TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 60 - Part Two: Applying Risk Management Processes

Introduction

In an electronic environment, where records do not exist in physical form, information risks are often mistakenly identified and treated as technology risks. Applying risk management processes can assist in identifying and effectively mitigating information risks.

The first section of this Advice (Part One - Introduction to Risk Management Processes) is designed for you to gain an understanding of your agency's existing Risk Management framework. This section describes the application of risk management processes to identify and manage information risks. Part Three contains risk analysis tools and templates.

This Advice adapts the Risk Management methodology from the Tasmanian Government Project Management Guidelines (V7.0). It is intended to provide additional supporting information to accompany Guideline 25 - Managing Information Risk and Guideline 1: Records Management Principles to assist agencies to implement recordkeeping requirements under the Archives Act 1983.

Risk management overview

The successful introduction of risk management processes will require sustained commitment and planning from your agency. Sufficient resources should be allocated, and responsibility for risk management processes should be appropriately assigned. The risk management process recommended in this advice follows the Australian Standard AS/NZS ISO 31000: 2009:

1. Design the framework

Create a framework for managing risk. Define the risk process and outcomes; clarify roles and responsibilities, objectives and scope. Analyse and understand the business environment and community expectations.

2. Risk Assessment

Step One: Identify and describe information risks.

Step Two: Make decisions about treatments by analysing risks and determining the risk level.

Step Three: This step prioritises information risks. Unacceptable risks can then be treated or included in risk mitigation plans. Completion of this step will shape the future direction of your Records Management Program and provide a picture of the health of current agency recordkeeping practices.

3. Create an Action Plan to treat risks

Match treatments to information risks. Create an Information Risk Register. Identify options for risk control, considering treatment effectiveness, cost and ease of implementation. Assign actions to ensure that the treatment is carried out.

4. Monitor and review

Review and monitor information risks to ensure that treatment is effective and appropriate.

Risk Management is not a project

Digital information is especially vulnerable at times of technical, organisational and business change. These risks can increase over time. To counteract this, integrate risk management processes into your Records Management Program, rather than conducting a one-off project. You may also choose to adopt a scaled approach, extending the steps for large, high risk initiatives and streamlining the process for low risk activities. For example, risk assessments should be more extensive for migration to a new business system than upgrading an existing system.

Diagram 1 - The risk management process

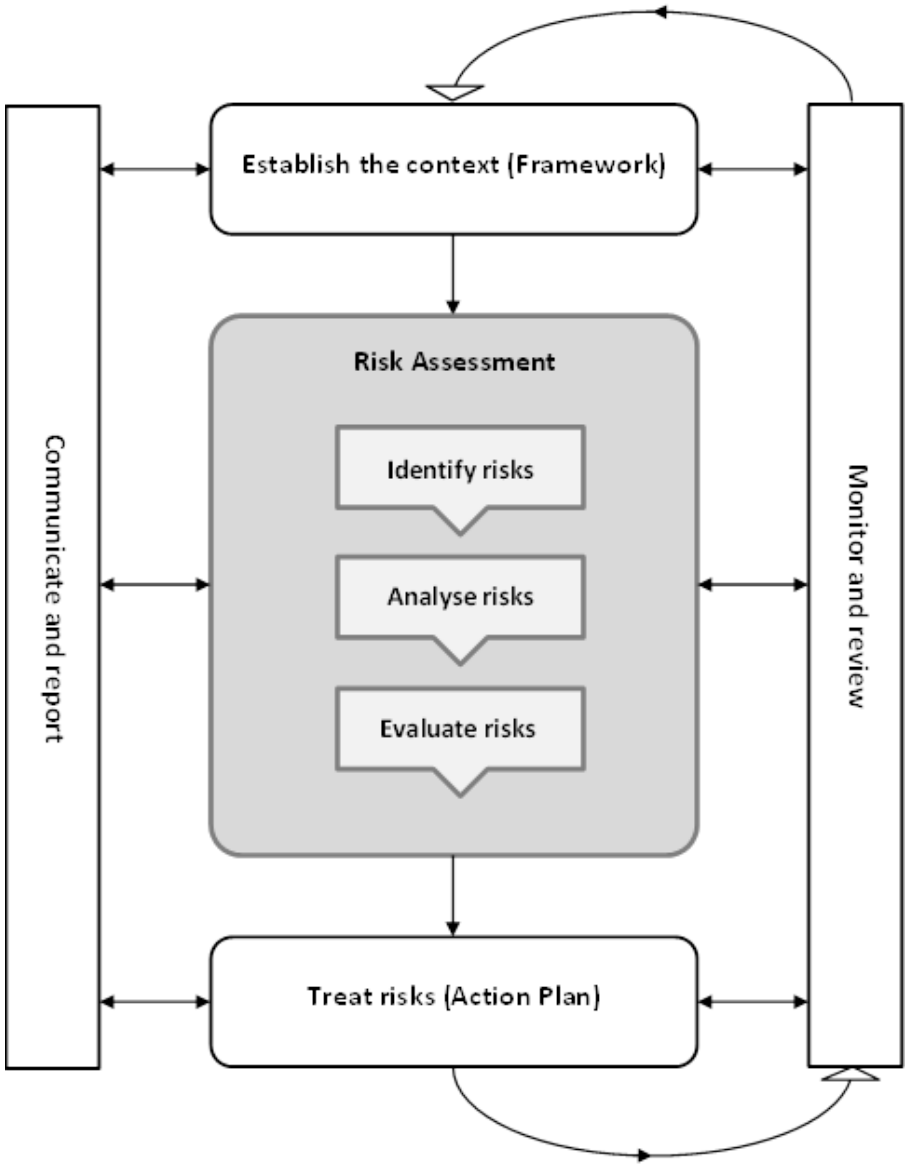

Diagram adapted from Tasmanian Government Project Management Guidelines V7.0

1. Establish the context

Start the process by developing your risk management framework and your communication and reporting strategy. If you are establishing a risk management framework because none already exists, you will first need to understand your agency's regulatory environment, business operations and community expectations. This will help you to identify your high priority information issues and risks.

