TAHO
Tasmanian Archive + Heritage Office

State Records Guideline No 25

Managing Information Risk

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

Table of Contents

Information Security Classification

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

Document Development History

Build Status

Version	Date	Author	Reason	Sections
2.0	03-06-2015	Christine Woods	Template	All
1.0	17-09-2014	Samara McIlroy	Initial Release	All

Amendments in this Release

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

Issued: September 2014

Ross Latham
State Archivist

1 Introduction

Information enables Tasmanian government to operate transparently, accountably, legally and efficiently. The pace of change in the digital age means new risks to information can appear quickly, and may not be as visible as other risks such as financial or physical threats. However, the consequences of information loss due to insufficient consideration of risks could be very serious. The application of risk management processes to address information risks will assist agencies to adapt to doing business in a digital environment, and to comply with the *Archives Act 1983*

1.1 Purpose

The purpose of this Guideline is to set down risk management processes that are approved by the State Archivist for management of State records. This Guideline also supports Guideline 1 - Records Management Principles, which requires agencies to conduct risk analysis as part of their Records Management program. An Advice on Risk Management has also been developed to assist agencies to implement these processes.

1.2 Authority

This guideline is issued under the provisions of Section 10A of the *Archives Act 1983*. Guidelines issued by the State Archivist under this Section set standards, policy, and procedures relating to the making and keeping of State records. This section also requires all relevant authorities to take all reasonable steps to comply with these guidelines, and put them into effect.

Keyword	**Interpretation**
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS RECOMMENDED	The item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in capitals throughout the Guideline. Agencies deviating from these MUST advise TAHO of the decision to waive particular requirements.

Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

Agencies deviating from a 'RECOMMENDS' or 'RECOMMENDED' requirement are encouraged to document the reasons for doing so.

2 Risk Management and Information

2.1 Overview

Information is at the core of government business, and is a core agency asset. Information management strategies must be developed and implemented to support this core asset.

Applying risk management processes is crucial to effectively managing information in the digital environment, and can assist agencies to:

- Develop an information governance framework to meet accountability, probity and legal requirements
- Support the identification and implementation of information security requirements
- Support the development, integration, upgrading and decommissioning of business systems, and the transition to new systems
- Identify information risks associated with outsourcing or using cloud services
- Contribute to agency-wide risk assessments by identifying information risks, and inform agency business continuity and disaster recovery plans
- Support information sharing between agencies and with the public
- Implement training and support for users to understand, leverage and utilise business information
- Manage digital continuity so that information will continue to meet business, client and accountability needs into the future
- Ensure State records remain usable and accessible for the duration of their retention as stipulated in authorised Retention and Disposal Schedules

Adopting a risk management approach assists agencies to identify and prioritise high risk business areas and apply appropriate levels of control where risks to information are highest.

2.2 Risk management

A **risk** is defined in the Australian Standard *AS/NZ ISO 31000:2009* as the 'effect of uncertainty on objectives.' This can be positive or negative, but in practice usually refers to threats or other factors that may adversely affect outcomes. The objective of **risk management** is to control risk in a structured way in order to minimise any negative effects of risk. Risk management describes any processes that identify, analyse and respond to risks.

Conducting a **risk assessment** involves:

- Identifying inherent risks and evaluating likelihood and consequences,
- Identifying all existing controls and other mitigation strategies,
- Understanding any residual risk (likelihood and consequence) to identify high priority risks for action or treatment.

NOTE: For more guidance on conducting risk assessments, see *Advice 60: Part Two - Applying Risk Management Processes.*

2.3 Risks to State records

Agencies MUST apply risk Management processes to State records in all formats

Agencies often do not consider how poor recordkeeping practices contribute to broader operational and business risks. Risk assessments are a useful tool for identifying those areas where information and records may be at risk. Risk analysis also assists to prioritise areas of information risk that need more intensive treatment. These areas can be brought to management attention and prioritised when developing or improving organisational recordkeeping controls.

2.4 Mitigating business risk by making records

Agencies MUST undertake information risk assessments for core business areas

Business risks could expose your agency or the government to serious consequences. A strong information management regime SHOULD be one of your primary risk mitigation strategies. You can protect your agency by applying risk management processes as a component of your Records Management Program.

Agencies MUST undertake an information risk assessment for each of the agency's core business areas and look for processes and activities that:

- Receive a high level of public and media scrutiny
- Instigate or are subject to litigation
- Allocate or spend large amounts of money (Government Procurement Guidelines require purchases valued at $250,000 or more go to public tender)
- Relate to issues of security
- Are outsourced
- Undergo administrative change (e.g. the reassignment of functions between State government departments)
- Are conducted in cloud-computing systems (refer to our Cloud Computing Guideline 17)
- Relate to the health, welfare, rights and entitlements of citizens and/or staff
- Involve organisational change management and/or transitioning to new systems
- Relate to employment conditions of staff

Records documenting high risk business activities generally need to be more detailed and of a higher quality than those that document low risk activities. Such records will therefore require more intensive management to ensure that they provide evidence of proper accountability.

