-24 baseline for principle 4.

Behaviours

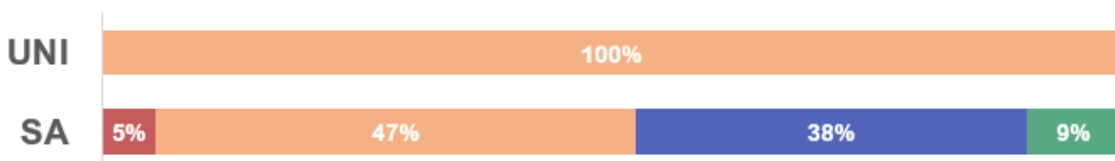
4.1 Create and keep full and accurate information assets appropriate to their business processes, regulatory environment and risk and accountability requirements



4.2 Ensure information assets are saved into systems in a timely manner that meet relevant Standards and whole of government security Frameworks to ensure they are protected from compromise

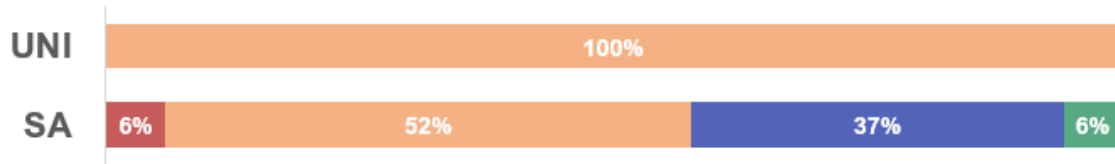


4.3 Record relevant details (metadata) in systems so that the business context of information can be readily understood

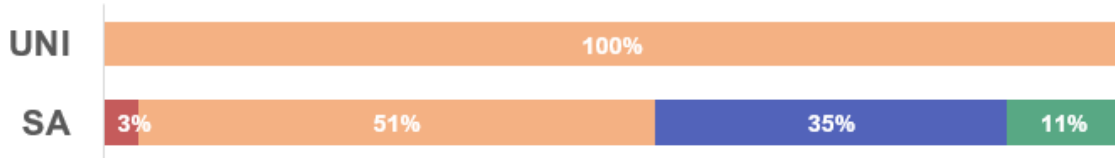


OFFICIAL

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



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



Principle 4 - Commentary

To achieve the benchmark for principle 4, universities need to:

- » create and keep, full and accurate information assets with identified requirements and the value and risk assessment undertaken
- » save information assets (in a timely manner) into protected business or information systems that meet Standards, frameworks and metadata requirements.
- » ensure all business or information systems manage the minimum metadata requirements of the Minimum Recordkeeping Metadata Requirements Standard
- » use established and existing information definitions
- » implement practices and systems to ensure quality and authenticity of information assets

Universities are operating below the 2023-24 baseline for every behaviour under principle 4.

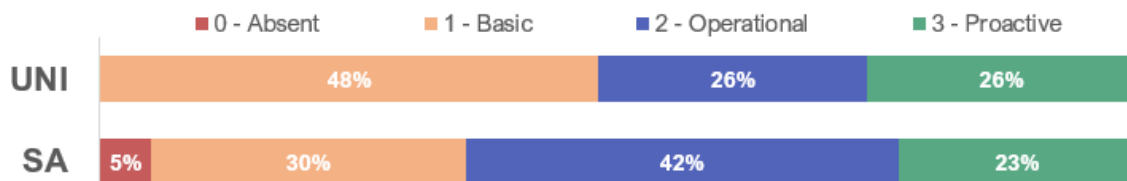
As can be seen from the charts above, almost all scores for universities under this principle were at the basic level. This could indicate that universities don't always create and keep full and accurate documents and they aren't always saved in business or information systems. Some systems manage metadata and some do not.

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.

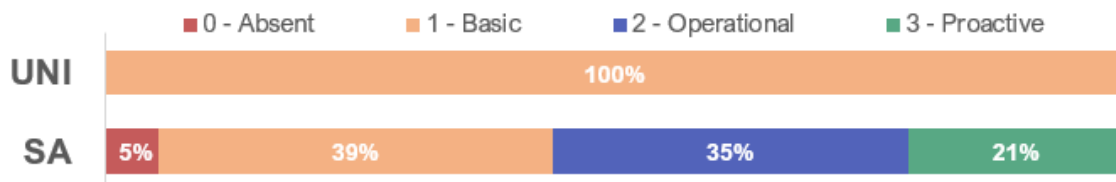
Principle Result



Universities are operating below the 2023-24 baseline for principle 5.