Research the environment

You need to gain an understanding of your organisational environment in order to effectively undertake risk identification, analysis and treatment. This is the context in which business is conducted, and includes identifying any agency projects, business activities or work processes that have significant recordkeeping issues.

This contextual research will inform your risk assessments and help you effectively communicate to your agency how and why information risks occur. Document this research as part of your communication and reporting strategy.

Existing records management controls should also be considered as part of the operating environment, and by including them, you won't go over ground that has already been covered. (See Table 1 for some examples of records management controls).

Design the framework

The framework could be a single document or combine a number of elements which define the management of information risks in the agency. It is important that you utilise any existing risk management frameworks your agency has in place. Your agency's Risk Manager or Risk Management team will be able to assist you with this. The framework should align information risk management with existing risk management frameworks in the agency, such as the agency Corporate/Strategic Risk Strategy and any counter disaster and business continuity plans.

The framework should enable all parties to speak a common language and communicate the benefits and outcomes of managing risks to information assets. It should provide direction for all levels of management and be useful for regulators and auditors (such as TAHO) to evaluate the effectiveness of the agency's response. It should define the key elements necessary for managing information risks, and explain how these elements relate to agency-wide business activities. This includes identifying and documenting:

- Legislative and regulatory environment (Archives Act 1983, Right to Information Act 2009, any enabling legislation, etc. Advice 36: Legislative Mapping for Information Managers gives more information about this process)
- Business environment (e.g. joint ventures, partnerships, out-sourcing arrangements and contractual responsibilities)
- Organisational culture and capabilities (e.g. existing risk management frameworks, standards, policies, procedures, people, assets and systems)
- Community expectations (customer service charters, service provision, access to information, public accountability, etc.)
- Key stakeholders, both internal and external

The information risk management framework should also define:

- Resources, roles and responsibilities
- The scope of the process
- Implementation plans and key milestones
- The risk assessment methodology
- Tools (e.g. Information Risk Register)
- Relationship to other agency policies and procedures (e.g. Information Security, Information Privacy and IT procedures)
- Any existing controls, including records management controls

Identify existing controls

Any agency processes that have already been put in place to control information risks should be identified in this step. For example your agency may have contingency plans, such as business continuity and disaster preparedness plans, which have been put in place to reduce the level of risk in the event of disasters. There may also be records management controls in place which mitigate information risks.

Table 1 - Existing Records Management controls

Control	How it mitigates risk
Records Management Framework/Program	• A governance framework to ensure that information risks are identified and reported. • Provide a road map of future agency directions regarding record management so that all agency recordkeeping is planned and managed rather than being ad-hoc.
Records Management Policy and Procedures	• Outlines directives and responsibilities regarding recordkeeping so that agency personnel are aware of their responsibilities. • Issues directives regarding the use of USB, Bring Your Own Device (BYOD) and portable drives, social media, information privacy, security and confidentiality requirements, all of which lessens the risk of security breaches. • Procedures covering the entire process of records management ensure consistency, lessening risk of inappropriate and inadequate recordkeeping.
Recordkeeping Systems	• Systems such as Electronic Document and Records Management Systems (EDRMS) lessen the risk of digital records being lost, inaccessible or inappropriately disposed of.
Business Classification Scheme/File Plan	• Classification schemes provide consistency in naming records. This lessens risks around inappropriate filing and improves 'findability'.

Control	How it mitigates risk
Disaster Preparedness/Business Continuity	• Disaster preparedness and business continuity plans address operations during emergencies. This includes identifying areas of risk and developing contingency plans to preserve agency records.
Retention and Disposal Schedules	• A functional Retention and Disposal Schedule (R&DS) reduces risk because records are retained for the appropriate amount of time. • Reduces risk of non-compliance with legislation.
Information Asset Register	• Identifying information assets (content and systems) across the agency assists with information security classification. • Assists in identifying critical business systems for disaster recovery and business continuity plans.
Communication & training	• Communication and regular promotion of recordkeeping requirements lessens the risk of inappropriate or inadequate recordkeeping due to staff ignorance. • Training lessens the risks by allowing staff to gain practical experience of the impact of inadequate recordkeeping practices.
Assessments & audits	• Self-assessments and internal audits provide the means for assessing and benchmarking recordkeeping practice. Identifying problem areas and gaps allows for risk mitigation and treatment to be carried out. • External audits and compliance checks lessen the risks by identifying non-compliance areas, which can be acted upon for risk mitigation.

NOTE: Even with controls in place, there may still be threats or risks to information in your agency. Residual risks may still exist even after controls are developed or treatments are applied.

Communicate and report regularly

Successful implementation of Risk Management will be more likely if you take a consultative approach to framework development. In consultation with your agency's Risk Manager or Risk Management team, design a communication strategy for raising awareness of information risk. Frequent communication with key stakeholders will give everyone a shared vision of the proposed framework, the benefits and the outcomes.

Regular reports about information risks should be directed to the agency Risk Management Steering Committee, if there is one. Agencies who do not have an established risk management program should direct reports about information risks to their Manager of Corporate Services and/or the agency's Executive team.

2. Risk Assessment

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.

As we transition to digital recordkeeping, rapid technology changes bring new risks to information. Your agency may have started communicating with the community via websites, social media or mobile devices, or even exposing subsets of corporate information in databases to the public. Any improvements to information delivery can also expose threats to that information. For this reason, TAHO recommends that you conduct a risk assessment workshop every 3 years to identify any new information risks.

Step One - Identify information risks

This step establishes a process for identifying and describing information risks. It is the first part of the risk assessment process.

Risk identification tools

Begin identifying specific information risks by looking at the research you conducted in the first stage of the process (Establish the Context). You could also conduct a workshop, brainstorm disaster scenarios, take a walk around your worksite, read any previous audits, or consult staff that have operational knowledge of buildings and processes and talk to users of business systems.