Any strategic and specific risk assessments such as legal compliance, audit or fraud risk assessments SHOULD also consider misuse or mismanagement of information and other recordkeeping risks.

2.5 Risks associated with managing records

> Risk management processes MUST cover records in all formats, including digital records outside formal recordkeeping systems. Risk assessments MUST be undertaken for all Permanent records.

There are higher risks associated with particular record formats or record types, including digital records such as email, websites and records held in business systems. These record types will require more intensive management to ensure that they are accurate, authentic, have integrity and are useable for the entire lifecycle of the records.

Record formats which MUST be considered in risk management processes include:

Permanent records - records that MUST be transferred to TAHO 25 years after the date of creation for retention as State archives (or a transfer exemption MUST be applied for.)
Vital records - records that are essential for the ongoing business of an agency, and without which the agency could not operate effectively. The primary object of records management disaster planning is to identify and manage vital records.
Unscheduled records - unscheduled records are records not covered by an approved Retention and Disposal Schedule (R&DS).
Unstructured digital records - information created without strict controls (e.g. documents on network drives and emails).
Digitised records - records transformed into a digital form from an analogue form (e.g. a paper record which has been scanned).
Records in **business systems** that have a retention period of over five years
Records in **business systems** that are about to undergo migration
Records stored in **cloud-computing systems** and applications (e.g. Dropbox, Docs on Tap)
Records that contain **sensitive and security classified information**
Records in **hybrid environments** with content created in both paper and digital formats
Records of decision-making, policy or advice delivered via **telephone**
Records of decision-making, policy or advice delivered using **websites, social media or Web 2.0 technology**
Records stored or transmitted via **mobile devices**

Agencies MUST undertake risk assessments of all permanent records in the agency, including any permanent records held in business systems which support the agency's core business. Permanent records MUST NOT be destroyed, and will need to be appropriately managed for 25 years in the agency before transfer to TAHO, unless a transfer exemption is granted.

2.6 Implementing risk management

> Risk analysis MUST underpin records management operations, to ensure that risks to the agency's records and recordkeeping systems are minimised. Records management staff MUST ensure that risks to the agency's records and recordkeeping systems, especially vital records, are addressed as part of the agency's Records Management Program.

Agency records may be stored in a variety of business systems, in localised and cloud-based applications, social media sites and on portable devices. Managing records in such a complex environment can be a daunting prospect. In a hybrid digital/hard-copy environment, implementing risk management processes will assist in identifying and managing those risks, bringing significant benefits as well as providing evidence of proper accountability.

Benefits of managing information risks include:

- Contributes to the smooth operation of your agency's programs by identifying the information needed for decision making and service delivery
- Facilitates effective performance of business activities throughout the agency
- Protects the rights of the agency, employees and stakeholders
- Provides continuity in the event of a disaster
- Protects records from inappropriate and unauthorised access

If risk assessments of State records are left out of broader strategic risk assessments, Records staff MUST address these risks as part of their records management operations. They MUST ensure that risks to the agency's records and recordkeeping systems, especially vital records, which are essential for the agency to function effectively, are addressed as part of the Records Management Program scope. See *Advice 52 -Identifying and Managing Vital Records.*

To determine where records-related risks exist, use the risk management processes outlined in *Advice 60: Part Two - Applying Risk Management Processes* to assess the agency's current Records Management Program and what actions are required to ensure compliance with this Guideline. A new technical report, *ISO/TR 18128:2014 Information and documentation - Risk assessment for records processes and systems* is another useful resource.

3 Aligning Records Management and Risk Management functions

3.1 Overview

Risk management is recognised as an essential component of good management practice in the Tasmanian Government (see Tasmanian Government Project Management Guidelines V7.0). This section of the Guideline describes actions that agencies can take to link records management to risk management at both a strategic and operational level.

Linking records management to risk management may be achieved by; integrating information risk into the agency's existing risk management regime, and applying risk management processes specifically to manage State records.

3.2 Benefits

The advantage of aligning the records management and risk management functions across the agency is that both business risks and information and recordkeeping risks will be consistently identified and addressed. Other benefits include:

- Continuous improvement of agency processes and practices
- Encouraging a high standard of accountability
- Supporting better business decision making
- Compliance with legal and regulatory requirements, such as the *Archives Act 1983*
- Protecting staff, assets, visitors, property and reputation

Ideally, Records Management staff will be involved in planning agency-wide risk mitigation strategies. However, Records Managers can also apply risk management processes to those operational areas for which they have direct responsibility. Examples include:

- Records and Archives storage areas
- Corporate recordkeeping systems such as Electronic Document and Records Management Systems (EDRMS)
- Records disposal programs
- Records Management training and induction

Raising staff awareness of agency-wide recordkeeping risks through communication and training can also be addressed as part of Records Management core business.