Behaviours

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

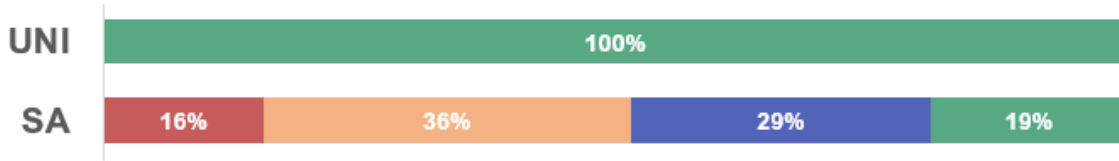


5.3 Migrate digital information assets as systems, software and media are upgraded or become obsolete to ensure it remains accessible for as long as it is required

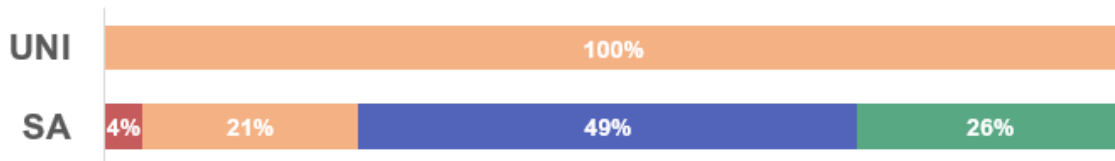


OFFICIAL

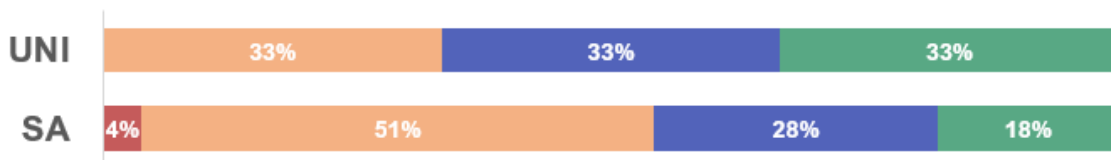
5.4 Identify requirements for retaining information assets not covered by general disposal schedules, and seek a disposal determination for these information assets



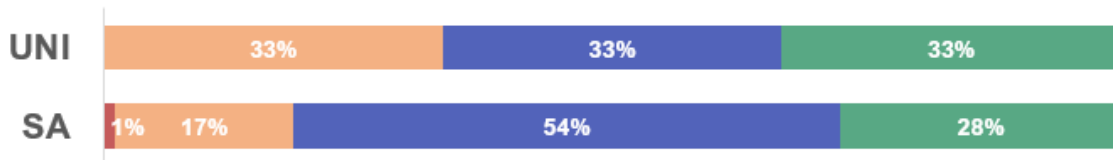
5.5 Ensure that no information asset is destroyed unless in accordance with current, approved disposal determinations



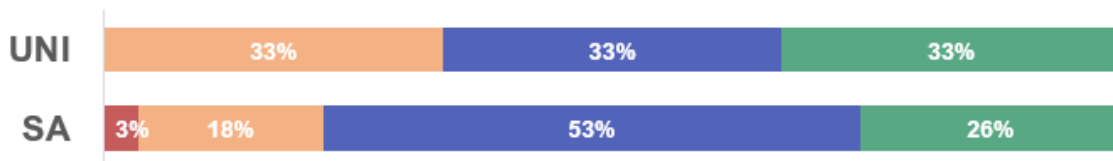
5.6 Collect, use, disclose, store, and dispose of personal information in accordance with the information privacy principles



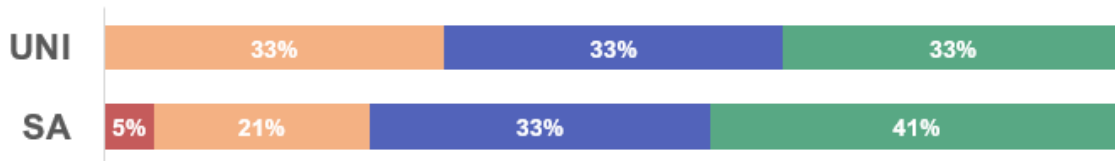
5.7 Share information across government as appropriate or where authorised



5.8 Proactively publish information in line with government policy



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.