Other methods to identify information risk include:

- Undertake PESTLE (Political, economic, social, technological, legal and environmental) and SWOT (Strengths, weaknesses, opportunities and threats) analysis to identify the landscape within which the agency operates and any internal strengths and weaknesses, as well as external opportunities and threats (See Appendix A for SWOT and PESTLE templates)
- Tailored questionnaires, such as records management self-assessments
- Audit reports conducted by internal or external auditors
- Interviews with agency personnel and external stakeholders about potential information risks (see Appendix B for a list of possible interviewees).

Information risks may have already been documented in the agency's Records Management Strategy and/or Policy or as part of any business process analysis that has been undertaken, so it may be worth looking at past risk management, information management or other agency governance documents (see Appendix C for examples). It may also be useful to conduct research into other jurisdictions or internationally for examples of information risks.

Don't overlook events that don't directly impact your agency. While your agency might not be directly affected by a natural disaster, effects on stakeholders, suppliers or clients may still have an impact on the agency. For specific guidance on how to prepare for, and recover from, natural and man-made disasters see Advice 26 - Disaster Preparedness and Recovery on our website.

Devising clear risk statements

It is important to devise clear risk statements before you undertake the risk assessment. Often risks are expressed as just a couple of words on risk registers. Risks like "System migration" or "Inadequate recordkeeping" or "Server crashes" don't provide enough information about the threat. Shorthand terminology or ambiguous language like this can make it difficult to rate the likelihood and consequences of the risk and to devise effective mitigation strategies.

Describing the risk involves consideration of:

- The Risk or Threat - an occurrence, trigger, event or a particular set of circumstances
- Cause - factors that increase the likelihood of the risk occurring
- Impact - the impact, outcome and consequence of the threat occurring

A better way to express "System migration" as a risk statement might be: "Important business records become inaccessible because the IT department doesn't identify recordkeeping metadata before performing system migration and decommissioning." Expressed this way, the likelihood and consequence can be more easily measured, and the risk can be easily assigned a priority rating for treatment.

Risk categories

To implement a consistent and repeatable risk management process for identifying information risks, it may be useful to establish a standard set of risk categories. This gives consistency when identifying risks by establishing a common language to describe them. Risks can be categorised by type (e.g. business risks, system risks or information risks) or by cause (financial, environmental, workplace, natural disasters, human-related) or by classifying internal and external threats to the agency's business operations.

Use the examples in the table below to begin thinking about the categories of information risks that could impact on your agency's business, and on the delivery of services. There will be other agency-specific areas of risk that are not listed here.

Table 2 - Information risks classified by type

There may be higher risks associated with particular record formats or record types, such as:

Permanent records - records that MUST be transferred to TAHO 25 years after the date of creation for retention as State archives.
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 - 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**

Completion of this step (Identify Information Risks) will provide you with a list of information risks, of standard information risk categories, and a systematic process for identifying information.

NOTE: Examples of information risks are described in this Advice at Appendix D. They are intended only as a starting point, because each agency will have risks which are specific to their business environment.

Step Two - Analyse information risks

Analyse each identified risk and use consequence and likelihood scales to measure and assign an initial risk rating. You will then review each risk, after considering any existing controls or other mitigation strategies, to understand the residual risk level to identify high priority risks for action or treatment.

The filtering process conducted in this step can help identify risks which:

- Are so low that mitigation strategies are not required
- Need monitoring, but no proactive mitigation strategies are immediately required
- Need to be escalated for the attention of agency senior management because of the risk to overall agency or whole-of-government business
- Need planned mitigation strategies and can be incorporated into the agency's Records Management Plan and/or agency procedures.

Risk Likelihood and Risk Consequence scales

For each information risk that you have identified, undertake a qualitative assessment. Through this step, information risks can be classified and ranked according to the likelihood that the event may occur and the level of seriousness/impact this will have if the event does occur.

Risk likelihood is a measure of probability. It is a statement that expresses a belief of how likely it is that a threat will emerge or risk event will occur. The example scale at Table 3 ranks risk likelihood from Almost Certain to Unlikely.

Table 3 - Risk likelihood

Likelihood	Description
Almost Certain	This event is expected to happen/ commonly repeating/ occurs weekly
Likely	This event is will probably occur/ occurs monthly
Possible	This event may happen at some time, say yearly/ has a one in twenty chance of occurring
Unlikely	There is little chance that this event could happen/ less than a 5% chance of occurring

Risk consequence is the outcome of an event or situation. It can be expressed qualitatively or quantitatively, and measured in terms of loss, injury, disadvantage or gain. Risk consequence is expressed in this Advice as a qualitative measure of negative impacts, such as loss or damage to information.

This scale is an example approach. It is important that any consequence scales you use are specifically designed to fit your agency. If not, then the level of risk won't be assessed properly.

Table 4 - Information Risk consequence scale

Minor	• Loss of information or records of short-term administrative value (e.g. routine advice) • Unauthorised access to PUBLIC and UNCLASSIFIED agency information.
Moderate	• Loss of information or damage to records of moderate value (e.g. minor contracts or project records, or required for audit purposes) • Unauthorised access to IN CONFIDENCE agency information.
Major	• Loss of information or damage to records of high value records that relate to long term or ongoing rights, obligations and entitlements (e.g. employee health monitoring and incident management records) • Unauthorised access to PROTECTED agency information.
Catastrophic	• Loss or irreparable damage to vital records essential for the ongoing business of an agency, and without which the agency could not operate effectively. • Loss of information or irreparable damage to records recognised by a broader audience than the original creating agency to be of enduring value, including future generations (e.g. PERMANENT records) • Unauthorised access to HIGHLY PROTECTED agency information.

