Public Record Office Victoria

PROS 10/10

Strategic Management

Guideline 6

Records & Risk Management

Version Number: 1.0

Issue Date: 19/07/2010

Expiry Date: 19/07/2015

Table of Contents

Copyright Statement

Disclaimer

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Guideline. This Guideline does not constitute, and should not be read as, a competent legal opinion. Agencies are advised to seek independent legal advice if appropriate.

Acknowledgements

The Public Record Office Victoria would like to acknowledge the valuable contribution of members of the *Strategic Management Advisory Group* during the development of this Guideline.

The Public Record Office Victoria would also like to acknowledge the work done by the Victorian Managed Insurance Authority, National Archives Australia, Territory Records Office of the Australian Capital Territory, State Records Authority New South Wales, and Department of Premier and Cabinet on risk and records management. PROV referred to their expertise in drafting this Guideline.

1. Introduction

1.1. Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973*, the Keeper of Public Records ('the Keeper') is responsible for the establishment of Standards for the efficient management of public records and for assisting Victorian government agencies to apply those Standards to records under their control.

Recordkeeping Standards issued by PROV reflect best practice methodology. This includes international Standards issued by the International Organisation for Standardisation (ISO) and Australian Standards (AS) issued by Standards Australia in addition to PROV research into current and future trends.

Heads of government agencies are responsible under section 13b of the *Public Records Act 1973* for carrying out, with the advice and assistance of the Keeper, a programme of efficient management of public records that is in accordance with all Standards issued by the Keeper.

In Victoria, a programme of records management is identified as consisting of the following components:

- A Recordkeeping Framework;
- Recordkeeping Procedures, Processes and Practices;
- Records Management Systems and Structures;
- Personnel and Organisational Structure; and
- Resources, including sufficient budget and facilities.

A programme of records management will cover all an agency's records in all formats, media and systems, including business systems.

1.2. Purpose

The purpose of this Guideline is to facilitate the implementation of the following requirements from *the Strategic Management Specification*:

- Requirement 2: The records management function is strategically linked to the risk management function.
- Requirement 9: The records management strategy identifies the agency's records management environment and assesses its exposure to risk.
- Requirement 13: The risk management strategy includes records management requirements.
- Requirement 17: Assessment of individual business areas records management practice includes the reporting of high level risks identified to the executive.
- Requirement 18: Reporting mechanisms in place include the reporting of recordkeeping risks in the agency's risk register.
- Requirement 20: The records management policy is aligned with the risk management policy.

This Guideline describes a methodology for the assessment and management of risk related to recordkeeping in accordance with the six-step approach of the Australian/New Zealand Standard on risk management. It aims to help Victorian government agencies to include recordkeeping and records management into their risk management framework.

1.3. Scope

This Guideline applies to agencies that are strategically linking their records management and risk management functions. Agencies may be integrating records management in their existing risk management programme, or developing records management or risk management programmes.

The Guideline follows the steps and principles established by the Australian Standard AS/NZS ISO 31000 2009, *Risk Management—Principles and guidelines*. This Guideline is not intended as an exclusive approach to risk management and the development and implementation of a risk management strategy.

1.4. Related Documents

This Guideline supports the *Strategic Management Standard* and Specification which are supported by a number of other Guidelines and Fact Sheets as shown in the following relationship diagram:

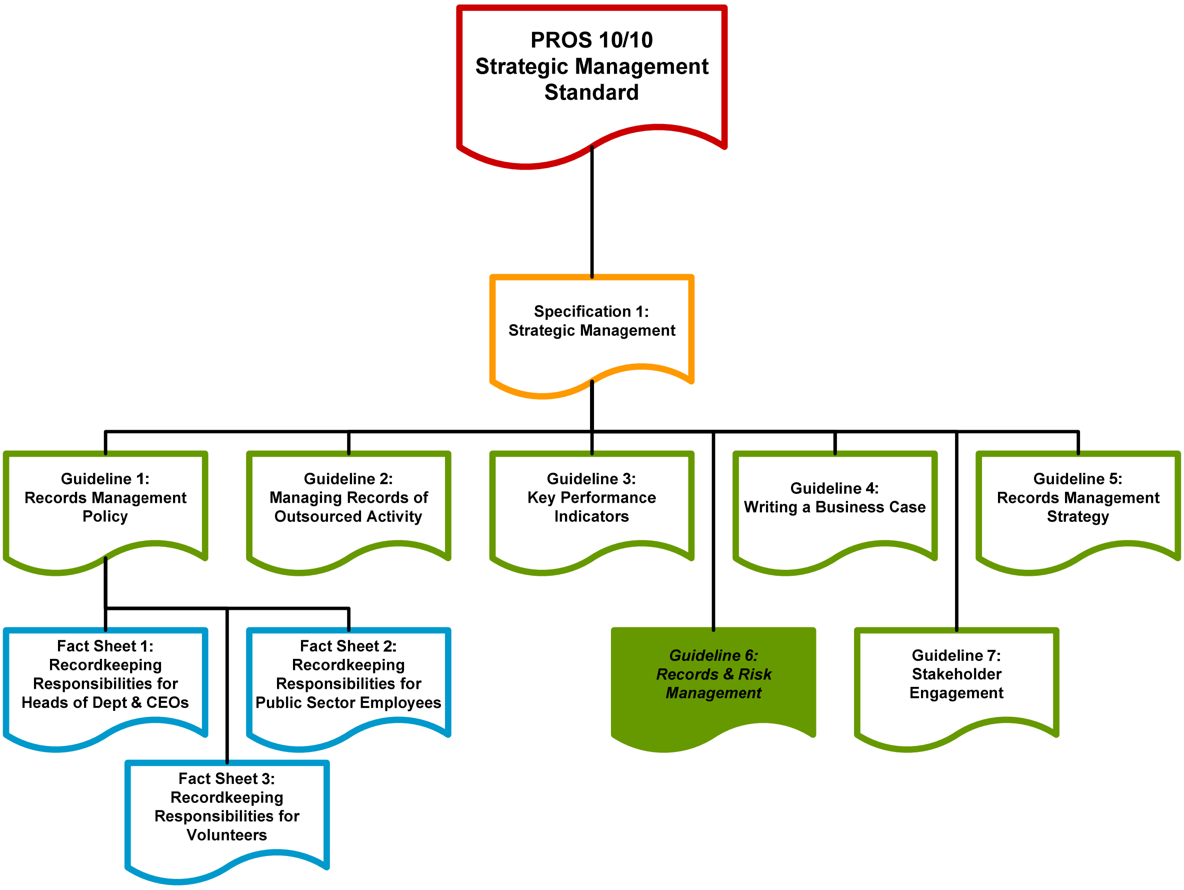


Figure 1: Relationship Diagram

2. Risk Management: An Overview

2.1. Definitions of Risk & Risk Management

A risk is defined as being the ‘effect of uncertainty on objectives’.[1] It may be a positive or a negative effect.

Risk management is defined as being the ‘coordinated activities to direct and control an organisation with regard to risk’.[2] The objective is to maximise the positive effects of risk and to minimise or negate the negative effects of risk.

2.1.1. Where does records management fit in?

Records management deals with two main areas of risk – records related risks and business related risks.[3]

Records related risks occur as a direct result of records management activities. That is, they occur as a result of activities related to capture, control, access, storage, or disposal of records, or to the general management of records. Examples may include the following:

- Risks resulting from failing to capture records:
    - Failure to capture a record into a recordkeeping system leading to compliance breaches with regulations that require the record to be registered.
    - Failure to save a record to the correct drive leading to non compliance with business requirements due to the inability to locate the record required.
- Risks resulting from failing to control records:
    - Failure to prevent agency personnel from taking work files home and not returning them leading to accusations of negligence and breaches of confidentiality.
    - Failure to prevent the post-creation adjustment of the date a document was created, leading to accusations of deliberate tampering to create a false record when contested in court.
- Risks resulting from failing to control access to records:
    - Inadequate records access controls leading to political embarrassment as confidential documents are leaked to the media.
    - Inappropriate security provisions leading to litigation for breach of contract as confidential consultancy files are emailed to the wrong external email address.

[1] Standards Australia, *AS/NZS ISO 31000 Risk Management: Principles and Guidelines*, Standards Australia, Sydney, 2009, section 2.1 p 1

[2] Standards Australia, *AS/NZS ISO 31000 Risk Management: Principles and Guidelines*, Standards Australia, Sydney, 2009, section 2.2 p 2

[3] National Archives of Australia, Use Records to Manage Risk, National Archives of Australia, Canberra, <http://www.naa.gov.au/records-management/im-framework/risk/index.aspx> viewed 11 May 2010

- Risks resulting from failing to store records appropriately:
    - Flooding of the basement after torrential rain leading to the impairment of operations due to client files being reduced to a pulp.
    - Infestation of pests (including tiger snakes) in the storage area leading to the hospitalisation and near death of a registry officer, destruction of paper files, and damage to the wiring of a key server.
- Risks resulting from failing to dispose of records appropriately:
    - Failure to prevent email from being deleted from inboxes without checking for and saving corporate emails leading to the agency damaging its reputation by not being able to produce proof of an agreed course of action.
    - Failure to ensure records destruction services provided by a contractor are using appropriate destruction methods leading to political embarrassment as confidential records are found by the media under a bush in a farmer's paddock.
- Risks resulting from failing to manage records strategically:
    - Failure to ensure that agency personnel are aware of their recordkeeping responsibilities leading to key records (such as corporate email) not being captured into the corporate recordkeeping system, and therefore not accessible when needed to answer the questions of an auditor from the Victorian Auditor General's Office.
    - Failure to prevent the deletion of electronic documents by the information technology unit (to increase hard drive space) without checking with the records management unit for implications leading to the agency being fined under the Crimes (Document Destruction) Act for breach of compliance.

Business related risks occur as a result of business action but are indirectly related to records management activities. That is, they occur as part of normal business operations rather than as a direct result of records management activities. The risk identified may not be specifically linked to records management practice, but may be mitigated through improved recordkeeping practice. Examples may include the following:

- An audit of agency practice regarding its management of contracts being undertaken leading to a lack of transparency regarding the agency process being noted that is suggestive of bribes being taken. Risks revealed by the audit may be addressed through the implementation of a consistent and transparent records management process for agency contracts.
- Failure to pass on critical business knowledge when staff members leave leading to the inability for the agency to explain why a particular course of action was taken. Risks may be treated through capture of key knowledge in policies, procedures, guidelines, and other records.