OFFICIAL

Principle 5 - Commentary

To achieve the benchmark for principle 5, universities need to:

- » ensure information security classifications are appropriately applied to all information assets
- » regularly review and update access restrictions
- » plan migration of information when systems are upgraded or before they become obsolete
- » have a records disposal schedule (approved by State Records Council) that covers all information assets
- » destroy information assets through authorised and current approved disposal determinations
- » collect, use, disclose, store and dispose of personal information appropriately
- » undertake privacy impact assessments for projects and initiatives
- » share information in line with information sharing protocols
- » proactively publish information in line with policy or legislation, or as requested
- » sell or donate information through an authorised process

For the behaviours under principle 5, universities results vary. Universities are operating:

- » above the 2023-24 baseline for behaviours 5.4 and 5.6
- » below the 2023-24 baseline for behaviours 5.1, 5.2, 5.3, 5.5, 5.7, 5.8 and 5.9.

100% of universities scored at the basic level for behaviour 5.1. This indicates that information security classifications are applied to some information assets, but not all.

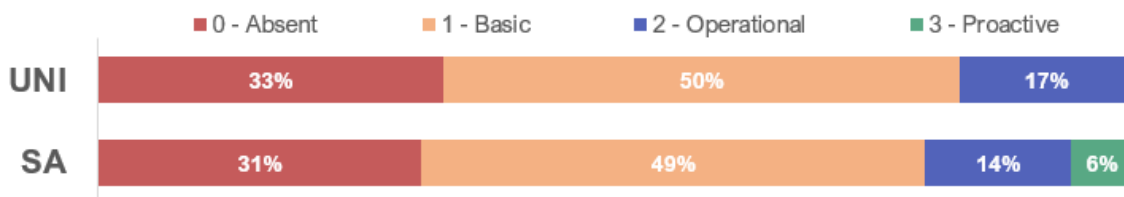
All universities operate at a proactive level (above the benchmark) for behaviour 5.4, indicating universities have current agency specific records disposal schedules which are reviewed and updated in response to administrative, functional or legislative changes.

All universities scored at the basic level for behaviour 5.5 signifying some information is destroyed in accordance with current approved disposal determinations but some destruction is also occurring outside of a disposal determination.

Information Management Program and Plan

An Information Management Plan provides practical direction for implementing a Program and is a core element of an agency’s Information Management Program. It should be developed to support the agency’s broader strategic and corporate goals and objectives.

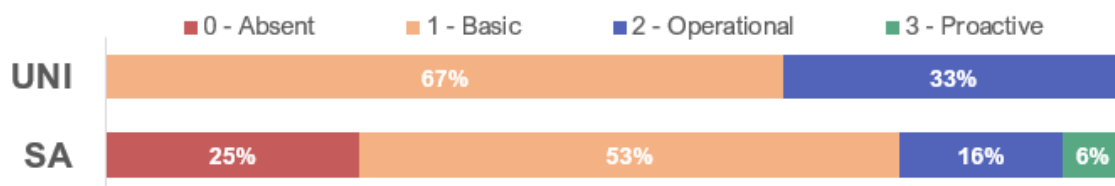
Result



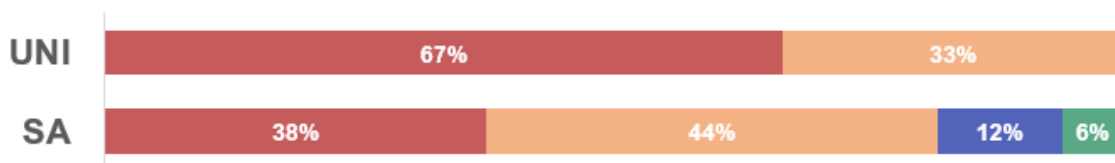
Universities are operating just below the 2023-24 baseline for the Program and Plan.

Behaviours

iii.1 An information Management Plan exists



iii.2 Progress against the Information Management Plan is assessed and reported on



Principle iii - Commentary

To achieve the benchmark for principle iii, universities need to:

- » have an information management plan that encompasses all information assets and business systems
- » monitor and assess progress against the plan

Universities are operating below the 2023-24 baseline for principle iii.1 indicating information management plans are in place with some actions defined and implemented.

However, pursuant to iii.2 processes to assess and report against the program and plan appear to be limited or non-existent.

OFFICIAL

As the requirement to establish an Information Management Program and Plan is new to the Standard, all organisations surveyed are well below the benchmark.