3.3 Strategic Alignment

Agencies MUST align the functions of records management and risk management strategically.

To achieve alignment at a strategic level, reports about information risks SHOULD be directed to the agency Risk Management Steering Committee, if there is one. Agencies that do not have an established risk management program can direct reports about information risks to their Manager of Corporate Services and/or the agency's Executive.

For successful alignment, information risks SHOULD be included in the agency-wide Risk Register. Senior management SHOULD coordinate the risk management process and ensure that it is implemented across the whole agency.

Other ways that strategic alignment of records management and risk management can be achieved are by:

- Ensuring that the agency has a Risk Management Strategy which references information management, and addresses information risks and impacts on agency operations.
- Any agency risk assessments, such as legal compliance, audit or fraud risk assessments, also considering information risks.
- Aligning agency risk management and records management policies, ensuring that each policy refers to the other and the terminology used in both documents is the same. TAHO RECOMMENDS that these policies align in order to ensure that all agency responsibilities and directives are consistent with each policy.
- Ensuring that responsibility for both risk management and records management is assigned to appropriate agency staff, all the way up to management level. This includes specifying clear ownership of information risks, and who is responsible for treating or escalating risks, in line with the agency's governance structure.

3.4 Operational alignment

Agencies MUST align the functions of records management and risk management operationally.

Before commencing any risk management processes, it is RECOMMENDED that Records Management staff consult the agency's Risk Manager (or equivalent). This will ensure that a common understanding of the outcomes can be achieved, using each other's processes if possible.

Operational alignment of records management and risk management can be achieved by:

- Establishing an Information Risk Register for the Records Management unit.
- Recording information risks in the agency-wide Risk Register, not just the risk register which is kept within the Records Management unit.
- Establishing regular communication between the Risk and Records Management teams to ensure that work processes are aligned, and a common language is established.
- Implementing regular self-assessments and internal audit programs which assess recordkeeping practices across the agency. Such programs could be jointly managed by both Risk and Records Management staff.
- Promoting good recordkeeping as a risk mitigation tool to agency staff through regular newsletters, via the intranet, at staff meetings or through the induction process.
- Implementing processes for agency employees to take responsibility for identifying and reporting potential risks around information and recordkeeping, such as:
- Conducting spot checks which assess recordkeeping practices
- Scheduling performance-based reporting in EDRMS systems (eg. Regular staff management of tasks collated & sent to supervisors)
- Adding a specific agenda item to staff meeting templates
- Include identifying information risks as part of the procurement process for new systems
- Providing regular training to agency staff on what is good recordkeeping practice, and the risks and consequences associated with poor recordkeeping practices.

3.5 Reporting alignment

It is RECOMMENDED that agencies align the reporting of information risks with existing risk management reporting processes.

If risk management is established and more widely understood than records management in the agency, it may be wise to report information risks using existing risk reporting templates. Other reports that can assist when identifying and reporting information risks include:

- System generated reports from EDRMS and business systems
- Self-assessment questionnaires
- Internal and external audit reports
- Information Asset Register
- The agency's Corporate Risk Register

4 Monitoring and Review

Agencies MUST review their Information Risk Register annually.

Agencies MUST ensure that the Information Risk Register is up-to-date and regularly reviewed. When identified information risks are treated, and controls are improved or implemented, they may alter risk priorities or risk mitigation efforts. The Risk Register is an ideal tool for measuring compliance with Guidelines and Advice issued by TAHO. It also provides a means to review agency recordkeeping practices and the efficacy of the records management program.

If an identified information risk turns into an event that happens, the event SHOULD be reviewed by the risk owner or business owner in a timely fashion, and the review findings SHOULD be implemented. In addition, agencies SHOULD conduct a risk assessment workshop every three years to identify any new information risks.

5 Definitions

Information risk is any risk which relates to the inherent characteristics and value of information in any form that is maintained by an agency and which may be transmitted, manipulated, and stored.

Records are the subset of information that constitutes any evidence of activities.

A **risk** is defined in the Australian Standard AS/NZ ISO 31000:2009 as the 'effect of uncertainty on objectives,' which can be positive or negative, but in practice usually refers to threats or other factors that may adversely affect outcomes.

Risk analysis is the overall process to comprehend the nature of risk and to determine the level of risk.

Risk assessment is the process of identifying, analysing and evaluating risks.