2.2. The Risk Management Framework

A risk management framework is the 'set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation'.[4]

[4] Standards Australia, *AS/NZS ISO 31000 Risk Management: Principles and Guidelines*, Standards Australia, Sydney, 2009, section 2.3 p 2

The risk management framework should include a risk management strategy, policy, a stakeholder engagement plan, and governance structure. Records managers should be aware of the risk management framework that exists in the agency. This is due to the importance of aligning the records management and risk management functions across the agency. Alignment enables records related risks and business risks with a recordkeeping component to be identified and addressed consistently. Alignment may be achieved by:

- Ensuring that the risk management strategy includes recordkeeping requirements;
- Aligning the risk and records management policies;
- Regular communication between the records management and risk management teams;
- Identifying any risks associated with the agency's current records management practices and procedures through regular self-assessments and internal audits;
- Emphasising records management as a good risk mitigation tool as poor recordkeeping practices increase the agency's liability and risk sensitivity;
- Ensuring that potential risks are identified and reported to the relevant people; and
- Implementing records management practices and tools that contribute to risk mitigation.

It is recommended that agencies adopt an accepted risk management process so that the risks within its functions and activities are actively managed. A risk management framework is described in the following publications (see the References section for publication details):

- AS/NZS ISO 31000: 2009 *Risk management—Principles and guidelines;*
- The Victorian Managed Insurance Authority's *Victorian Government Risk Management Framework,* and
- IEC/ISO 31010: 2009 *Risk management—Risk assessment techniques.*

Effectively managing current and future recordkeeping risks:

- Contributes to the continuous improvement of agency processes and practices;
- Increases the likelihood of your records management programme succeeding;
- Encourages a high standard of accountability;
- Ensures good recordkeeping practices are established and adhered to;
- Supports better business decision making;
- Facilitates compliance with government requirements; and
- Protects staff, assets, visitors, property and reputation.

2.3. The Risk Management Process

The risk management process recommended in this guideline follows that proposed by the Australian Standard AS/NZS ISO 31000. It consists of the following steps:

- Step One: Establish Context
- Step Two: Identify Risks
- Step Three: Analyse Risks
- Step Four: Evaluate & Prioritise Risks
- Step Five: Treat Risks

- Step Six: Review & Monitor Risks

Communication and consultation with both internal and external stakeholders provides a full understanding of recordkeeping risks and the risk management process. The benefits of managing recordkeeping risks should be clearly identified to all stakeholders to draw their support and commitment. This can be achieved through awareness and training programmes, and regular communications. For information on stakeholder engagement, please see PROV *Guideline 7: Stakeholder Engagement*.

Appendix A shows a detailed chart of the recommended risk management process as addressed in steps one through to six below[5].

Step One: Establish Context

This step establishes the internal and external context within which risks will be identified, assessed and treated. For risks relating to records, this means establishing the records management context, including the legislative and regulatory environment, business environment, and cultural environment[6]. This step includes the development of the risk assessment framework and criteria.

Step Two: Identify Risks

This step establishes methodologies and practices to identify and describe risks. This means identifying and describing risks related to recordkeeping, or which have recordkeeping implications.

Step Three: Analyse Risks

Step three assesses each risk identified to determine the level of risk so that an informed decision can be made regarding how to treat it. There are a number of records management activities that require a risk assessment to be conducted.

Step Four: Evaluate & Prioritise Risks

This step evaluates the results of the analysis conducted in step three in order to determine which risks are higher than others. Step four evaluates the level of risk so that decisions can be made regarding which risk to address first. This will include consideration of the future direction of records management within the agency as well as current practice.

Step Five: Treat Risks

During this step identified risks are matched to an appropriate treatment, and the actions associated with the treatment are carried out. Records management treatments may include the development and communication of procedures or tools, the alignment of key strategies and policies, or the adjustment of the records management programme.

Step Six: Review & Monitor Risks

Step six reviews and monitors risks to ensure that the treatment actions have been completed, determine the effectiveness of the treatment conducted, and identify any resulting

[5] The risk management process as described in this Guideline is based on the Australian and New Zealand Standard, *AS/NZS ISO 31000 Risk Management – Principles and Guidelines*, 2009.

[6] Cultural environment refers to the actual practice in the agency and community expectations regarding what the practice should be.

risks or actions required. Records management tools, such as records management programme self-assessments, can be used to assist with the monitoring and review of recordkeeping risks.

2.4. Assessing Recordkeeping Risks

Records related risks require an assessment of the following:

- The records management programme; and
- Agency compliance with the records management programme.

Business related risks require an assessment of the following:

- Information security systems and processes;
- Information access systems and processes;
- Internal audit systems and processes; and
- Reporting systems and processes.

3. Aligning Risk & Records Management

Identifying, assessing and managing risks related to records and records management should be incorporated into the agency's records management programme. This will enable recordkeeping risks to be addressed holistically and consistently across the agency. For example:

- Alignment of the risk management policy and the records management policy will ensure that the responsibilities regarding each policy for all agency personnel are clarified.
- Alignment of the risk management strategy and the records management strategy will enable risks related to records and records management to be considered, reported, and addressed, as part of the agency-wide risk management process.
- The risk management team will be a key stakeholder group, with the records management stakeholder engagement plan including methodologies for engaging with their representative to align the records management and risk management functions.
- Development and communication of recordkeeping procedures that describe the identification of recordkeeping risk and how to report them will provide direction to agency personnel.
- Recordkeeping processes for assessing and reporting risks may be aligned with the risk management process and with the review and update of key records management services and activities.
- Auditing processes for assessing agency business practice may include a component that flags and reports to the records management unit risks with a recordkeeping component.
- Assessment of recordkeeping practices (self-assessments or audits) may be used to identify and report risks related to records or records management.
- Records management systems and structures may be designed to automatically identify and report systems-related recordkeeping risks.
- Resources may be brought into the records management team to ensure that the entire records management programme of the agency is assessed for potential risks and adjusted to minimise any risks identified.

3.1. Functional Alignment

Aligning the records management and risk management functions provides the following benefits:

- Recordkeeping risks are identified and reported through risk management processes, enabling their mitigation.
- Evidence (in the form of records or procedures and directives) to support the appropriate mitigation of risk exists and may be produced if required.
- Awareness of the risks associated with records and the benefits of effective records management regarding mitigation of risks is increased.

Alignment may be achieved by engaging with the risk management team as a key stakeholder group so that common understanding is achieved.

3.2. Strategic Alignment

Aligning the records management and risk management strategic directives provides the following benefits:

- Risk and records management are perceived of as complimentary methods of achieving agency strategic objectives.
- Responsibilities of agency personnel are clearly defined and described regarding both risk management and records management.
- Mutual understanding of the relationship between risk management and records management is achieved by open and ongoing communication between the risk management and records management teams.

Strategic alignment is achieved through the alignment of the risk management and records management strategies and policies.

3.2.1. Alignment with Strategy

The records management strategy will include an assessment of risks related to recordkeeping. The risk management process outlined in this guideline may be used to identify and assess the risks described in the strategy. The strategy's objectives, goals and actions should mitigate risks that were identified in the assessment.

The risk management strategy should include records management requirements. To achieve this, the risk management team will need to understand the relationship between records and risk. That means understanding both records related risks and business risks that have records or recordkeeping implications. Both of these risks are referred to as recordkeeping risks in this Guideline. The risk management process should also be clearly documented. Communication between the records management and risk management team is essential to achieve mutual understanding of records management requirements.

3.2.2. Alignment with Policy

The records management policy will document the responsibilities of agency personnel, and the agency directives, regarding recordkeeping. The risk management policy will document the responsibilities of agency personnel, and the agency directives, regarding risk management. The two policies will need to align in order to ensure that the responsibilities and directives documented in them are consistent with each other.

Suggested responsibilities are as follows:

Head of Government Agency

The head of a government agency has ultimate responsibility for the efficient management of records within an agency.

Senior Executives

An agency's senior executives are responsible for:

- The records management framework;
- Monitoring and reporting on risks; and
- Integrating reporting with the agency's risk management process.

Records Managers

Records managers are responsible for:

- Ensuring that the records management framework identifies recordkeeping risks and strategies to mitigate them;
- The ongoing development of the records management programme so that systems, processes, tools and procedures are continuously developed and assist with the identification, reporting, assessment and mitigation of recordkeeping risks;
- Regular monitoring of records management practice so that new recordkeeping risks may be identified, reported and mitigated; and
- Reporting the risks identified to the appropriate person so they may be captured in the risk register.

Staff, Contractors & Volunteers

Staff and contractors need to follow risk procedures and are responsible for:

- Identifying risks related to recordkeeping and reporting these to the relevant risk champion;
- Monitoring and reviewing recordkeeping risks within their areas; and
- Providing risk information when requested.

3.3. Reporting Alignment

There are a number of records management tools and reports that can be used to record and report risks related to recordkeeping. For example:

- Monitoring reports, such as systems reports of recordkeeping systems, may include functionality that automatically collates and issues regular reports on systems faults and errors that may be a risk.
- Self-assessment questionnaires and internal audits of agency business practice, processes and systems against the requirements of the records management programme may be used to identify and report on recordkeeping risks.
- Records management activities, such as the records management strategy, can be used to record and report risks to the senior executive.

Additional reporting mechanisms may be required to ensure that reporting of recordkeeping risks occurs and that the right people are kept informed. This may include the following:

- Reporting recordkeeping risks to the risk management team;
- Recording recordkeeping risks in the risk register;
- Keeping the senior executive informed of risks related to recordkeeping;
- Using the Risk Management Steering Committee, if one exists, as a forum for reporting and discussing recordkeeping risks;
- Setting up reporting procedures; and
- Assigning responsibilities to ensure that risks are reported and recorded appropriately.

4. Conducting a Risk Assessment

Risk assessments will need to be conducted as part of various records management activities, including:

- Records management strategy;
- Business case for records management projects;
- Records management programme development or update; and
- Records management systems development or upgrade.

The risk management process identified in section 2.3 (above) may be used to conduct a risk assessment, and incorporate the results into the agency's risk management framework. The assessment will be focused on an assessment framework that is based on the agency's records management context.

4.1. Step One – Establish Context

The records management context of the agency will need to be established so that an assessment framework can be developed. This step requires an examination of the external, organisational and records management environment in which risk identification, analysis and treatment options will be considered. Including the:

- Legislative and regulatory environment regarding records;
- Business environment, including actual agency practice, regarding recordkeeping; and
- Community expectations regarding the creation, maintenance and disposal of agency records.

Internal and external stakeholder identification and analysis is an important component in establishing the context. See PROV *Guideline 7: Stakeholder Engagement* for further information.

The agency may have already drafted several documents that will help you identify the context under which you will establish a risk assessment framework. These may include:

- Records Management Strategy;
- Records Management Policy;
- Stakeholder Engagement Model; and
- Recordkeeping Key Performance Indicators.

The *Victorian Government Risk Management Framework* (VGRMF)[7] may also help. Agencies may be required to adopt the VGRMF in order to comply with the *Financial Management Act 2004* and Ministerial Standing Orders made under that Act.

