TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 60 Part One: Introduction to Risk Management processes

Introduction

Dealing systematically with possible risks, threats or disasters to records and information is an indispensable skill in the digital business environment.

This Advice is designed to give Records and Information Management (RIM) practitioners a practical grounding in risk management principles and an understanding of any existing risk frameworks in your agency.

Advice 60 Part Two - Applying Risk Management Processes builds on your knowledge in preparation for applying risk management processes, and Part Three includes risk analysis tools and an Information Risk Register template.

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

Understanding Risk Management in your agency

Records and Information Management (RIM) practitioners are encouraged to perform risk assessments in order to identify potential risks to agency records and information assets, and to put in place strategies to mitigate those risks.

The risk management process may be applied agency-wide, to particular business units or only to certain projects or activities. Your agency will already have processes in place to identify and manage risks. This Advice will assist you to adapt existing agency risk management processes to best fit your needs, rather than adopting a generic framework from elsewhere that may not be appropriate to your specific business environment.

Your agency's existing risk management frameworks may include:

- Work Health and Safety Risk
- Business Continuity and Disaster Preparedness Planning
- Environmental Risk Management
- Project Risk Management
- Strategic Risk Management (sometimes referred to as Corporate Risk)

"Organisations have historically managed various types of risk in silos, typically known by the name of the silo. Common examples are health and safety (which is concerned with managing risk related to personal injury and health), environment (which is concerned with managing environment-related risk) and continuity management (which is concerned with disruption-related risk). It is not unusual that these silos have adopted a distinctive vocabulary, in some cases being derived from relevant legislation. Nevertheless, all such specialist functions (or silos), whatever their name or descriptor, are specifically managing risk.".

SA/SNZ HB 436:2013 Risk Management guidelines - Companion to AS/NZS ISO 31000:2009

Getting familiar with your risk management framework

Risk management starts with developing a systematic process for thinking about risk. Once you have gained a practical grounding in risk management, it will be easier for you to establish repeatable processes to:

- Manage information risks
- Minimise the impact of risk on the agency's information assets, and
- Better handle the consequences if a risk event occurs.

Typically, the agency will have a steering committee and an officer who looks after the risk management function. It is important that you cultivate a relationship with those responsible for risk management in your agency. Your Risk Manager will be able to assist you in your efforts to align treatment of information risks with the strategic objectives of the agency, and help communicate and promote your efforts to a wider audience within the organisation.

Are you familiar with Risk Management processes?

At the end of this Advice (Appendix A) there is an exercise designed to familiarise you with the concepts.

Strategic risk management

To manage risks and take advantage of opportunities, which may be both internal and external, agencies are increasingly adopting a strategic risk management framework.

Most agencies will be required to identify and consider management of risks associated with their business and its operating environment. For example, the Department of Treasury and Finance's *Guidelines for Tasmanian Government Business* recommends that Government Business Enterprises and State-owned Companies establish a system of risk management and internal control and publish those details in their Corporate Plan. (See Department of Treasury and Finance - *Guidelines for Tasmanian Government Businesses: Corporate Governance Principles,* 2008.) [1]

Elements of a solid risk management framework will include strategic planning, compliance monitoring and internal audit programs, supported by the agency's executive. In addition to assisting staff in their day-to-day

[1] http://www.treasury.tas.gov.au/domino/dtf/dtf.nsf/LookupFiles/Corporate-Governance-Principles.pdf/$file/Corporate-Governance-Principles.pdf

decision-making, risk management processes can also bring a strategic and comprehensive focus to addressing key risks that require sustained attention by senior management.

Exercise - Understanding your agency's risk management framework

A Strategic Risk Register is different from a Work Health and Safety Risk Register, which is for controlling health and safety hazards and risks in the workplace, or a Project Risk Register which manages risk associated with specific projects over the project lifetime. A Strategic Risk Register describes the main risks that the agency faces when doing business. This will be used by management or the agency's governing body as a governance tool to prioritise areas for treatment and action. It is also used as a basis for reporting risks in the Annual Report.

This exercise is designed to give you a practical understanding of how your agency manages risk at an enterprise level. You will research your agency's existing risk management framework, from which you will identify key information risks to carry out your own risk analysis (See Part Two of this Advice, *Applying Risk Management Processes*). The key document for this activity is your agency's Strategic Risk Register.

1) Locate the Strategic Risk Register, which may be included in your agency's Corporate Plan. If this is not available, obtain a Risk Register from your agency's Risk Manager that has been developed for a past project or business unit.
2) From the register, identify the agency's high risk business activities. These risks will be rated highest on the register, or perhaps have consequence ratings of 'Major'.
3) Find out how these particular risks are included on the corporate Strategic Risk Register. Questions you might ask are:
    - What is the process for strategic risk analysis and who manages it?
    - Does the agency have an Audit Committee or Risk Management Steering Committee who maintains the Risk Register?
    - Is there a designated Risk Officer in the agency, or someone with risk management responsibilities?
    - Does the agency undertake risk assessments and where is this documentation kept?
    - Does the agency conduct internal audits to assess and monitor high-risk business activities?
4) Identify any risks on the corporate register that relate to records. They may not specifically address recordkeeping, but may refer to corporate information systems or data, for example: "Non-compliance with record-keeping legislation and standards" or "Hacking/altering of data" or "Failure of corporate business systems". If there are no records-related risks on the register, questions to consider include:
    - What records-related risks might you expect to see, given your knowledge of the business?
    - Were Records Officers or RIM experts invited to contribute to the development of the Strategic Risk Register?
    - Do the risk analysis tools (criteria, scales, etc.) used by the agency include methods for assessing records and information risk?
5) From the register, identify key stakeholders or business owners who are responsible for high-risk areas of the agency. Make an appointment with then to discuss their risks, bringing your own RIM perspective. Questions you might ask:

- What problems have they experienced that involve data, records, information or documentation?
- What evidence do they need to provide for compliance purposes in their business area?
- On prior projects, what issues around documentation have come up, maybe more than once?