Table 4 describes levels of consequence to information using a scale of Catastrophic to Minor. This scale has been expanded to include a Catastrophic grading, which is automatically assigned to any risks which, if realised, will cause a project to fail or result in a major adverse impact on business operations. Other consequences of catastrophic risks might be: serious political consequences, major financial losses, disaster event or life is threatened. These types or risk consequences are included in the Consequence scale in Part Three of this Advice.

This approach is a **suggested** starting point. Your agency will have already developed scales that reflect agency-specific functions and requirements. The main point is that you must assign likelihood ratings and consequence ratings to each identified risk **before** progressing to the next step.

The results of this exercise should be documented. A summary of all the risks you identify can then be recorded in an Information Risk Register. The Information Risk Register should be regularly reviewed to help shape the direction of your agency's Records Management Plan, and will form part of any evidential documentation required for TAHO audits.

Step Three - Evaluate information risks

This step evaluates the results of the analysis conducted in the previous step. This enables agencies to prioritise each risk and include unacceptable risks in treatment and risk mitigation plans. Completion of this step will shape the future direction of records management as well as give a picture of the health of current agency recordkeeping practices.

Your risk evaluation should consider:

- The importance of the activity (or the records)
- If the risk is related to the agency's core business
- Any current controls you have over the risk
- Any potential losses (e.g. financial)
- Any benefits or opportunities presented by the risk.

Table 5 - Risk impact matrix or heat map

This step begins by using a risk impact matrix to grade each risk, from low likelihood/low consequence, to certain likelihood/extreme consequence. The risk matrix shown here is an example which could be used to rate and prioritise risks so a decision regarding treatment can be made.

		Consequence			
		Minor	**Moderate**	**Major**	**Catastrophic**
Likelihood	**Almost Certain**	**High**	**High**	**High**	**Extreme**
	Likely	**Medium**	**Medium**	**High**	**Extreme**
	Possible	**Low**	**Medium**	**Medium**	**Extreme**
	Unlikely	**Low**	**Low**	**Medium**	**High**

Example 1: Heavy rainfall causes flooding, and client files stored in off-site storage are damaged and cannot be salvaged. Because the storage area was originally built on flood prone land, this risk scores a Likelihood of Almost Certain, and a Consequence rating of Major, because the records are of high value. In this case, the risk would achieve a rating of **High**.

Example 2: Social media pages maintained by agency staff are used as public consultation forums. The provider goes out of business and suddenly closes the site, resulting in public submissions and feedback being lost. However, because the agency captures a daily snapshot of the site in their recordkeeping system, this risk is rated as Unlikely. So even though the Consequence is considered Moderate, this risk would be rated at **Low**.

Using a risk heat map such as the one in Table 5 enables the level of risk to be determined. Agencies may already have a risk matrix to plot information risks. The point of this exercise is to enable the high risk areas to be clearly identified so that they can be treated as a priority.

Prioritising risks

On completion of the initial risk grading, if risks are mostly in the middle range, think carefully about the impact on the agency's business. Sometimes the effects of an information risk can be difficult to predict or evaluate, so it is worthwhile documenting all possible impacts. This helps to clarify risk priorities.

When prioritising risks, it is important to recognise that the occurrence of a single risk may have a compounding effect. We have measured risks against the consequence and impact of loss of information in our consequence scale in this Advice. However, you should use a risk impact scale that best fits your agency's business operations. Your agency risk scales may use financial cost, time and resources or quality impacts.

NOTE: Advice 60: Part Three - Risk Assessment tools and templates includes a Consequence scale with Information impacts as well as Financial, Insurance, Personnel, OHS, Service Delivery, Operations, Compliance, Reputation, Political and Environment factors.

3. Plan to treat information risks

In this step, appropriate treatments, risk mitigation strategies and action plans are put into practice. This step brings together all of the previous steps (context, risk categories, risk likelihood and consequence levels and priorities) to match treatment options to each risk.

Mitigation and treatment strategies can be developed once your risk priorities are agreed upon. This may include the development of new procedures and tools, strategic alignment of key agency policies, or it may be the adjustment of current records management operations. Implementing treatment plans relies upon all risks having been evaluated and prioritised as either acceptable or unacceptable risks.

Acceptable risks may be:

- Risks where the risk level is low and treatment would require too many resources
- Risks for which a treatment is not yet available
- The cost of the treatment outweighs the benefits of the treatment
- The risk is positive, and actually provides an opportunity for the agency

There may be a range of risk mitigation strategies that you identify to treat each risk, but you must assess each of them for likely effectiveness, taking into account likely costs and ease of implementation. Sometimes a combination of actions should be applied. It is important that you set a measurable outcome for each risk treatment action that can be monitored for effectiveness over time.

It is also important in this step to assign business owners to manage the risks, and include associated tasks in work plans. Assigning ownership of risks and responsibility for treatment will ensure that action is taken.

Assign responsibility

In order to ensure risks are appropriately monitored, managed and treated, ownership must be allocated appropriately. For lower level information risks, responsibility is usually allocated to the Records Manager and/or Records Team.

However, it may be appropriate to escalate responsibility for mitigating high-level information risks to particular members of the Risk Steering Committee or Business Owners (depending on their operational role and influence within the agency), or to the Manager of Corporate Services and/or the agency's Executive team. These are likely to be risks that:

- Receive a high level of public and media scrutiny
- Instigate or are subject to litigation or formal investigation
- 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
- Relate to employment conditions of staff
- Involve organisational change management and/or transitioning to new systems

Treatment options based on risk levels

As part of the risk management process it is also necessary to identify what options will be used to treat, control or mitigate risks.

Treatment options must be scaled to the level of risk posed. For example:

- High risk must be managed by specific monitoring or response procedures using a detailed plan overseen by senior management.
- Medium risk must be managed by specific monitoring or response procedures
- Low risk should be managed by routine records management procedures.

Table 6 discusses the different types of treatment options and divides them into pre-emptive actions (which can be taken immediately and lower the risk likelihood) and contingencies (which lower the risk consequence after the risk has occurred).