[7] Department of Treasury and Finance 2007, *Victorian Government Risk Management Framework*, DTF, Melbourne, viewed 30 April 2010 <http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/VicGovtRiskMgmtFramework/$File/VicGovt%20Risk%20Mgmt%20Framework.pdf>

4.1.1. Existing Controls

Contingency plans, such as business continuity plans and disaster preparedness plans, put in place controls that can mitigate possible future risks. Records management processes and services may have a contingency plan component in that they can also mitigate possible future risk.

Existing controls are the services and processes that the agency already has in place to manage their business operations. Existing controls minimise negative risks and maximise positive ones. Table 1 (below) provides a number of controls that may be in place to manage agency records.

Control	*How it mitigates risk*
Records Management Strategy	• Aligns with risk management to ensure that recordkeeping risks are identified and reported so that they can be mitigated. • Provides a holistic road map of the future direction of the agency regarding records management so that recordkeeping activities, such as capture, disposal, and storage are strategically planned across the entire agency, rather than being ad hoc. Risks related to ad hoc records management will be lessened as a result.
Records Management Policy	• Communicates agency directives and responsibilities regarding recordkeeping so that agency personnel are aware of expectations regarding recordkeeping activities. Risks related to agency personnel being unaware of their responsibilities will be lessened. • Directives regarding the use of USB Sticks, application of the Information Privacy Principles, and security or access provisions lessen the risk of accidental security breaches.
Records Management Procedures	• Procedures that cover the entire records management process ensure actions are carried out consistently, lessening the risk of inappropriate records management practice. • Procedures can be used to govern the records management of business systems that contain records but have no recordkeeping functionality. This lessens the risk of records contained within business systems not being assigned appropriate disposal or access provisions.
Records Management Systems	• Electronic records management systems lessen the risk of electronic records being lost or inappropriately disposed of. • Manual records management systems can be used to control a records management process, such as the disposal process. This lessens the risk of inconsistent practice across the agency.
Programme	• The records management programme provides an agency wide and strategic approach to records management that is supported by procedures, systems, and appropriate resources. This lessens risk by providing sufficient direction and tools for agency personnel to undertake consistent and appropriate records management. • The disposal programme provides a consistent and holistic approach to the disposal of agency records. This lessens risk by ensuring that records are retained for the duration of their retention period so that the cost of retaining records is reduced, and records are disposed of appropriately.
Plan / Scheme	• Classification and naming schemes provide a consistent method for filing of records. This lessens the risk of records becoming lost due to inappropriate filing as the names of files are consistent, and the methodology used to file records is consistent, across the agency. • Disaster recovery, disaster preparedness, and business continuity plans provide the means for agencies to plan for continual operations in the event of an emergency. This lessens risk by identifying the areas of concern so that risks regarding them can be mitigated, and by developing contingency plans to preserve records needed for ongoing operations.
Communications	• Stakeholder engagement plans and other formalised communications provide the means for recordkeeping requirements to be promoted across the agency. This lessens the risk of records being lost, or inappropriate access, due to ignorance of what the recordkeeping requirements are. • Training in records management practice provides hands-on experience of recordkeeping to agency personnel. This lessens risk by providing the opportunity for agency personnel to understand the implications of what is being asked of them so that they can raise any issues they may have, and improve recordkeeping practice.

Control	*How it mitigates risk*
Assessments	• Self-assessments and internal audits provide the means for the assessment of recordkeeping practice against the requirements specified in the agency's records management programme. This lessens risk by identifying problem areas so that risks identified can be mitigated. • Inspection of recordkeeping practice undertaken on behalf of the agency provides the means for the agency to identify any compliance issues. This lessens risk by identifying issues, such as incorrect disposal practice, so that they may be mitigated before the agency is politically embarrassed by the issue being made public.

Table 1: Existing Recordkeeping Controls

Completion of step one, should provide an understanding of the context within which recordkeeping risks occur. This will help with identifying risks, establishing assessment criteria, and evaluating risks. Treatments for mitigating risks may need to be incorporated into aspects of the records management programme. See Appendix E for a risk assessment checklist.

4.2. Step Two – Identify Risks

An assessment framework for recordkeeping risks requires a consistent methodology for identifying and describing risks. This includes a set of risk categories to classify risks, a set of tools for identification of risks, and common language to describe them.

4.2.1. Risk Categories

The context identified at step one may suggest common agency recordkeeping risks that can be used to determine the types of recordkeeping risks an agency may face. For example, the risk categories that arise from the results of step one may be as follows:

- *Unauthorised Disclosure*, such as staff emailing a confidential document to the media causing significant embarrassment to the agency.
- *Unauthorised Destruction*, such as someone deleting documents without approval resulting in the loss of a court case as the agency was unable to produce the documents or provide a reasonable excuse for records not being available.
- *Unauthorised Modification*, such as someone editing final versions of records leading to questions as to why an agency's document is radically different from that provided by a client in court.
- *Accidental Loss*, such as staff failing to save a record into a recordkeeping system resulting in death or injury as emergency services staff used the wrong version of building plans or drawings.
- *Environmental Damage*, such as a rodent infestation, fire, flood, or electromagnetic fields, severely impairing business operations as records central to continuing operations were lost or irretrievably damaged.
- *Hardware Failure*, such as a computer server hard disk crash resulting in the loss of all agency records for the past five years as the agency had no disaster recovery plan, did not back up their electronic files, and no longer kept paper files.
- *Malicious Damage*, such as a hacker deleting a database that held the only details about the childhood of a former ward of the state.
- *Theft*, such as an intruder stealing key infrastructure files from an office and selling them to a known terrorist organisation.

4.2.2. Risk Identification Tools

There are a number of tools and methods that records managers can use to identify risks related to records and recordkeeping:

- SWOT analysis to identify risks associated with the strengths, weaknesses, opportunities and threats of the agency's records management programme.
- Political, Economic, Socio-cultural, and Technology (PEST) analysis to brainstorm risk factors, identify the context, and draw conclusions from this information regarding what the recordkeeping risks are.
- Tailored questionnaires, such as records management self-assessments.
- Reports of audits conducted by the agency's internal audit team, or by an external agency such as the Victorian Auditor-General's Office or Ombudsman.
- Interviews with agency personnel to understand recordkeeping practice and issues.
- Interviews with external stakeholders to determine potential recordkeeping risks.
- Brainstorming exercises and focus groups to identify recordkeeping risks associated with specific processes or business activities.
- Research conducted for records management or other areas of the agency that identify potential recordkeeping risks.

The tool or selection of tools used to identify risk will depend on the risk management framework that the agency is using, and on the purpose for the risk assessment. For example, the records management strategy uses SWOT analysis to identify risks.

Risks identified may be under the control of the agency or external to the agency.

4.2.3. Describing Risks

When describing a risk the following three elements should be considered:

- **Risk Description/Event:** An occurrence or a particular set of circumstances;
- **Causes:** The factors that may contribute to a risk occurring or increase the likelihood of risk occurring; and
- **Consequence:** Outcome or impact of an event.

When the risk is recorded in the risk register, the event, causes and consequences will also need to be recorded. The agency may already have a risk register in place as part of an existing risk management framework, or one may need to be developed. A process to report recordkeeping risks so that they are recorded in the risk register will also be needed.

Example Risk:

The agency record's storage is in an area where there is a high incidence of flooding, including their client case files which are stored in the building's basement. So that they are easier to access by staff, the client case files are stored on the two bottom shelves. There have been numerous cases in the community where 50 cm of water flooded basements after a heavy rainfall and damaged the owner's property. In most cases, the property had to be replaced.

- The risk description is basement flooding;
- The cause is heavy rainfall; and
- The consequence is destruction of records which could not be salvaged.

Completion of step two should provide a common list of risk categories, tools, methodologies and information that should be captured when describing records related risks.

4.3. Step Three – Analyse Risks

Risk analysis is about developing an understanding of the risk. It is the process of reviewing all available information about the identified risks and measuring them against established criteria for impact (consequence) and likelihood of occurrence.

An assessment framework for recordkeeping risks requires a consistent methodology for analysing the risks identified. The context and risks identified in steps one and two will enable a set of recordkeeping risk criteria to be developed so that the likelihood and consequences of recordkeeping risks can be assessed consistently.

Current recordkeeping systems and the records management programme should be designed so that they either reduce the likelihood of the risk or mitigate the consequences if the risk occurs. After the agency has analysed the risks identified against the current systems and programme, they can assess the impact (consequence) of each and record the results in the risk register.

4.3.1. Consequence & Likelihood Ratings

The consequences rating will depend on the specific context of the agency, which may include:

- The functions it performs;
- The requirements that the agency is required to meet; and
- General recordkeeping practice.

Table 2 (below) provides the scale of risk consequences from 1 (Extreme) to 5 (Insignificant).

Scale	*Rating*	*Consequence if the risk occurs*
1	Extreme / Catastrophic	Operations would be impaired and life may be threatened.
2	Very High / Major	Political embarrassment would occur; Actions or decisions could not be explained to the satisfaction of courts, or regulatory and inquisitorial bodies; Financial loss would occur due to duplication of work already done or compensation to affected parties.
3	Medium / Moderate	Compliance with regulatory, legislative, or business requirements would not occur.
4	Low / Minor	Key information would be lost and duplication of work would occur.
5	Negligible / Insignificant	Work processes would be inefficient; Decision made and actions taken would be made on the basis of incomplete or out of date information.

Table 2: Risk Consequence Rating Scale

In conjunction with analysing the impact of each risk, the agency needs to determine the likelihood of an event associated to the risk happening. Likelihood should be determined by examination of agency practice as well as policy. Determining the likelihood of the risk will help the agency to evaluate and prioritise risks. Table 3 (below) provides the levels of likelihood from A (Almost Certain) to E (Rare).

Level	*Likelihood*	*Description*
A	Almost Certain	The event is expected to occur
B	Likely	The event will probably occur
C	Possible	The event may occur at some time
D	Unlikely	The event could occur at some time
E	Rare	Remote chance event may occur

Table 3: Risk Likelihood Rating[8]

Example Risk:

The risk control would be qualified as poor because the client case files are stored in an area where water damage can occur. After analysing the risk further, the agency determined that the consequence of the basement flooding and damaging the records stored on the bottom two shelves scores “3” on the consequence rating scale:

There is a significant financial loss because the records affected constitute 10% of the agency’s records and most are irreplaceable. The recordkeeping system’s integrity is undermined because it does not meet PROV requirements for appropriate storage of records. Business will be affected because some records are used on a daily basis and they will need significant staff effort to recreate.

Although the agency building meets construction standards, a review of incidences of flooding in the area over the last 10 years suggests that it is possible for the basement to flood, but it is not likely.