6) Based on your interviews, compose your own personal list of the **top five** information risks in the agency, and the **top five** risks to records in your agency's recordkeeping systems (eg. TRIM or other EDRMS).

This activity may well have stimulated your thinking about risks to other areas in the agency that you are responsible for, such as records storage areas and recordkeeping systems. If you do not already have one in place, this is where developing an appropriate disaster management plan would assist.

Disaster management and business continuity risk

Disaster management for records and recordkeeping systems should take place within the framework of the agency's Business Continuity Plan, and in conjunction with staff responsible for risk management.

However, if records related risks have been neglected in the broader Business Continuity and Risk Management plans of the organisation, Disaster Management plans and/or Disaster Recovery manuals and 'disaster kits' developed by Records staff can help.

Development of a robust Disaster Management Plan requires the following:

1) Identification and assessment of risks affecting records and recordkeeping systems, and the subsequent activities to reduce the probability of a disaster, and reducing the probability of loss should a disaster occur
2) Planning activities to establish a counter disaster plan to assist staff to respond to an emergency event
3) Activities to identify and protect vital records
4) Response and recovery – the activities involved in implementing the plan and initiating resources to protect or secure the organisation from loss; and restoring records and operations to 'business as usual' status.

For more identification and assessment of risks affecting records and recordkeeping systems for your Disaster Management Plan, see Tasmanian Archives and Heritage Office (TAHO) *Advice 26 Disaster Preparedness and Recovery.* For more on vital records, see *Advice 52 Identifying and managing Vital Records*.

Systematically managing information risk

Risk management starts with developing a systematic process for thinking about risk. Once you have gained a practical grounding in risk management, it will be easier to establish repeatable processes to manage information risks, to minimise the impact of risk on the agency's information assets and to better handle the consequences. By identifying possible problems or disasters before they happen, you are helping to protect the agency, staff, stakeholders, the community and ultimately, protecting yourself.

It may at first feel like a daunting task to introduce a whole new process to your workload; however it is likely that your agency already has a strategic risk management strategy or program in place. It is much easier to build

on this existing framework, and adapt it to manage information risks, than to start entirely from scratch. Part Two of this Advice, *Applying Risk Management Processes* will describe this process in more detail.

Recommended Reading

Tasmanian Government Project Management Guidelines (V7.0) [2] and associated Toolkit [3]

Australian Standard for Risk Management AS/NZ ISO 31000:2009

TAHO, Disaster Preparedness and Recovery (2012: Advice 26)

WorkSafe Tasmania, Resources [4]

WorkSafe Tasmania. Publications [5]

[2] http://www.egovernment.tas.gov.au/project_management/tasmanian_government_project_management_guidelines
[3] http://www.egovernment.tas.gov.au/project_management/supporting_resources/toolkit/risk_management
[4] http://worksafe.tas.gov.au/resources
[5] http://worksafe.tas.gov.au/resources/publications

Further Advice

For more detailed advice, please contact:

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

Acknowledgements

- Tasmanian Department of Treasury and Finance, *Guidelines for Tasmanian Government Businesses: Corporate Governance Principles* (October 2008) [6]
- National Archives Australia (NAA), *Advice on Managing Recordkeeping Risks* [7]
- WorkCover NSW, *Small Business Safety Checklist: Checking out your workplace* (2003) [8]

Information Security Classification

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

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	May 2015	Christine Woods	Template	All
1.0	02-09-2014	Samara McIlroy	Initial Release	All

Amendments in this Release

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

Issued: September 2014

Ross Latham
State Archivist

[6] http://www.treasury.tas.gov.au/domino/dtf/dtf.nsf/LookupFiles/Governance-Framework-Guide.pdf/$file/Governance-Framework-Guide.pdf
[7] http://www.naa.gov.au/records-management/strategic-information/linking/Recordkeepingrisks.aspx
[8] http://www.workcover.nsw.gov.au/print-guide?source=20233

APPENDIX A

Work Health and Safety Risk

If you are unfamiliar with risk management processes, and feel that you need a more practical grounding in the principles before tackling information risks, start by familiarising yourself with your agency's health and safety risk framework.

If you have never done a workplace inspection before, conduct an inspection of your immediate work area to identify any safety problems. Any observations you make during the inspection should be recorded directly onto a risk register, as this will provide a valuable reference source for future inspections. Keeping a risk register will help you monitor any safety risks in your work area and take appropriate actions to make your workplace safer. You may want to use the following list as a guide:

Category	**Examples**
Work Environment and Layout	• Adequately lit work areas • No direct or reflected glare on screens • Temperature is comfortable • Noise level is acceptable • Ventilation is adequate • Well-stocked first aid kit is accessible nearby • Work health and safety information is displayed and up-to-date • Walkways are unobstructed and clearly marked • Adequate storage and tidy areas • Floor surfaces are even and in good condition
Emergency procedures	• Nominated person responsible for evacuation • Emergency procedures are clearly posted • Fire extinguishers easily located and recently checked • Alarm can be heard • Fire exits are clear • Emergency lighting/signage is operational • Evacuation route and assembly place is identified
Electrical	• No damage to sockets, plugs, leads and switches • No loose or exposed leads on the floor' • Current tag testing
Manual handling	• Items in frequent use are within easy access between knee and shoulder • Work benches and chairs adjusted to appropriate heights • Heavy items stored at appropriate height' • Stepladders available to access items on high shelves • Trolleys available for heavy loads • Staff are aware, trained and follow Manual Handling Procedures • Repetitive tasks are identified and appropriately managed