Risk control is a measure to modify risk. Controls are the result of risk treatment, and include any policy, process, device, practice or action designed to modify risk.

Risk management - The objective of risk management is to control risk in a structured way in order to minimise any negative effects of risk and optimise positive effects. Risk management describes any processes that identify, analyse and respond to risks.

Risk mitigation is the systematic reduction of risk.

Further Advice

For more detailed advice, please contact:

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

Acknowledgements

- Tasmanian Government Project Management Guidelines V7.0
- Advice 60: Part Two - Applying Risk Management Processes (forthcoming TAHO Advice)
- Australian Standard for Risk Management AS/NZ ISO 31000:2009
- ISO/TR 18128:2014 Information and documentation - Risk assessment for records processes and systems
- *Disaster Preparedness and Recovery (2012: Advice 26)*

6 Checklist of minimum requirements

Managing information risk		**Compliance Achieved?**
1.1	Agencies MUST apply risk management processes to State records in all formats.	
1.2	Agencies MUST undertake an information risk assessment for each of the agency's core functional business areas.	
1.3	A strong information management regime SHOULD be one of your primary risk mitigation strategies.	
1.4	Strategic and specific risk assessments such as legal compliance, audit or fraud risk assessments SHOULD consider misuse or mismanagement of information and other recordkeeping risks.	
1.5	Risk management processes MUST cover records in all formats, including digital records outside formal recordkeeping systems, such as email, websites and business systems. See *Advice 60 - Part Two: Applying Risk Management Processes* for more on information and recordkeeping risks.	
1.6	Risk assessments MUST be carried out for all permanent records, including permanent records held in business systems. Permanent records MUST NOT be destroyed, and will need to be appropriately managed for 25 years in the agency before transfer to TAHO, unless an exemption is granted.	
1.7	Risk management processes MUST underpin records management operations, to ensure that risks to the agency's records and recordkeeping systems are minimised.	
1.8	Records management staff MUST ensure that risks to the agency's records and recordkeeping systems, especially vital records, are addressed as part of the agency's Records Management Program.	
1.9	Agencies SHOULD consider records as part of the agency's broader risk management program.	

Aligning Risk Management and Records Management		**Compliance Achieved?**
2.1	Agencies MUST align the functions of records management and risk management strategically and operationally.	
2.2	It is RECOMMENDED that the agency Records Management Policy and Risk Management Policy are aligned to ensure that all responsibilities and directives are consistent.	
2.3	It is RECOMMENDED that Records Managers consult with Risk Managers before commencing any risk management processes.	
2.4	Agencies SHOULD include information risks in the agency-wide Risk Register.	
2.5	Reports about information risks SHOULD be directed to the agency Risk Management Steering Committee or to the agency's Executive Management if no committee exists.	
2.6	Senior management SHOULD coordinate the process and ensure that it is implemented agency-wide.	
2.7	It is RECOMMENDED that agencies align the reporting of information risks with existing risk management reporting processes.	
2.8	Agencies MUST review their Information Risk Register annually.	
2.9	If an identified information risk turns into an event that happens, the event SHOULD be reviewed by the risk owner or business owner in a timely fashion, and the review findings SHOULD be implemented.	
2.10	Agencies SHOULD conduct a risk assessment workshop every 3 years to identify any new information risks.	

7 Evidence that supports mandatory requirements

Ref.	Mandatory Requirement	Evidence
1.1	Agencies MUST apply risk management processes to all State records	• - Information Risk Register • - Information Asset Register • - Audit reports that consider information risks
1.2	Agencies MUST undertake an information risk assessment for each of the agency's core functional business areas.	• PESTLE and SWOT analysis • Risk Assessment Worksheets
1.5	Risk management processes MUST cover records in all formats, including digital records outside formal recordkeeping systems, such as email, websites and business systems.	The following cover all record formats: • Information Risk Register • Information Asset Register • Retention & Disposal Schedule
1.6	Risk assessments MUST be carried out for all permanent records, including permanent records held in business systems.	• Risk Assessment Worksheets • Approved and current functional Retention & Disposal Schedule
1.7	Risk management processes MUST underpin records management operations, to ensure that risks to the agency's records and recordkeeping systems are minimised.	• Risk Treatment Action plans • Records Disposal program • Records Management Training program • Disaster Preparedness and Business Continuity Plans include agency's records and recordkeeping systems
1.8	Records management staff MUST ensure that risks to the agency's records and recordkeeping systems, especially vital records, are addressed as part of the agency's Records Management Program.	• Vital Records Plan/Register
2.1	Agencies MUST align the functions of records management and risk management strategically and operationally.	• Records Management Policy refers to Risk Management Policy • Corporate Risk Analysis scales measure Information Risk
3.1	Agencies MUST review their Information Risk Register annually.	• Information Risk Register is up-to-date