Table 4 (below) uses the risk categories identified in section 4.2.1 (above) to determine possible records management risks and risk consequences. Each risk consequence has been assigned a potential risk consequence rating and likelihood rating, based on an agency with minimal records management coverage. Please note that these ratings will change depending on the context and circumstances of the agency concerned.

[8] Note that this table is an adaptation of the scale illustrated in AS/NZS 4360: 2004, p. 54 which uses eight levels of likelihood on its scale.

Risk Category	*Risk*	*Consequence*	*Risk Consequence Rating*	*Risk Likelihood Rating*
Unauthorised Disclosure	Inadequate records access controls leading to political embarrassment as confidential documents were leaked to the media.	Potential embarrassment to the agency, the parent department, minister, and / or Victorian government may lead to the sacking of personnel or investigation by a regulatory or investigatory authority.	2 – Very High / Major	C – Possible
	Inappropriate security provisions leading to litigation for breach of contract as confidential consultancy files were emailed to the wrong external email address.	As the information is commercial in confidence, the agency may be sued for damages or for breach of contract. If business was lost as a result, the agency may be required to compensate the consultancy for their losses.	2 – Very High / Major	C – Possible
	Private information gathered about clients was not protected with an appropriate level of security, leading to an accusation of breach of compliance with Information Privacy legislation.	Privacy Victoria may be called in to investigate potential compliance breaches with the Information Privacy Act 2000.	3 – Medium / Moderate	B – Likely
Unauthorised Destruction	The deletion of electronic documents by the information technology unit to increase hard drive space without checking with the records management unit for implications leading to the agency being fined under the Crimes (Document Destruction) Act for breach of compliance.	It could be argued that the deletion occurred to prevent records from being produced when required to do so. This may result in damage to an agency's reputation and reduce the impact of other agency records produced in court. The agency may be fined as a result, or be required to financially compensate the other party.	3 – Medium / Moderate	C – Possible
	Records destruction services provided by a contractor do not use appropriate destruction methods leading to political embarrassment as confidential records were found by the media under a bush in a farmer's paddock.	A confidential document could be recovered from a dump site and made public when it should have been destroyed. As a result, the agency, minister, or the Victorian Government could be publicly embarrassed. Records management staff may be blamed for not checking that the contractors were carrying out the service they were hired to do properly, and may be terminated as a result.	2 – Very High / Major	B – Likely
	Email is deleted from inboxes without checking for and saving corporate emails leading to the agency damaging its reputation by not being able to produce proof of an agreed course of action.	The agency may not be able to counter email produced as evidence in court. Damage to the agency's reputation as a result may lead to the demand for investigations into agency practice. The agency may not be able to demonstrate appropriate recordkeeping culture when addressing charges under the Crimes (Document Destruction) Act.	2 – Very High / Major	B – Likely

Risk Category	*Risk*	*Consequence*	*Risk Consequence Rating*	*Risk Likelihood Rating*
Unauthorised Modification	Changing key phrases in a 'final' version of a policy without saving it as a new version leading to questions regarding whether or not staff members are carrying out specified responsibilities appropriately.	Responsibilities of staff are documented in policies, which may be translated across to performance plans for individual staff. If the policy has been adjusted and the adjustment is not saved as a new version, there will be conflict regarding what is in the performance plans and what is in the policy. This will lead to confusion over what the authorised policy says, and may result in accusations of mismanagement of records that could reduce the agency's professional reputation.	3 – Medium / Moderate	B – Likely
	Adjustment of the date a document was created leading to accusations of deliberate tampering to create a false record when contested in court.	If the document is a key piece of evidence and the date of creation is important, the fact that the date of the document was adjusted will be seen as a deliberate act to hide something. When detected, the agency may be required to answer criminal charges, its reputation may be damaged, and political embarrassment may occur.	2 – Very High / Major	C – Possible
	Not saving a 'final' record in a format that is approved and supported by the agency leading to the record not being accessible or readable five years later as required by its assigned retention period.	The agency breaches compliance with the retention and disposal authority created under the Public Records Act 1973 if its records are not accessible and readable for the duration of its retention period.	3 – Medium / Moderate	B – Likely
Accidental Loss	Failure to capture a record into a recordkeeping system leading to compliance breaches with regulations that require the record to be registered.	Possible compliance breaches if the record is required to be formally registered, or it is not assigned appropriate access provisions or disposal actions. The agency may not be able to locate the record when required.	3 – Medium / Moderate	B – Likely
	Failure to save a record to the correct drive leading to non compliance with business requirements due to the inability to locate the record required.	The agency may not be able to locate the record when required. Another danger is that the record will no longer be accessible if it is located due to changes in software and hardware over time.	3 – Medium / Moderate	B – Likely
	Failure to pass on critical business knowledge when staff members leave leading to the inability for the agency to explain why a particular course of action was taken.	Knowledge is lost due to it not being captured as part of the corporate record. As a result the agency is not able to benefit from that knowledge. Loss of knowledge regarding normal business practice may result in the agency failing to explain why something occurred when addressing a court, regulatory authority, or inquisitorial body.	2 – Very High / Major	A – Almost Certain

Risk Category	*Risk*	*Consequence*	*Risk Consequence Rating*	*Risk Likelihood Rating*
Environmental Damage	Flooding of the basement after torrential rain leading to the impairment of operations due to client files being reduced to a pulp.	If the damage results in the information contained within the documents not being legible, the agency may lose records vital to its ongoing operations. If the damage results in the growth of mould, the agency may endanger the health of its employees.	1 – Extreme / Catastrophic	A – Almost Certain
	Bush fire totally destroys the main storage repository for agency records leading to impairment of agency operations and the death of the repository manager.	Agency personnel may have died in the fire. Technology and paper records may be irretrievably damaged, or completely destroyed. The agency may lose the corporate memory it requires for business continuity, and not be able to produce records when required to do so. Valuable historical and personal identity records may also be lost.	1 – Extreme / Catastrophic	B – Likely
	Infestation of pests (including tiger snakes) in the storage area leading to the hospitalisation and near death of a registry officer, destruction of paper files, and damage to the wiring of a key server..	If the pest infestation is poisonous spiders or snakes, it may result in injury or death to agency employees. Vital records or information may be lost, which may reduce the ability for the agency to access and read records when required to do so. Pest infestation may increase the risk of fire by increasing the amount of fuel available, or by chewing electrical wires.	1 – Extreme / Catastrophic	C – Possible
	Decreases in oxygen caused by pollution in a storage area leading to the death of a repository worker.	Pollution may decrease the amount of oxygen available in storage areas, increasing the risk to employees' health if they are required to work in such areas. Records may deteriorate faster if the pollution leads to increases in humidity or acidity, especially for fragile media such as video or film.	1 – Extreme / Catastrophic	D – Unlikely
Hardware Failure	The crash of a computer-server hard drive leading to financial loss due to work having to be duplicated.	Electronic records that have not been backed up are lost. This results in duplication of work to recreate lost files, or the possibility of the agency no longer being able to reproduce records when required to do so.	2 – Very High / Major	B – Likely
	Failure of the agency to back up computer systems leading to the loss of records required to address potential litigation as evidence of past actions.	The agency will not be able to satisfy the concerns of a regulatory or inquisitorial body, or a court, if the records are needed to demonstrate actions or decisions made. The agency may need to fund the duplication of work lost as a result.	2 – Very High / Major	B – Likely
	Failure to open old-format files as the system used was not backwards compatible leading to retention periods being compromised.	Retention periods may be compromised as records, regardless of format, must remain accessible and readable for the duration of their retention period. Failure to retain accessible and readable records for the duration of their retention periods may result in the agency being accused of negligence.	3 – Medium / Moderate	B – Likely

Risk Category	*Risk*	*Consequence*	*Risk Consequence Rating*	*Risk Likelihood Rating*
Malicious Damage	Failure of the agency to prevent a database being hacked leading to the financial costs of the computer and security systems being reviewed, and deleted or adjusted data reclaimed.	The agency may be required to reproduce the database. Measures may be needed to reduce the impact of the potential disclosure of this information. The agency will need to undergo a systems check to determine what has been compromised.	2 – Very High / Major	C – Possible
	Terrorists destroying records central to the operations of key Victorian infrastructure leading to multiple deaths of the public.	Destruction of records central to the operations of key Victorian infrastructure may lead to the deaths of multiple people due to lack of essential services information they contain.	1 – Extreme / Catastrophic	D – Unlikely
	Recently fired employee changes the passwords of a crucial database before leaving to hamper agency operations leading to the cost of retrieving the passwords.	The agency may require specialists to retrieve the new passwords so that key databases can be accessed, This may be expensive, and time consuming, and hamper operations temporarily.	2 – Very High / Major	D – Unlikely
Theft	Failure to prevent office files from being stolen leading to the inability to supply records to support key decisions or actions when required.	The agency may not realise that files have gone missing until they are required to produce them, which may be months or years after they were taken. This will cause embarrassment, and may lead to accusations of negligence.	2 – Very High / Major	C – Possible
	Failure to prevent agency personnel ‘rescuing’ records of potential historical value leading to breaches of the Public Records Act 1973.	When detected, the agency will be required under the Public Records Act 1973 to recovery any missing records identified as being State Archives.	3 – Medium / Moderate	D – Unlikely
	Failure to prevent agency personnel from taking work files home and not returning them leading to accusations of negligence and breaches of confidentiality.	The agency may face accusations of negligence and compliance breaches by permitting this practice without properly tracking and ensuring the maintenance of access provisions on the records concerned, and the return of the records. Public embarrassment may occur if confidential files are thrown out rather than disposed of properly.	3 – Medium / Moderate	B – Likely

Table 4: Risk Categories and some associated Risks and Consequences

Completion of step three should provide a clear understanding of what the recordkeeping risks are, as well as the level of risk for each. This will enable decisions to be made regarding the treatments required for each risk identified.

4.4. Step Four – Evaluate & Prioritise Risks

An assessment framework for recordkeeping risks will include mechanisms for making decisions regarding what to do about the risks. The risk evaluation and prioritisation use the analysis conducted in the previous step to make decisions about which risks need what treatment. This requires an analysis of the level of risk and of the controls that currently exist to mitigate the risk.

4.4.1. Mapping the Level of Risk

Mapping the consequence and likelihood ratings against the identified risks provides the agency with sufficient information to determine the level of risk involved. Recordkeeping risks predominantly involve risk to the agency's reputation or ongoing operations. Whilst this may have a financial consequence (such as the loss of a potential court case), determining the actual cost may be problematic.

Evaluation consists of examining the information collated in step three. The consequence and likelihood ratings are examined to determine the level of risk, and identify those with a high rating. Where risks scored a consequence rating of 1 (Catastrophic) and likelihood rating of A (Almost Certain), the level of risk would be evaluated as being very high. The risk would therefore be prioritised as being in great need of treatment. On the other hand, a consequence rating of 5 (Insignificant) and a likelihood rating of E (Rare) would result in the level of risk being evaluated as very low, and treatment given a low priority.