Table 6 - Treatment options

Treatment option	How it mitigates risk
Avoidance (Pre-emptive)	This could be changing the scope, timeframe or any other actions which may alter the risk consequence.
Transfer (Pre-emptive)	Transferring the risk to a third party more capable of dealing with the problem or opportunity. This does not eliminate the potential risk, but transfers the treatment actions as a risk mitigation strategy. Responsibility for the risk remains with the agency.
Acceptance (Pre-emptive)	Accepting the risk without planning any response to counter it.
Preventative (Pre-emptive)	Actions that reduce the possibility that the risk will occur such as acquiring technical expertise or implementing new procedures or conducting a training program. An example may be implementing an annual pest inspection, which helps keep records storage areas rodent-free.
Mitigation (Pre-emptive)	Actions that reduce the possibility that the risk will occur such as acquiring technical expertise or implementing new procedures or conducting a training program. An example may be implementing an annual pest inspection, which helps keep records storage areas rodent free.
Contingency Actions	Planned actions that can reduce the consequences after it has occurred. An example of contingency action after loss of information held in electronic storage may be to conduct recovery operations from previous backups.

Table adapted from Tasmanian Government Project Management Guidelines V7.0

Control measures

Control measures (e.g. policies and procedures) may be behavioural, technical and/or operational. Controls are the result of treatment options and will lower the likelihood of the risk occurring or the seriousness of the consequences, and are generally actions that can be applied immediately.

Before implementation, controls should also be evaluated for effectiveness and cost-efficiency. Treatment options or control measures which are pre-emptive (preventative actions) are often far more cost-effective than contingencies (disaster mitigation and recovery).

NOTE: If the Records Management controls listed in Table 7 are not already in place, the agency should develop them as part of the Risk Treatment Action Plans, or include in Records Management work planning.

Table 7 - For more information on Controls

Control	More information
Records Management Policy and Procedures	Advice 50: Developing an Information Management Policy and Sample policy to accompany Advice 50
Recordkeeping Systems	See Advice 19: EDRMS implementation; some tips. Recordkeeping metadata standard (2011: Advice 14) specifies metadata requirements for recordkeeping systems. Advice 17: Implementing better records and information management includes a section on systems.
Business Classification Scheme/File Plan	See Advice 19: EDRMS implementation; some tips for developing a Business Classification Scheme and Advice 17: Implementing better records and information management for additional information about conducting business analysis.
Disaster Preparedness/Business Continuity	For advice on identifying vital records see Advice 52: Identifying and Managing Vital Records. See Advice 26: Disaster Preparedness and Recovery to prepare for and recover from disasters.
Retention and Disposal Schedules	Advice 28: Getting Started on the Development of an Agency Functional Disposal Schedule describes this process. Also see Writing disposal classes (Advice 13).
Information Asset Register	See Advice 39: Developing an Information Asset Register for more on Information Asset Registers.
Communication & training	Advice 1 - Government employees responsibilities in relation to State records gives guidance on the recordkeeping responsibilities of all agency staff, contractors and volunteers. Change Management - Preparing for Change (2014: Advice 55) gives advice about communication strategies. TAHO also conducts regular training programs on Records Management issues.
Assessments & audits	Guidelines issued by TAHO usually contain compliance checklists. These can be used for developing internal audits. For more information and examples consult the Guidelines on our website.

Risk Treatment Action Plans

Treatment plans document the risk, the identified control or treatment option and any actions taken for risk mitigation. If treatment options include developing and implementing new processes or services, the treatment plan should be incorporated in the agency's Records Management program. The plan should include the following elements:

- The process for identifying, analysing, evaluating and treating risks (i.e. the risk management framework) and who is responsible;

- The process for transferring risk mitigation activities into the Records Management work plan;
- How often the Information Risk Register will be reviewed, the process for review and who will be involved;
- How risk status and treatment actions will be reported and to whom;
- A snapshot of the high-level risks, risk ratings, planned mitigation strategies, costs and who will be responsible for implementation (i.e. a snapshot of the Information Risk Register);
- How any recovery actions will be managed if a threat or risk event occurs.

4. Monitor and review information risks

Review and monitor information risks to ensure that the treatment actions have been completed, to evaluate the effectiveness of treatments, to manage any residual risks and to identify any additional treatment actions. Treatment actions can also bring with them a new set of risks, and these will need to be evaluated as part of the monitoring and review process.

Monitoring information risks is not a one-off activity. Regular reviews should be built into the Records Management program. Methods and tools agencies can develop to monitor and review risks include:

- Internal audits using the Information Risk Register as a checklist (see the Generic Information Risk Register template in Part Three of this Advice)
- Recordkeeping self-assessments (or health checks) which measure agency recordkeeping practices
- Regular formal reporting to management on risk status
- Implement an internal process for risk notification and review
- The checklist provided as part of Guideline 1: Records Management Principles - Overview
- External audits, including any TAHO audits

Agencies should also include (or reference) the high-level information risks and associated management strategies from the Information Risk Register in their Information Management and/or Information Security policy, and in any agency counter disaster and business continuity plans.

Further information

- Tasmanian Government Project Management Guidelines (V7.0), and associated Toolkit
- AS/NZ ISO 31000:2009 Risk Management - Principles and Guidelines and associated SA/SNZ HB 436:2013 - Risk Management Guidelines
- ISO/TR 18128:2014 Information and documentation - Risk assessment for records processes and systems
- Disaster Preparedness and Recovery (2012: TAHO Advice 26)
- Identifying and Managing Vital Records (2014: TAHO Advice 52)

Further guidance on mitigating specific information risks is available in the Guidelines and Advice on TAHO's website under Government Recordkeeping.