OFFICIAL

Attachment 1: Universities – survey results

This attachment provides a summary of the most common maturity ratings (also known as the Mode) reported by universities. It also identifies the variance against the benchmark.

Principles and Behaviours		Benchmark (Standard)	State Mode 2024	Uni Mode 2024	Variance (Benchmark)
Principle 1 - the value of information is known					
1.1	Identify and document what their information assets are, where they are stored and who is responsible for their management	2	1	1	↓ 1
1.2	Understand and document how their information assets support their business objectives and operations or their compliance obligations	2	1	1	↓ 1
1.3	Ensure information assets are linked to business functions and activities	2	1	1	↓ 1
1.4	Induct and train staff in the value of information and in their information management responsibilities	2	2	2	-
1.5	Foster an organisational culture that values and manages information as an asset and supports business objectives and activities	2	1	1	↓ 1
Principle 2 – information assets are created and managed appropriate to risk					
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	1	↓ 1
2.2	Develop and issue policies and procedures outlining how information assets will be managed	2	2	1	↓ 1
2.3	Assess the risks of not creating or managing information assets where there is a legal, evidential, or business need	2	2	2	-
2.4	Manage information assets digitally unless there are specific reasons for keeping hardcopy information assets	2	2	2	-
2.5	Design and implement systems according to relevant standards so that they support the effective management and disposal of information assets	2	2	1	↓ 1
2.6	Manage and store information assets appropriately, to ensure they remain accessible for as long as required	2	2	1	↓ 1
2.7	Only destroy information assets when no longer required, and in accordance with current, approved disposal determinations issued by State Records	2	1	1	↓ 1

OFFICIAL

Principles and Behaviours		Benchmark (Standard)	State Mode 2024	Uni Mode 2024	Variance (Benchmark)
2.8	Review and audit how well their information management policies and practices support their business	2	2	2	-
2.9	Monitor, report and improve staff adherence to internal information management policies	2	1	1	↓ 1
Principle 3 – ownership of information assets is assigned					
3.1	Ensure ownership of information assets are assigned	2	1	1	↓ 1
3.2	Ensure that owners are aware of their responsibilities and accountabilities for managing the information assets	2	2	1	↓ 1
3.3	Ensure responsibilities for information assets management are delegated appropriately, in writing	2	1	1	↓ 1
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.	2	2	2	-
3.5	Ensure that ownership and accountability for information assets are managed consistently through a governance structure	2	1	1	↓ 1
Principle 4 – information assets can be relied upon					
4.1	Create and keep full and accurate information assets appropriate to their business processes, regulatory environment and risk and accountability requirements	2	1	1	↓ 1
4.2	Ensure information assets are saved into systems in a timely manner that meet relevant Standards ¹ and whole of government security Frameworks to ensure they are protected from compromise	2	1	1	↓ 1
4.3	Record relevant details (metadata) in systems so that the business context of information can be readily understood	2	1	1	↓ 1
4.4	Use established and existing definitions for information assets where possible, so that there is consistency across the agency	2	1	1	↓ 1
4.5	Implement practices and systems that ensure the quality and authenticity of information assets.	2	1	1	↓ 1

Principles and Behaviours		Benchmark (Standard)	State Mode 2024	Uni Mode 2024	Variance (Benchmark)
Principle 5 – information assets are available as required					
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	2	1	1	↓ 1
5.2	Review access restrictions on information and amend as sensitivity alters	2	1	1	↓ 1
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	2	2	1	↓ 1
5.4	Identify requirements for retaining information assets not covered by general disposal schedules, and seek a disposal determination for these information assets	2	1	3	↑ 1
5.5	Ensure that no information asset is destroyed unless in accordance with current, approved disposal determinations	2	2	1	↓ 1
5.6	Collect, use, disclose, store, and dispose of personal information in accordance with the information privacy principles	2	1	2	-
5.7	Share information across government as appropriate or where authorised	2	2	2	-
5.8	Proactively publish information in line with government policy	2	2	2	-
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.	2	3	2	-
Program and Plan					
iii.1	An information management plan exists	2	1	1	↓ 1
iii.2	Progress against the information management plan is assessed and reported on	2	1	0	↓ 2

OFFICIAL

Need further assistance?

State Records

Tel (+61 8) 7322 7081

Email staterecords@sa.gov.au

Web www.archives.sa.gov.au

OFFICIAL