A difficulty with recordkeeping risks is that in many instances the ratings provided will be mid-range (for example, a consequence rating of 3, and a likelihood rating of C). When identifying the possible consequences of recordkeeping risks, think very carefully about what impact it will have on the business of the agency. This may help to clarify the consequence so that it is assigned an appropriate consequence and likelihood rating.

Existing records management controls may mitigate the level of recordkeeping risk fully or partially.

Likelihood	**Consequence**				
	Negligible/ Insignificant 5	Low/ Minor 4	Medium/ Moderate 3	Major/ Very High 2	Catastrophic/ Extreme 1
E (Rare) - 5	25	20	15	10	5
D (Unlikely) - 4	20	16	12	8	4
C (Moderate) - 3	15	12	9	6	3
B (Likely) - 2	10	8	6	4	2
A (Almost Certain) - 1	5	4	3	2	1

Table 5: Risk Heat Map[9]

[9] Based on AS/NZS 4360: 2004, p. 55 used to analyse the level of risk. An example of a risk heat map can also be found in VMIA 2008, *Guide to developing and implementing your risk management framework*, p. 80.

Results of the Risk Heat Map

1 – 6 = High Risk (Red)

8 – 15 = Medium Risk (Yellow)

16 – 25 = Low Risk (Green)

Using a risk heat map, such as the one in Table 5 (above), enables the level of risk to be determined (for example, high, medium, or low). A matrix can be developed to plot the risks so that the level may be determined for each risk. This will enable the high risk areas to be clearly identified so that they can be treated first.

The agency may already have processes or services in place that will reduce the level of risk. These will need to be taken into consideration and the level of risk adjusted accordingly. The reason for this is to ensure that the risks are prioritised according to what needs to be done to mitigate them.

Table 6 (below) uses the data from Table 4 (above) and the risk heat map (Table 5) to determine the level of risk.

Risk Category	*Risk*	*Consequence Rating*	*Likelihood Rating*	*Level of Risk*
Unauthorised Disclosure	Inadequate records access provisions leading to political embarrassment as confidential documents were leaked to the media.	2 – Very High / Major	C – Possible	High
	Inappropriate security provisions leading to litigation for breach of contract as confidential consultancy files were emailed to the wrong external email address.	2 – Very High / Major	C – Possible	High
	Private information gathered about clients was not provided with an appropriate level of security, leading to an accusation of breach of compliance with Information Privacy legislation.	3 – Medium / Moderate	B – Likely	High
Unauthorised Destruction	The deletion of electronic documents by information technology unit to increase hard drive space without checking with the records management unit for implications leading to the agency being fined under the Crimes (Document Destruction) Act for breach of compliance.	3 – Medium / Moderate	C – Possible	Medium
	Records destruction services provided by a contractor do not use appropriate destruction methods leading to political embarrassment as confidential records were found by the media under a bush in a farmer's paddock.	2 – Very High / Major	B – Likely	High
	Email is deleted from inboxes without checking for and saving corporate emails leading to the agency damaging its reputation by not being able to produce proof of an agreed course of action.	2 – Very High / Major	B – Likely	High
Unauthorised Modification	Changing key phrases in a 'final' version of a policy without saving it as a new version leading to questions regarding whether or not staff members are carrying out specified responsibilities appropriately.	3 – Medium / Moderate	B – Likely	High
	Adjustment of the date a document was created leading to accusations of deliberate tampering to create a false record when contested in court.	2 – Very High / Major	C – Possible	High
	Not saving a 'final' record in a format that is approved and supported by the agency leading to the record not being accessible or readable five years later as required by its assigned retention period.	3 – Medium / Moderate	B – Likely	High

Risk Category	*Risk*	*Consequence Rating*	*Likelihood Rating*	*Level of Risk*
Accidental Loss	Failure to capture a record in a recordkeeping system leading to compliance breaches with regulations that require the record to be registered.	3 – Medium / Moderate	B – Likely	High
	Failure to save a record to the correct drive leading to non compliance with business requirements due to the inability to locate the record required.	3 – Medium / Moderate	B – Likely	High
	Failure to pass on critical business knowledge when staff members leave leading to the inability for the agency to explain why a particular course of action was taken.	2 – Very High / Major	A – Almost Certain	High
Environmental Damage	Flooding of the basement after torrential rain leading to the impairment of operations due to client files being reduced to a pulp.	1 – Extreme / Catastrophic	A – Almost Certain	High
	Bush fire totally destroys the main storage repository for agency records leading to impairment of agency operations and the death of the repository manager.	1 – Extreme / Catastrophic	B – Likely	High
	Infestation of pests (including tiger snakes) in the storage area leading to the hospitalisation and near death of a registry officer, destruction of paper files, and damage to the wiring of a key server..	1 – Extreme / Catastrophic	C – Possible	High
	Decreases in oxygen caused by pollution in a storage area leading to the death of a repository worker.	1 – Extreme / Catastrophic	D – Unlikely	High
Hardware Failure	The crash of a computer-server hard drive leading to financial loss due to work having to be duplicated.	2 – Very High / Major	B – Likely	High
	Failure of the agency to back up computer systems leading to the loss of records required to address potential litigation as evidence of past actions.	2 – Very High / Major	B – Likely	High
	Failure to open old-format files as the system used was not backwards compatible leading to retention periods being compromised.	3 – Medium / Moderate	B – Likely	High
Malicious Damage	Failure of the agency to prevent a database being hacked leading to the financial costs of the computer and security systems being reviewed, and deleted or adjusted data reclaimed.	2 – Very High / Major	C – Possible	High
	Terrorists destroying records central to the operations of key Victorian infrastructure leading to multiple deaths of the public.	1 – Extreme / Catastrophic	D – Unlikely	High
	Recently fired employee changes the passwords of a crucial database before leaving to hamper agency operations leading to the cost of retrieving the passwords.	2 – Very High / Major	D – Unlikely	Medium
Theft	Failure to prevent office files from being stolen leading to the inability to supply records to support key decisions or actions when required.	2 – Very High / Major	C – Possible	High
	Failure to prevent agency personnel ‘rescuing’ records of potential historical value leading to breaches of the Public Records Act 1973.	3 – Medium / Moderate	D – Unlikely	Medium
	Failure to prevent agency personnel from taking work files home and not returning them leading to accusations of negligence and breaches of confidentiality.	3 – Medium / Moderate	B – Likely	High

Table 6: Level of Recordkeeping Risk

Example Risk:

The agency identified that the likelihood and consequence of the risk that the basement may flood represent a significant risk that needs to be addressed. The records manager will draft a report explaining all the risks identified and include in them in risk register. Recommendations will be provided on the risks that can be managed under current controls, risks that are acceptable and risks that need to be treat. The issue of the records on the bottom two shelves in the basement is a risk that the risk committee is recommending for treatment to the agency's executive team.

4.5. Step Five – Treat Risks

An assessment framework for recordkeeping risks will require risks identified to be treated. The treatment options considered will be assessed based on the following information:

- The context established in step one;
- The risk category determined in step two;
- The likelihood, consequence and level of risk assessed at step three; and
- The priority assigned to the risk at step four.

Risk treatment involves identifying the range of options for treating risks, assessing these options and implementing treatment plans. The risks remaining after implementation of risk treatment plans are known as residual risks.

Existing controls may be adjusted, revised, updated, or upgraded to treat identified risks. New controls may need to be developed and implemented. The records management strategy may be used to identify systems or services that need to be developed or adjusted to treat recordkeeping risks.

Risks are evaluated as to whether they are acceptable and can continue to be managed within the parameters of the existing controls, or if they are unacceptable. A risk may be acceptable for some of the following reasons:

- The overall risk level is so low that treatment is not appropriate given an agency's resources;
- The risk is such that a treatment is not available;
- The cost of treatment is so manifestly excessive compared to the benefit that acceptance is the only option; or
- The risk is positive as it provides an opportunity for the agency.

Unacceptable risks will need to be mitigated. A treatment option will need to be identified and strategy determined to mitigate unacceptable risks.

4.5.1. Treatment Options

Options for treating risks may include the following[10]:

- Avoiding the risk;
- Taking the risk in order to take advantage of an opportunity;
- Removing the source of the risk;
- Changing the likelihood of the risk;
- Changing the consequence of the risk;
- Sharing the risk; and
- Retaining or accepting the risk after careful consideration.

Table 7 (below) explores the above options for the risks identified in Tables 4 and 6 (above).

Risk Category	*Risk*	*Treatment Option*	*Description*
Unauthorised Disclosure	Inadequate records access provisions leading to political embarrassment as confidential documents were leaked to the media.	Avoiding the risk	Ensure that all confidential documents are assigned the appropriate level of security and stored in a secure location. Ensure that agency employees are aware of the consequences to them for any deliberate unauthorised disclosure.
	Inappropriate security provisions leading to litigation for breach of contract as confidential consultancy files were emailed to the wrong external email address.	Taking the risk	The agency is confident that the security systems in place and filing practice across the agency are already sufficient to prevent this from happening.
	Private information gathered about clients was not provided with an appropriate level of security, leading to an accusation of breach of compliance with Information Privacy legislation.	Removing the source of the risk	Agency no longer collects private information.
Unauthorised Destruction	The deletion of electronic documents by information technology unit to increase hard drive space without checking with the records management unit for implications leading to the agency being fined under the Crimes (Document Destruction) Act for breach of compliance.	Changing the likelihood of the risk	Promote the consequences of unauthorised destruction, and the procedure for obtaining approval for destruction. Place posters above the shredders, and near all desktops. Train all agency employees in the procedure for identifying what documents can be destroyed and how they can be destroyed.

[10] Standard Australia and Standards New Zealand, *AS/NZS ISO 31000: Risk Management – Principles and Guidelines*, Standards Australia, Sydney 2009, p 19

Risk Category	*Risk*	*Treatment Option*	*Description*
	Records destruction services provided by a contractor do not use appropriate destruction methods leading to political embarrassment as confidential records were found by the media under a bush in a farmer’s paddock.	Changing the consequence of the risk	Monitor regularly the service provided by the contractor to ensure that the appropriate method of destruction is being applied.
	Email is deleted from inboxes without checking for and saving corporate emails leading to the agency damaging its reputation by not being able to produce proof of an agreed course of action.	Sharing the risk	Responsibility for ensuring corporate email records are identified and appropriately filed is assigned to all agency employees. Information technology team are required to liaise with the records management team prior to deleting employees email inboxes.
Unauthorised Modification	Changing key phrases in a ‘final’ version of a policy without saving it as a new version leading to questions regarding whether or not staff members are carrying out specified responsibilities appropriately.	Retaining the risk	After careful review of agency procedures and practices regarding document versions, the agency has decided not to take any action. The likelihood of the risk occurring is too low to warrant action.
	Adjustment of the date a document was created leading to accusations of deliberate tampering to create a false record when contested in court.	Avoiding the risk	The agency has installed new computer software that makes it impossible for dates to be changed on a document without leaving a clear and detectable audit trail.
	Not saving a ‘final’ record in a format that is approved and supported by the agency leading to the record not being accessible or readable five years later as required by its assigned retention period.	Taking the risk	The formats normally used and maintained by the agency are different to those used by their outsourced service provider. The contract between the agency and service provider did not mention document formats. Amending the contract to include this will be expensive, and the records concerned are unlikely to be wanted by anyone after the contract has ended.
Accidental Loss	Failure to capture a record in a recordkeeping system leading to compliance breaches with regulations that require the record to be registered.	Removing the source of the risk	Software is implemented that requires all documents to be captured into the electronic document and records management system at the time of the document’s creation.
	Failure to save a record to the correct drive leading to non compliance with business requirements due to the inability to locate the record required.	Changing the likelihood of the risk	A policy is introduced requiring all agency employees to undergo mandatory training in classification and filing procedures so that they are aware of where to file records.