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

- Department of Premier and Cabinet Tasmanian Government, Project Management Guidelines V7.0 (pp. 90-106)
- Public Records Office of Victoria (PROV), PROS 10/10 Guideline 6: Records and Risk Management (2010).
- State Records NSW, Guideline 5: Counter disaster strategies for records and recordkeeping systems (2002)
- National Archives Australia (NAA), Advice on Managing Recordkeeping Risks
- JISC infoNet, Northumbria University, PESTLE and SWOT analyses (2014)
- The National Archives UK, Risk Assessment Handbook Version: 1.2 (2011)

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
1.0	03-09-2014	Samara McIlroy	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: 2014

Ross Latham
State Archivist

Appendix A - Conducting analysis

PESTLE analysis

Use PESTLE analysis to provide a context for the agency's current business activities and recordkeeping practices in relation to the external environment. The analysis covers Political, Economic, Social, Technological, Legal and Environmental (PESTLE) factors or areas of uncertainty.

Don't worry if you find that factors fit under several categories, this exercise is simply about identifying them. Some examples have been included here.

Category	Factors
POLITICAL ***What are the key political drivers of relevance?*** e.g. international, Federal and State government directives, Agency policy, topical, new industries	• Government administrative changes causing records transfers and changes to records custody arrangements • Change to government policy affecting records (e.g. Tasmanian Government Information Security Policy) • Government open data initiatives
ECONOMIC ***What are the important economic factors?*** e.g. funding mechanisms and streams, business and enterprise directives, internal funding models, budgetary restrictions, income generation targets	• Budgetary restrictions cause changes to management priorities around agency resourcing of records systems • Increased costs of travel mean that record staff are unable to support dispersed worksites • Perceived savings of moving records to the cloud
SOCIAL ***What are the main societal and cultural aspects?*** societal attitudes, lifestyle changes, changes in populations, distributions and demographics and the impact of different mixes of cultures	• Tech-savvy public demands instant response from agency staff and 24 hour on-line access • Aging workforce not comfortable with technological change
TECHNOLOGICAL ***What are current scientific and technology imperatives, changes and innovations?*** new and emerging technologies, scientific research and discoveries	• Frequent system upgrades causing interoperability problems with EDRMS (e.g. Microsoft Office 365 upgrade) • The average business system lifecycle is 7-10 years but the records stored in the system have a retention of 75 years • Increased use of personal electronic devices by agency staff for work purposes
LEGAL ***What legal and regulatory requirements affect the agency?*** e.g. Privacy laws, Archives Act, Right to Information, enabling legislation	• Increase in public enquiries and applications under RTI Act • Agency required by Archives Act 1983 to transfer all permanent records to TAHO 25 years after creation (unless exemption granted) • Guidelines and Advice released by TAHO to assist agencies (e.g. cloud computing, information security) • Increased awareness of information and records management issues due to e-discovery
ENVIRONMENTAL ***What are the environmental considerations, locally and further afield?*** e.g. energy and resource consumption, sustainability, waste	• Potential for acts of terrorism to cause damage to premises and disruption of services • Local events such as flooding cause damage to records in storage • Disruption to power service disruptions

SWOT Analysis

Once you have established the agency's PESTLE context, you can use this output to map out a SWOT analysis. SWOT stands for:

- Strengths
- Weaknesses
- Opportunities
- Threats

To conduct the SWOT analysis, take the factors from PESTLE and separate them into Strengths and Weaknesses, and add any more you identify. Use Opportunities and Threats to analyse the internal factors that will act against the agency. Examples have been included here to provide a starting point.

	Positive Factors	**Negative Factors**
External Factors (Future)	**OPPORTUNITIES** External trends or conditions that the agency can capitalize on or use to its advantage. • Guidelines and Advice released by TAHO to assist agencies (e.g. cloud computing, information security) • Increased awareness of information and records management issues due to e-discovery	**THREATS** External factors or conditions that may negatively impact on the agency. • The average business system lifecycle is 7-10 years but the records stored in the system need to be retained for 75 years • Perceived savings of moving records to the cloud
Internal Factors (Present)	**STRENGTHS** Internal capabilities and resources that could support a successful outcome, maximise an opportunity and minimise a threat. • Government open data initiatives • Senior Manager is a champion for best-practice recordkeeping • Information Security Policy and information security procedures have recently been implemented across agency. • Agency-specific Retention and Disposal Schedule (R&DS) has just been approved by TAHO	**WEAKNESSES** Internal attributes and resources (or lack of) that work against a successful outcome, and increase the likelihood or consequence of a threat. • Frequent system upgrades affect interoperability between business systems and EDMRS • Aging workforce is not comfortable with technological change • Agency systems (particularly legacy systems) and business processes are poorly documented

- The **Factors**, **Opportunities** and **Threats** you identified in your PESTLE and SWOT analysis could form the basis of your Risk Register, if you don't already have one.
- The **Strengths** you have identified may also be **controls** which minimise threats, and this could be recorded in your Risk Register (e.g. Information Security Policy and Procedures).
- While **Weaknesses** are not strictly risks (risks are about the potential for something to happen), **treatment actions** that would address **Weaknesses** could go in the Risk Register because they would decrease the likelihood or impacts of **Threats**.

Information Security Risk Assessment

Risk analysis is also performed as part of Information Security Policy implementations, including the identification and assessment of risks to agency Information Assets. Information Security Risk processes consider key threats and vulnerabilities to the information asset together with any business initiatives potentially impacting the security of the information asset in relation to three security objectives (confidentiality, integrity and availability). The Information Asset Owner is responsible for ensuring that risk identification is undertaken and that appropriate input is obtained from information custodians and information users.

Risk identification for information security considers each of the three security objectives (confidentiality, integrity and availability) and the key risks to achieving the required level of security for the information asset. Risk assessments support decisions about security classification requirements for each information asset.

Risk assessments should consider the following:

- Physical location and environment;
- Extent of use and transmission;
- Attractiveness to theft or change (potential value to employees or third parties);
- Potential for error;
- Nature of computer operations tasks;
- Network environment and structure;
- Transactional integrity requirements (including evidentiary weight);
- Known or previous incidents;
- Extent and nature of system or application changes;
- Source of data and nature of data entry;
- Nature of access and use of information, including the identity of those who access and use the information.