Risk Category	*Risk*	*Treatment Option*	*Description*
	Failure to pass on critical business knowledge when staff members leave leading to the inability for the agency to explain why a particular course of action was taken.	Changing the consequences of the risk	Information vital for the continuing operations of the agency, including key processes and procedures, is documented and captured in the corporate recordkeeping system.
Environmental Damage	Flooding of the basement after torrential rain leading to the impairment of operations due to client files being reduced to a pulp.	Sharing the risk	Storage of records is outsourced to an approved public record office storage supplier.
	Bush fire totally destroys the main storage repository for agency records leading to impairment of agency operations and the death of the repository manager.	Retaining the risk	The agency has a disaster preparedness plan in place, agency records are stored in a space that meets fire safety requirements, and a state of the art sprinkler system is in place. The agency therefore decides to take no further action.
	Infestation of pests (including tiger snakes) in the storage area leading to the hospitalisation and near death of a registry officer, destruction of paper files, and damage to the wiring of a key server..	Avoiding the risk	The agency routinely monitors its storage areas to ensure that there is no pest or rodent infestation. If the presence of rodents or other pests are detected, the agency has procedures regarding their immediate identification and elimination.
	Decreases in oxygen caused by pollution in a storage area leading to the death of a repository worker.	Taking the risk	The agency determines that the benefits of having office space and a storage area within the city's business district are more important than the potential effect this may have on agency records, or potential oxygen levels in the storage area.
Hardware Failure	The crash of a computer-server hard drive leading to financial loss due to work having to be duplicated.	Removing the source of the risk	The agency stores its electronic records in two locations (on two different servers) so that records may be recovered if one server crashes.
	Failure of the agency to back up computer systems leading to the loss of records required to address potential litigation as evidence of past actions.	Changing the likelihood of the risk	The agency installs a policy of routinely backing up all electronic files. It monitors backup systems and practices regularly to ensure that the backup systems in place work effectively.
	Failure to open old-format files as the system used was not backwards compatible leading to retention periods being compromised.	Changing the consequence of the risk	The agency saves all electronic corporate files in a long-term preservation format so that they remain readable and accessible over time.
Malicious Damage	Failure of the agency to prevent a database being hacked leading to the financial costs of the computer and security systems being reviewed, and deleted or adjusted data reclaimed.	Sharing the risk	The agency shares its information technology management with CenITex, a service shared across multiple departments. This provides an increased level of security, ability to track, and reverse the effects of people who hack into the agency's computer system.

Risk Category	*Risk*	*Treatment Option*	*Description*
	Terrorists destroying records central to the operations of key Victorian infrastructure leading to multiple deaths of the public and political embarrassment.	Retaining the risk	The agency reviews its procedures for handling potential terrorist threats, including the identification of and security provided to vital records. The result of the review is that the agency is satisfied it is already doing all it can to limit the risk regarding possible terrorist threats.
	Recently fired employee changes the passwords of a crucial database before leaving to hamper agency operations leading to the cost of retrieving the passwords.	Avoiding the risk	System security is improved to ensure that any changes to key databases are logged, and the systems administrator is provided with the ability to adjust passwords to databases, should they be password protected.
Theft	Failure to prevent office files from being stolen leading to the inability to supply records to support key decisions or actions when required.	Taking the risk	The agency regards the likelihood of anyone stealing office files as being too low to worry about.
	Failure to prevent agency personnel 'rescuing' records of potential historical value leading to breaches of the Public Records Act 1973.	Removing the source of the risk	Records identified as being of historical value are transferred to Public Record Office Victoria (if they have been identified as a state archive) or offered to a Place of Deposit (if identified as having temporary value and they have passed their retention period).
	Failure to prevent agency personnel from taking work files home and not returning them leading to accusations of negligence and breaches of confidentiality.	Changing the likelihood of the risk	The agency introduces a policy whereby original work files are not to be taken home. If employees are to work from home they are either provided with remote access and save all files to the corporate drive, or are required to follow strict procedures regarding what may be taken and the measures to ensure the security and safe return of the documents.

Table 7: Examples of Treatment Options

4.5.2. Assessing Treatment Options

Determining which option would provide the best treatment for each risk will be based on the information gathered at steps one to four.

High level risks may require active treatment, such as changing the likelihood of the risk, changing the source of the risk, or changing the consequence of the risk. Active treatments will involve some level of work, such as the revision of procedures, creation of tools, and so on.

Low level risks may be treated more passively, such as the risk being accepted, or retained. The work required to treat these risks may have already been completed as part of the risk assessment itself. For example, practice and procedure may have been reviewed, the risks assessed and a decision made that current practice and procedure is sufficient considering the low level of risk involved.

Assessing the risk involves considering the information gathered about the risk and making a decision about the level of work that should be assigned to treat it. Some risks will require considerable effort and resources to address. If the risk is considered to be low, it will be more difficult to obtain the resources necessary to address it. In some cases, it will not be worth the effort to address the risk at this point in time.

The treatment options and actions to be taken as a result are usually recorded in a risk treatment plan.

4.5.3. Treatment Plans

Treatment plans document the risk, the identified treatment option, and the actions taken to address each risk. The treatment plan will be more effective if it corresponds with or is included in the agency's records management programme. For example, the treatment plan may be included in the records management strategy if it requires the development and implementation of processes or services and it fits within the objectives of the strategy. That way, the treatment of recordkeeping risk is included in the work planning, budget, and resources of the records management unit.

All treatment actions outlined in the treatment plan should be compared so that duplicated actions can be prevented and maximum use made of resources and controls required.

Example Risk:

The risk manager reviewed the treatment options available and recommended to the senior management team to implement option (c): do not renovate the basement, but move the records to a higher shelf and inform staff to leave the bottom two shelves empty. The risk manager then drafted a plan in collaboration with the facilities, records management and communications areas to implement the treatment selected within three months.

- The records management unit will outline how records should be redistributed;
- The facilities unit will organise a move of the records in line with the needs of the records management unit;
- The communications unit will work with the records management unit to develop a message that will inform staff of the changes and the reasons for the change;
- The records management unit will update procedures to ensure no records are stored on the bottom two shelves of the basement; and
- The records management unit will revise and update the training material and give staff a refresher on how to manage and store records.

4.6. Step Six – Reviewing & Monitoring

An assessment framework for recordkeeping risks should include:

- A method for regularly monitoring the progress of risks being treated; and
- The means to continually review recordkeeping practice and the records management programme for potential additional recordkeeping risks.

Recordkeeping risks need to be monitored and reviewed regularly to ensure that changing circumstances do not alter risk priorities or risk mitigation. The context for recordkeeping risks will change as identified risks are treated, and controls are improved or developed and implemented.

Review and monitoring methods will include:

- Continuous checking and monitoring of current and possible future recordkeeping risk as part of ongoing records management operations.
- Self-assessment and internal audits to identify and report risks associated with recordkeeping practice and the implementation of the records management programme.
- External audits (such as those conducted by the Ombudsman, the Auditor-General, the Privacy Commissioner, or the Health Commissioner) that identify or suggest recordkeeping risks.
- To assist with identifying which aspects of records management may be at risk in the agency, a short self assessment has been developed (see Appendix 4). This assessment will provide a quick indication of the general area (such as disposal, storage, or capture, for example) that may be at risk. The assessment is divided into seven segments that correspond with the seven Standards developed by PROV.

Guidance on what activities may be conducted to help mitigate the risks associated with each Standard may be found in the documentation associated with each Standard.

Ongoing monitoring and review of recordkeeping risks may include the following actions:

- Implementation of triggers to review the legislative, regulatory, and business environment for recordkeeping.
- Regular engagement with key stakeholder groups, including the risk management team.
- Regular inspection of practice, especially if recordkeeping risks are associated with activities undertaken by external parties, such as a service provider, or are location based, such as a storage facility.
- Review of the risk management framework for identifying, assessing and treating recordkeeping risks when the records management strategy is reviewed.
- Including the means to identify potential recordkeeping risks during self-assessments and internal audits of recordkeeping practice within the agency.
- Including the following in records management reporting processes:
    - Reporting of recordkeeping risks identified to the executive;
    - Recording recordkeeping risks identified in the agency risk register; and
    - Regular reporting on the status of recordkeeping risks being treated to relevant stakeholders.

If an identified risk turns into an event that happens, the event should be reviewed by the risk owner (i.e. business unit manager) and focussed on:

- What led to the risk occurring;
- Whether there were warning signs that could be anticipated in order to prevent the event occurring again; and
- An assessment of the ratings previously applied to the risk.

The findings of the review may be incorporated into the framework for managing risk. This may include:

- Revision of the risk categories;
- Revision of the risk ratings;
- Adjustment of treatment options;
- Upgrade of systems and reporting mechanisms;
- New or updated procedures and processes; or
- Revision of the recordkeeping environment.

Example Risk:

- The treatment plan was implemented and all staff received training about the changes. Further, in their fortnightly team meeting, each manager confirmed with their staff that they had attended the training and understood the changes that took place.
- To ensure that putting the records on a higher shelf does not negatively affect productivity, staff were asked through a survey if they found it more difficult than before to access the information they need to perform their job.
- Organisational health and safety checks were also conducted to make sure placing the records on a higher shelf did not cause an added risk of injury to staff.
- However, through a yearly building inspection, an external building contractor found cracks in the building foundation which increases the risk of insects entering the basement and damage the records, a risk aggravated by a particularly dry season. The building contractor then writes a report to the facilities manager who asks the risk manager to add the new risk to the risk register and inform the risk committee. The agency now needs to go through each step of the risk assessment program to determine how to treat the risk and make a recommendation to the executive team.

5. References

Government of Western Australia 1999, *Guidelines for Managing Risk in the Western Australian Public Sector*, Government of Western Australia, Perth, viewed 15 January 2010, <http://www.rdec.gov.tw/DO/DownloadControllerNDO.asp?CuAttachID=17523>.

Territory Records Office 2008, *Guideline for Records Management: Number 8—Business Continuity and Records Management*, Australian Capital Territory, Territory Records Office, Canberra, viewed on 13 January 2010, <http://www.territoryrecords.act.gov.au/__data/assets/pdf_file/0019/122653/Guideline_8_Business_Continuity.pdf>.

State Records Authority of New South Wales 2002, *Guideline 5—Guidelines on Counter Disaster Strategies for Records and Recordkeeping Systems*, Government of New South Wales, State Records Authority of New South Wales, Sydney, viewed on 13 January 2010, <http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/guidelines/files/Guideline%205%20Counter%20Disasters%20Strategies.pdf>.

National Archives of Australia 2001, *DIRKS—A Strategic Approach to Managing Business Information. Appendix 11—Risk Analysis in DIRKS*, Commonwealth of Australia, National Archives of Australia, Canberra, viewed on 15 January 2010, <http://www.naa.gov.au/images/dirks_a11_risk_tcm2-939.pdf>.

Centers for Medicare & Medicaid Services (CMS) 2002, *CMS Information Security Risk Assessment (RA) Methodology*, United States Government, Department of Health & Human Services, Baltimore, Maryland, United States, viewed on 15 January 2010, <http://www.training-hipaa.net/hipaa_resources/RA_meth.pdf>.

Victorian Auditor-General's Office 2004, *Good Practice Guide. Managing risk across the public sector*, State of Victoria, Victorian Auditor-General's Office, Melbourne, viewed on 15 January 2010, < http://download.audit.vic.gov.au/files/Risk_guide.pdf>.

Department of Treasury & Finance, *Victorian Risk Management Framework*, State of Victoria, Department of Treasury & Finance, Melbourne, viewed on 3 February 2010, http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/VicGovtRiskMgmtFramework/$File/VicGovt%20Risk%20Mgmt%20Framework.pdf>.

Department of Treasury & Finance, *Insurance Management Policy & Guidelines for General Government Sector*, State of Victoria, Department of Treasury & Finance, viewed on 3 February 2010, <http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/InsuranceManagementGuidelines/$File/InsuranceManagementGuidelines.pdf>.

Victorian Managed Insurance Authority, 2008, *Guide to developing and implementing your risk management framework*, State of Victoria, Victorian Managed Insurance Authority, viewed on 3 February 2010, <http://www.vmia.vic.gov.au/skillsEDIT/clientuploads/48/VMIA_Risk%20Management%20Guide_1%20July%202008_1.pdf>.

Legislation

Financial Management Act 2004 (Vic)

Public Records Act 1973 (Vic)

All current Victorian legislation is available at http://www.legislation.vic.gov.au

Standards

Standards Australia/Standards New Zealand 2009, *AS/NZS ISO 31000: 2009, Risk Management—Principles and guidelines*, Standards Australia/Standards New Zealand, Sydney.

Standards Australia/Standards New Zealand 2004, *AS/NZS 436: 2004, Risk Management* (the Standard), Standards Australia/Standards New Zealand, Sydney.

Standards Australia/Standards New Zealand 2004, *AS/NZS 4360: 2004, Risk Management Guidelines. Companion to AS/NZS 4360: 2004*, Standards Australia/Standards New Zealand, Sydney.

Internal Organization for Standardization/International Electrotechnical Commission 2009, *IEC/ISO 31010, Risk management—Risk assessment techniques*, International Electrotechnical Commission, Geneva, Switzerland.

State Records Authority of New South Wales 2002, *Standard on counter disaster strategies for records and recordkeeping systems*, State of New South Wales, State Records Authority of New South Wales, Sydney, viewed on 13 January 2010, <http://www.records.nsw.gov.au/documents/recordkeeping-standards/Standard%20No%20%206%20-%20Disaster.pdf>

Territory Records Office 2008, *Standard for Records Management Number 8—Business continuity and records management*, Australian Capital Territory, Territory Records Office, Canberra, viewed on 13 January 2010, <http://www.legislation.act.gov.au/ni/2008-438/notification.asp>.

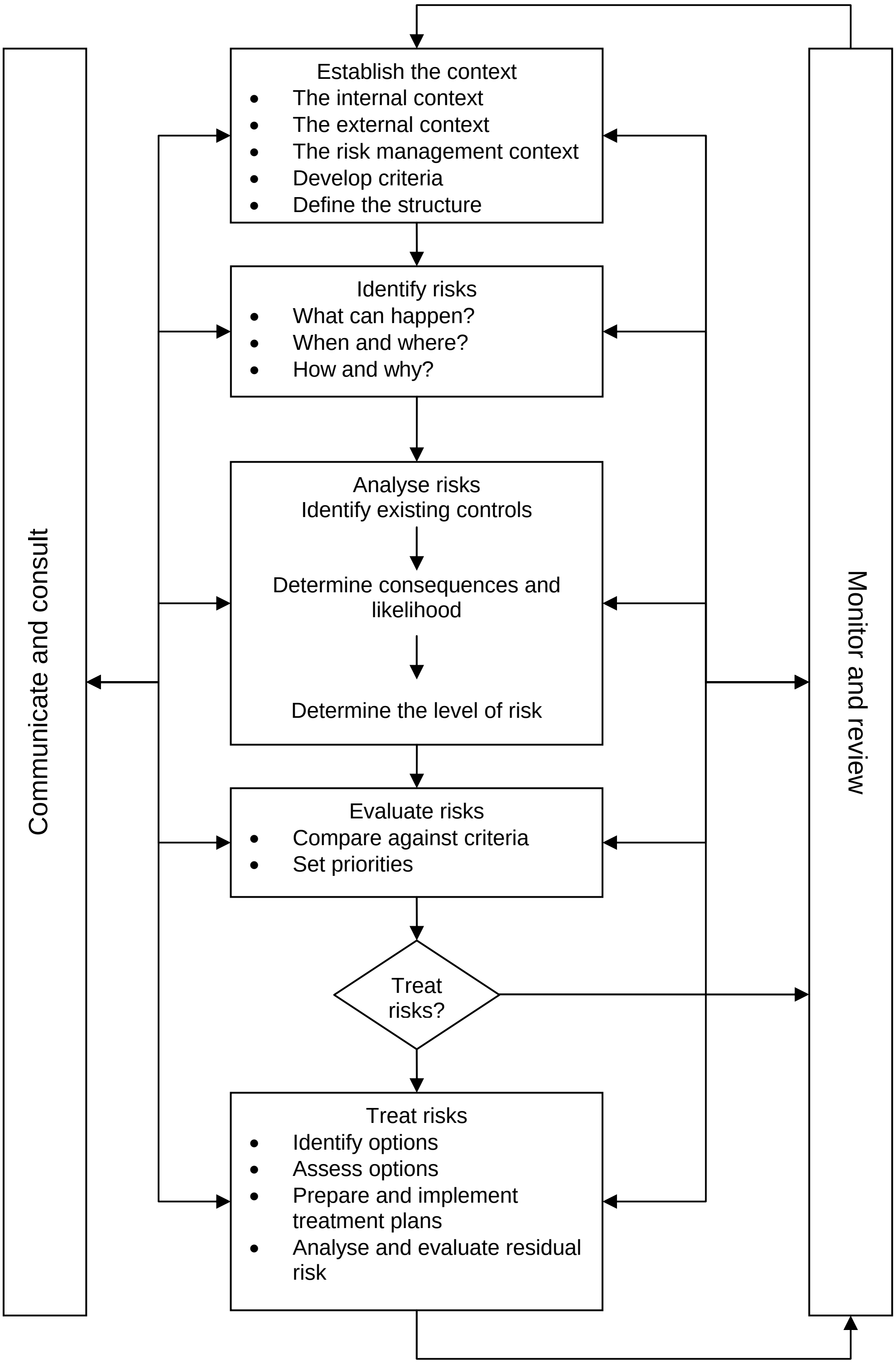
The National Archives, *The National Archives Report, Prompt Sheet 1—Strategic Assessment*, The National Archives, United Kingdom, viewed on 13 January 2010, http://www.nationalarchives.gov.uk/documents/assessments-part1.pdf>.

Other Resources

For more information about risk and records management, please contact:

Standards and Assessment
Public Record Office Victoria
Ph: (03) 9348 5600
Fax: (03) 9348 5656
Email: ask.prov@prov.vic.gov.au
Web: www.prov.vic.gov.au

Appendix 1: Risk Management Process Chart[11]



[11] Standards Australia, *AS/NZ 4360 – Risk Management* Standards Australia, Sydney, 2004

Appendix 2: Risk Register

Function/ Activity:		Compiled by:		Date:	
Date of risk review:		Reviewed by:		Date:	

Risk Category	*Risk*	*Consequence*	*Current Control*	*Consequence rating*	*Likelihood rating*	*Level of risk*	*Risk priority*	*Treatment Option*	*Treatment*
Unauthorised Disclosure									
Unauthorised Destruction									
Unauthorised Modification									
Accidental Loss									
Environmental Damage									

Risk Category	*Risk*	*Consequence*	*Current Control*	*Consequence rating*	*Likelihood rating*	*Level of risk*	*Risk priority*	*Treatment Option*	*Treatment*
Hardware Failure									
Malicious Damage									
Theft									

Appendix 3: Glossary[12]

Consequence: Outcome or impact of an event and may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequence can be positive or negative.

Control: Measure to modify risk. Controls are the result of risk treatment. Controls include any policy, process, device, practice or other actions designed to modify risk (ISO 31000).

Event: The occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.

Likelihood: General description of probability or frequency. It can be expressed qualitatively or quantitatively.

Loss: Any negative consequence or adverse effect, financial or otherwise.

Residual risk: Risk remaining after implementation of risk treatment.

Risk: Refers to the chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and their likelihood.

Risk acceptance: Informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risks accepted are subject to monitoring and review (ISO 31000).

Risk analysis: The systematic process to understand the nature of and to deduce the level of risk. It provides the basis for risk evaluation and decisions about risk treatment.

Risk appetite: Amount and type of risk an organisation is prepared to pursue or take (ISO 31000).

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk avoidance: A decision not to become involved in, or to withdraw from, a risk situation.

Risk criteria: Terms of reference by which the significance of risk is assessed. Risk criteria can include associated cost and benefits, legal and statutory requirements, socioeconomic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

Risk evaluation: Process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatment.

Risk identification: The process of determining what, where, when, why and how something could happen.

[12] This glossary is an abridged version of Victorian Managed Insurance Authority (WMIA) definitions for commonly used risk management terminology.

Risk management: Is the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.