An assessment of risk for each information asset should be performed giving consideration to:

- The business impact likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information asset, and;
- The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The Asset Owner should have reviewed the security risk rating and if necessary, identified further actions necessary to control, manage, transfer or monitor the security risk.

Any risk assessments that have been undertaken will have been documented and included in a summary form in the Information Asset Register. Each Information Asset will have an assigned Asset Owner who is responsible for monitoring and reviewing risks. Information Asset Owners may be a useful source when identifying information risks, especially risks to information in agency computer systems.

Adapted from: Government of South Australia, Information Security Management Framework, version 3.2.0, Sept. 2014

Appendix B - Suggested staff interviews

Staff in the following roles may be able to contribute to your comprehensive assessment of risks to agency information and records.

Please note many of these titles are specific to government, and sometimes one person may occupy multiple roles in a smaller agency, organisation, business enterprise or council:

- Head of Legal Services or Legal Officer
- Chief Information Officer (CIO) – this could be the IT Manager
- Risk Manager
- Audit & Compliance Manager
- Safety Manager
- Information Manager or Records Manager
- Departmental Records Officer
- Information Architect
- Right to Information / Compliance Advisor
- Head of IT/IT Manager
- IT Service / Solutions Manager
- IT Business Support Analyst
- IT Procurement Manager
- Database Analyst
- Enterprise Architect
- Business Analyst

Adapted from National Archives UK, Risk Assessment Handbook (V1.2), 2011

Appendix C - Documentation checklist

Review key documentation to obtain an understanding of agency governance structure, policies and objectives and also agency information assets. This enables you to define, ahead of consultations and interview sessions, potential lines of questioning. The documents included below are intended as a guide only.

File Ref	Document Title	Available (yes/no)	Notes
Whole of agency strategy and policy			
	Corporate/Strategic Risk Register		
	Organisation chart		
	High-level business objectives (Agency Strategic Plan or Annual Reports)		
Information Security Management			
	Information security management policy		
	Information security roles and responsibilities		
	Information Asset Register		
Information Management Environment			
	Information architecture, metadata mapping		
	Information Management and/or Records Management policy		
	Business classification scheme and associated retention and disposal schedules		
	Information re-use policy and supporting guidance		
Information Technology Environment			
	ICT strategy		
	Network diagrams and/ or mapping of IT systems		

Adapted from National Archives UK, Risk Assessment Handbook (V1.2), 2011

Appendix D - Example of risks classified by Risk Category

Risk Category	Risk	Cause	Impact	Treatment Actions & Controls
Permanent records	Insufficient pest and environmental monitoring controls	The agency stores records in a shipping container. The site is un-monitored. Rodent infestation occurs and some permanent records are destroyed.	• Agency unable to meet compliance requirements under the Archives Act. • Potential embarrassment and damage to agency's reputation.	The agency routinely monitors all records storage areas and stores in accordance with Guideline 11- Physical storage of State records, including establishing a pest control program.
Vital records	Vital Records Plan is out-of-date	Responsible staff member left agency and was not replaced.	• Records crucial to restoring business operations and systems after a disaster are not identified or protected and cannot be retrieved.	Responsibility for management and review of Vital Records Plan are assigned to a Senior Manager and included in Records Management Program work plan.
Unscheduled records - not covered by an approved Retention and Disposal Schedule (R&DS).	Records created by staff undertaking some specific functions for the agency are kept forever.	Agency does not have an approved functional R&DS which covers these record types.	• Increasing costs of storage as the volume of records increases. • Increased litigation risks.	Agency commences project to develop functional R&DS.

Risk Category	Risk	Cause	Impact	Treatment Actions & Controls
Unstructured digital records (e.g. network drives and email)	Unauthorised destruction of State records held in emails and on network drives	Business owners and records creators of important business documents and emails have left before saving in agency recordkeeping system.	• Vital information about business decisions is lost • Staff unable to find or re-use information. • Additional costs to keeps large amounts of digital records, and offline repositories for legacy records. • Agency loses a legal dispute because it is not able to provide key email messages as evidence.	• A policy is introduced requiring all employees to undergo training in digital records classification and filing procedures so that they are aware of where to file business information. All employees are made responsible for filing their email records in the EDRMS daily. • IT staff required to liaise with Records staff before deleting email inboxes. • Exit checklist is implemented which includes saving records into EDRMS.
Digitised records - (e.g. paper records which have been scanned)	Large volume of temporary and permanent retention paper records scanned as single .pdfs	Agency did not research recordkeeping requirements or consult TAHO Guidelines and Advice before commencing major digitisation project of legacy records to save on storage costs.	• Required to retain paper originals as agency cannot guarantee that the digital copies of permanent records are of sufficient quality with enough accompanying metadata for transfer to TAHO. • Additional post-processing costs to separate permanent and temporary records into separate .pdfs • No storage savings achieved as originals need to be retained.	• Agency refers to TAHO Guideline 8 and Advice 30 before commencing digitisation project and seeks additional advice from TAHO staff. • Agency researches industry best-practice technical and metadata requirements before commencing scanning. Temporary and permanent records are scanned as separate .pdfs. • Tests are conducted and quality checks carried out on digital files.