Risk management framework: Set of elements of an organisation's management system concerned with managing risk. Management system elements can include strategic planning, decision-making, and other strategies, processes and practices.

Risk mitigation: Measures taken to reduce an undesired consequence (ISO 31000).

Risk register: A risk register is a comprehensive record of risks across an organisation, business unit or project depending on the purpose/context of the register (VAGO).

Risk treatment: The process of selection and implementation of measures to modify risk. The term 'risk treatment' is sometimes used for the measures themselves. Risk treatment measures can include avoiding, modifying, sharing or retaining risk.

Victorian Government Risk Management Framework (VGRMF): Guidance document released by the DTF in July 2007, which "has been developed to support good practice in Public Sector risk management. Specifically the framework provides for a minimum common risk management standard for public sector entities and attestations by accountable officers that risk management processes are consistent with that standard in annual reports".

Appendix 4: Risk Assessment: Self Assessment

The assessment is divided into seven segments. Each segment corresponds with a suite of PROV recordkeeping Standards, Specifications and Guidelines. The current controls listed are records management activities and services that form part of an agency's records management programme. Where a tick appears in the column for a specific current control, it is expected that the agency will have developed and implemented the activity or service listed. The assessment is intended to act as a guide to enable agencies to identify which areas of records management will most likely be at risk.

			Current Controls							
No.	*Statements (Yes / No)*	*Points (Circle if Yes)*	*RM Strategy*	*RM Policy*	*RM Procedures*	*RM Systems*	*Programme*	*Plan / Scheme*	*Communication*	*Assessment*
Strategic Management										
1.1	The records management function is not strategically planned	0								
1.2	There are some procedures that govern records management, and some systems for managing records, but not all areas of the agency are covered and they do not cover the entire records management process.	1			✓	✓				
1.3	There is an agency-wide process for managing records, but the process operates in isolation from the agency's strategic direction	2		✓	✓	✓		✓		
1.4	Records management was strategically planned but it has not been reviewed or updated since it was issued.	3	✓	✓	✓	✓	✓	✓		
1.5	Records management is strategically planned across the agency for all records in all systems, and the records management programme is regularly assessed for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Operations Management										
2.1	Records management operations are ad hoc, or do not occur at all	0								
2.2	There are some procedures that govern records management, and some systems for managing records, but not all areas or records of the agency are covered and they do not cover the entire records management process.	1			✓	✓				
2.3	There is an agency wide process for managing records, but that process has not been implemented and communicated across the agency	2			✓	✓		✓		
2.4	There is an agency wide process for managing records, which includes communication and training for all agency staff on recordkeeping practice	3			✓	✓	✓	✓	✓	

No.	Statements (Yes / No)	Points (Circle if Yes)	Current Controls							
			RM Strategy	RM Policy	RM Procedures	RM Systems	Programme	Plan / Scheme	Communication	Assessment
2.5	Strategic planning of records management has been translated across into operational plans, and systems, training has been implemented, and operations are regularly assessed for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Capture										
3.1	Records are not systematically identified and captured into recordkeeping systems	0								
3.2	Some records are captured into recordkeeping systems, but there is no scheme in place to identify and capture all records that an agency should create and capture into recordkeeping systems to meet legislative, regulatory and business requirements	1			✓	✓				
3.3	There is a process in place to capture all identified corporate records into a recordkeeping system, but not all agency corporate records have been identified	2			✓	✓		✓		
3.4	There is a process in place to capture all identified corporate records into recordkeeping systems, and procedures in place for managing records captured in systems that do not have recordkeeping functionality	3		✓	✓	✓	✓	✓	✓	
3.5	All agency records are identified, created, and are either captured into corporate recordkeeping systems or are managed by recordkeeping procedures and schemes, which are regularly assessed for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Control										
4.1	There are no recordkeeping controls in place at all	0								
4.2	Some recordkeeping controls are in place to classify and file records	1			✓			✓		
4.3	Recordkeeping controls in place cover all agency corporate records and records in all formats	2			✓	✓		✓	✓	
4.4	Recordkeeping controls in place cover all corporate records in all formats, and include file tracking as well as the classification and naming of records	3		✓	✓	✓	✓	✓	✓	
4.5	Recordkeeping controls are in place covering all corporate records in all systems and all formats, and controls are regularly upgraded and assessed for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Access										
5.1	There are no access provisions assigned to agency records at all	0								
5.2	A policy has been issued to direct action regarding access provisions for agency records	1		✓						
5.3	A policy, supported by procedures, has been implemented and communicated through the agency regarding access provisions for agency records	2		✓	✓				✓	
5.4	Access provisions are implemented directly into business and recordkeeping systems, as well as being directed by policy and procedures, to prevent unauthorised access to agency records	3		✓	✓	✓			✓	
5.5	All agency records and systems have access provisions to ensure that all agency records in all formats are protected from unauthorised access, and those provisions are assessed regularly for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Storage										
6.1	There are no provisions in place for storage of agency records	0								
6.2	The agency has a special room, space, or drive dedicated to the storage of corporate records	1			✓				✓	

			Current Controls							
No.	*Statements (Yes / No)*	*Points (Circle if Yes)*	*RM Strategy*	*RM Policy*	*RM Procedures*	*RM Systems*	*Programme*	*Plan / Scheme*	*Communication*	*Assessment*
6.3	The agency has a secure location for the storage of corporate records.	2		✓	✓	✓			✓	
6.4	The agency has a secure location for the storage of corporate records, and methods for the preservation of the records within storage including a disaster recovery or preparedness plan and / or a business continuity plan	3		✓	✓	✓		✓	✓	
6.5	The agency has a location and strategy for the secure storage, preservation and retrieval of records, including a disaster recovery and / or business continuity plan, which are assessed and inspected regularly for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓
Disposal										
7.1	There is no disposal coverage or disposal programme for agency records	0								
7.2	There is some disposal coverage for common administrative records, but no disposal programme	1			✓			✓		
7.3	There is a disposal coverage for common administrative records and agency specific records but no disposal programme	2			✓		✓	✓	✓	
7.4	There is a disposal programme and disposal coverage, but it is not regularly administered	3		✓	✓	✓	✓	✓	✓	
7.5	There is a disposal programme and disposal coverage for all agency records in all formats, which is regularly administered, and regularly assessed for improvement	4	✓	✓	✓	✓	✓	✓	✓	✓

Abbreviations / Terms Used

RM = Records Management

Corporate = Records of agency business, decisions and actions

Assessment Grid

The Recordkeeping Risk Assessment: Self Assessment grid (above) provides a quick spot check for the recordkeeping activities within an agency that might need further investigation. The list of controls provides anticipated activities or services that would be expected to be in place for the score provided (identified by a tick in the relevant box).

0 – 7	=	Red	=	High Risk
8 – 21	=	Yellow	=	Medium Risk
22 – 28	=	Green	=	Low Risk

Appendix 5: Risk Assessment Checklist

Step One: Establish Context

Question	*Yes*	*No*	*Unsure*	*Comments*
Is the agency currently complying with its legislative and regulatory requirements for recordkeeping?				
Does the agency understand its strategic imperatives regarding recordkeeping?				
Have the functions and activities that require records to be created and kept been identified?				
Does the agency create and keep the records identified as being required to cover its functions and activities?				
Is the agency sentencing its records in accordance with a current disposal authority (a Retention and Disposal Authority, Single Instance Disposal Authority, or in accordance with Normal Administrative Practice)?				
Is the agency disposing of its records appropriately?				
Is protection of records included in the agency's business continuity plans, disaster management plans, policies, and procedures?				
Are records management issues reported upon to the Executive Team and/or Senior Members of the agency?				
Have the existing controls for recordkeeping risks been identified?				
Is there an existing risk management framework that is used by the agency?				
Are records management policies, procedures and guidelines current and adhered to by all agency staff?				

Question	*Yes*	*No*	*Unsure*	*Comments*
Have all relevant stakeholders been identified and consulted regarding recordkeeping requirements, expectations and practice?				

Step Two: Identify Risks

Question	*Yes*	*No*	*Unsure*	*Comments*
Have risk categories been determined?				
Do the risk categories cover risk to all records in all formats?				
Have appropriate risk identification tools been identified and used?				
Have interviews with agency personnel and other relevant stakeholders been conducted?				
Have mechanisms for the continual identification of risk been developed and implemented?				
Have the recordkeeping risks been identified?				
Have the risks identified been described appropriately?				
Have the risks identified been recorded in the risk register?				

Step Three: Analyse Risks

Question	*Yes*	*No*	*Unsure*	*Comments*
Has sufficient information been gathered to analyse the identified recordkeeping risks?				
Have the consequences for each risk been described?				

Question	*Yes*	*No*	*Unsure*	*Comments*
Has a consequence table been determined?				
Has a likelihood table been determined?				
Has each risk been matched with a consequence rating?				
Has each risk been matched with a likelihood rating?				
Have the risk, consequence, consequence rating and likelihood rates been captured in the risk register?				

Step Four: Evaluate & Prioritise Risks

Question	*Yes*	*No*	*Unsure*	*Comments*
Has sufficient information been gathered to evaluate and prioritise the identified recordkeeping risks?				
Has a risk heat table to evaluate the level of risk been identified or developed?				
Have existing controls for the identified recordkeeping risks been taken into consideration				
Has the level of risk been determined for each risk?				
Has the level of risk been documented in the risk register?				
Have the risks been prioritised from high to low				

Step Five: Treat Risks

Question	*Yes*	*No*	*Unsure*	*Comments*
Have the risks been assessed to determine if they are acceptable or unacceptable?				
Have treatment options been identified for each risk?				
Have the treatment options been assessed to ensure that maximum use is made of the resources required?				
Have the treatment options been assessed to ensure the maximum use is made of the processes and services required to mitigate the identified recordkeeping risks				
Have treatment strategies been identified for each risk?				
Have the treatment options and strategies been captured in treatment plans?				
Has the information in the recordkeeping risk treatment plans been incorporated into the records management programme				

Step Six: Review & Monitor Risks

Question	*Yes*	*No*	*Unsure*	*Comments*
After testing the effectiveness of the risk treatment plan, does the risk require further treatment?				
After monitoring the utilisation of resources for the treatment of risks, is the need for resources greater for treating other risks?				
Are processes in place to continually monitor changes in risk levels (reflected in changes to risk ratings) over time?				
Have the stakeholders who need to be informed of the risk treatment process been identified and kept informed?				
Has the feedback received from stakeholders suggested who is responsible for risk treatments, what the timeframe for completion is likely to be, and what resources are available?				
Are the changes to risk ratings (risk levels) over time been communicated to stakeholders to determine further risk treatment decisions and identify successes in managing risk?				
Have internal audits or self-assessments of agency practice been regularly conducted to identify and report risk?				
Have routine operations been adjusted so that potential risks are determined and the progress of existing risk been reported?				