Risk Category	Risk	Cause	Impact	Treatment Actions & Controls
Records in **business systems** that have a retention period of over five years	Critical business records not identified before system decommissioning	IT Staff not identifying records in business systems which need to be retained to support high risk business processes or that are Permanent records.	• Agency incurs additional costs to keep legacy systems operational. • Critical business records kept in short-term data backup systems. • Records of enduring value to government and to the community of Tasmania are not transferred to TAHO	• Agency implements regular audits of business systems, carried out by IT and Records staff. This identifies what records need to be retained. • Agency consults TAHO Guidelines and Advice about managing digital records before acquiring, designing, migrating between or decommissioning databases.
Records in **business systems** that are about to undergo migration	Minimum recordkeeping metadata not captured	The IT department carried out the migration without identifying what records needed to be carried forward out of the system, and what their metadata dependencies are.	• Metadata about record creators and action officers was not carried over. As a consequence, reporting and accountability needs could not be met.	• Agency uses minimum recordkeeping metadata requirements specified by TAHO in Advice 18 - Managing records in business systems, in specifications when purchasing new business systems.
Records stored in **cloud-computing systems** and **applications**	Project records stored in cloud-based commercial applications are more likely to be subject to cyber-attack.	Agency has no control over other users or the types of information stored in the application.	• Application's developers accept no liability or responsibility for deleted, lost or corrupted data. • Sensitive agency information may be made public	• Senior staff ordered to remove all business records from the application. • IT staff regularly monitor use of the application and enforce this policy.

Risk Category	Risk	Cause	Impact	Treatment Actions & Controls
Sensitive and security classified information	Information security models not applied to emails.	Staff not trained to use information security classification scheme	• Sensitive information is leaked to the media, causing embarrassment and damage to agency's reputation	• An information security classification system is rolled out across the agency. • Induction includes awareness of information security and employee responsibilities regarding classification of information.
Hybrid environments with content created in both paper and digital formats	Recordkeeping practices do not meet regulatory requirements	Agency must produce records for reporting and audit purposes. The agency has numerous business systems, but key records are still kept in paper format.	• The process of tracking down a document through various systems is time consuming and it is difficult to determine which record presents the best evidence.	• The agency implements an EDRMS and back-scanning project for key records in paper format. • The project includes quality controls and complies with TAHO Guidelines
Records of decision-making or advice delivered via **telephone**	Records not captured in agency recordkeeping systems	New staff not trained to create and capture records of advice given over the telephone.	• Investigation by Ombudsman regarding accusations of misleading advice given by the agency to the public.	• Policy of making 'Note to file' immediately after telephone call is introduced. • Regular training program for staff on recordkeeping requirements. • Posters about 'making a record' placed in offices.
Records of decision-making or advice delivered using **websites, social media or Web 2.0 technology**	Important public announcements made on social media and websites not captured in agency recordkeeping systems	Proprietary social media applications are used as consultation forums by agency staff, and not duplicated or recorded in EDRMS. The provider goes out of business and suddenly closes the site.	• Public submissions and feedback are lost. • The agency is forced to publicly apologise and repeat the consultation process causing loss of staff time and embarrassment.	• Implement a process to capture the submission process as a daily snapshot which will be saved in the agency's EDRMS.

Risk Category	Risk	Cause	Impact	Treatment Actions & Controls
Records stored or transmitted via **mobile devices**	Senior management decisions not captured in agency recordkeeping systems	New policy allows senior agency staff to use their own mobile phones as it requires less initial ICT establishment costs and maintenance.	• Important business decisions made via personal email or text message not captured in the EDRMS. • Unable to locate important records. • Possible compliance breaches.	• Policy amended to include warnings about the risks. • Process implemented to download SMS from phones into EDRMS. • Employment contracts are amended with a clause about possible termination if the policy is breached.

Appendix E - More guidance on information risks

Permanent records - records that must be transferred to TAHO 25 years after the date of creation for retention as State archives.	• Retention and disposal of State records (2005: Guideline 2) • Preparing hard copy records for transfer to the Tasmanian Archive & Heritage Office(2013: Advice 12)
Vital records - records essential for the ongoing business of an agency, and without which the agency could not operate effectively.	• Identifying and Managing Vital Records (2014: Advice 52) • Disaster Preparedness and Recovery (2012: Advice 26).
Unscheduled records - not covered by an approved Retention and Disposal Schedule (R&DS).	• Retention and disposal of State records (2005: Guideline 2) • Disposal of un-scheduled records (2012: Advice 10) Checklist to accompany Advice 10 (word version) • Developing a functional records disposal schedule (2005: Guideline 6) • Getting Started on the Development of an Agency Functional Disposal Schedule (2012:Advice 28)
Digital records - structured and unstructured (including network drives and email)	• Keeping Digital Records Accessible (2013: Advice37) • Information Custodians and Digital Continuity (2013: Advice 38) and associated Checklist • Digital preservation formats (2012: Guideline 19) • Managing records on shared network drives (2013: Advice 41) and Sample procedures for staff • Managing electronic communications as records (2009: Guideline 7) • Managing email (2012: Advice 27) • Keeping Digital Records Accessible (2013: Advice37)
Digitised records - (e.g. paper records which have been scanned)	• Management of source records that have been copied, converted or migrated (2013: Guideline 8) • Digitisation of records (2011: Advice 21) • Digitisation dilemmas (2013: Advice 30)

Records in **business systems**	• Managing records in business systems - Overview and Part 1 to 5 (2014: Advice 18)
Records stored in **cloud-computing systems** and **applications**	• Managing the recordkeeping risks associated with cloud computing (2010: Guideline 17)
Records that contain **sensitive and security classified information**	• For Implementing Information Security (Advice 33 - 35) see Government Recordkeeping website
Records in **hybrid environments** with content created in both paper and digital formats	• Advice for Agencies on Managing Legacy Records (2012: Advice 29) • Management of Digital Records on a Shoestring (2014: Advice 56)
Records of decision-making or advice delivered via **telephone**	• Government employees responsibilities in relation to State records (2005: Advice 1)
Records of decision-making or advice delivered using **social media or Web 2.0 technology**	• Recordkeeping strategies for websites and web pages (2005: Guideline 15) • Managing Web 2.0 records / Social Media (2012: Guideline 18)
Records stored or transmitted via **mobile devices**	• Managing electronic communications as records (2009: Guideline 7) • Managing electronic communications as records (2009: Advice 4)