Information Management Advice 60 Part Three: Information Risk Register Template

Introduction

This Information Risk Register template has been provided for agencies to manage agency information risks. Guideline 1 - Records Management Principles includes a requirement for agencies to undertake risk analysis (see Guideline 1 Principle 2: Govern Records). This template can be used as evidence that you have undertaken risk analysis of your recordkeeping and information risks. The Information Risk Register should be maintained and made available for inspection by TAHO staff as part of scheduled Recordkeeping Audits.

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

This Advice adapts the Risk Management methodology from the Tasmanian Government Project Management Guidelines (V7.0).[1] 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.

How to use the register

The risk scales, risk matrix and examples included here are a suggested starting point. Text enclosed in [square brackets] is provided as instruction and intended to be replaced.

At each annual review, add any new risks, and downgrade or upgrade existing ones. At the same time, review risk mitigation strategies and treatment options to see if they are working. The Register should be brief and to the point. It should be updated on a regular basis. The description of the risk should identify the consequences and/or impacts (where these are not obvious), as these can be useful when identifying appropriate mitigation actions. Treatment actions should include such things as:

- Preventative actions - planned actions to reduce the likelihood a risk will occur and/or reduce the seriousness should it occur. (What should you do now?)
- Contingency actions - planned actions to reduce the immediate seriousness of the risk when it does occur. (What should you do when?)
- Recovery actions - planned actions taken once a risk has occurred to allow you to move on. (What should you do after?)

[1] http://www.egovernment.tas.gov.au/project_management/tasmanian_government_project_management_guidelines

Example Consequence Scale

	Financial, Insurance	Personnel, OHS	Service Delivery, Operations	Compliance	Reputation, Political	Environment	Information
Minor	Minor impact on budget/ loss that can be replaced from budget Insurance up to $1m required.	Injury report and/or first aid only May include substantial stress but no lost time.	Work processes would be inefficient but decisions could still be made and actions taken.	Unlikely to result in adverse regulatory response or action.	No media attention Credibility may be questioned.	Minor damage to a localised area or that ceases once the event is over Environmental liability or remediation cost $0-50,000.	Loss of information or records of short-term administrative value (e.g. routine advice) Unauthorised access to UNCLASSIFIED & PUBLIC agency information.
Moderate	Serious impact on budget/ resource reallocation required Insurance between $1-5m required.	Medical treatment for Injury Substantial stress event requiring professional clinical support.	Service delivery interruptions of more than 24 hours.	Incident reportable to regulatory authorities with potential for formal notice or fine.	Local media coverage Senior management damage control required.	Measurable impairment on biological or physical environment Ecosystem will recover without intervention. Environmental liability or remediation cost $50,000-500,000	Loss of information or damage to records of moderate value (e.g. minor contracts or project records, or required for audit purposes) Unauthorised access to IN CONFIDENCE agency information.
Major	Critical impact on budget/ external recovery required Insurance between $5-20m required.	Hospital treatment for injury Serious temporary disability/ minor permanent disability.	Service delivery interruptions longer than 3 days but less than a month. Recovery would be expensive and time consuming.	Investigation, prosecution and major fine possible Actions or decisions cannot be explained to courts or regulatory bodies.	Significant media coverage Political embarrassment would occur. May jeopardise future funding.	Serious environmental effects Ecosystem will recover over time once clean-up has been completed. Environmental liability or remediation cost $0.5m - $5m	Loss of information or damage to records of high value records that relate to long term or ongoing rights, obligations and entitlements (e.g. employee health monitoring and incident management records) Unauthorised access to PROTECTED agency information.
Catastrophic	The agency would incur huge financial losses Insurance of more than $20m required.	Single death Permanent disabilities for multiple persons.	Agency operations would be rendered dysfunctional and not be able to recover from consequences.	May result in serious litigation including class actions.	National and international media coverage Total loss of confidence in agency.	Very serious environmental effects Remediation required. Environmental liability or remediation cost >$5m	Loss or irreparable damage to vital records essential for the ongoing business of an agency, and without which the agency could not operate effectively. Loss of information or irreparable damage to records of enduring value recognised by a broader audience than the original creating agency, including future generations (e.g. PERMANENT records) Unauthorised access to HIGHLY PROTECTED agency information

Adapted from University of Tasmania (UTAS) Risk Matrix (2012)

Example Risk Matrix

CONSEQUENCE / LIKELIHOOD	Minor	Moderate	Major	Catastrophic
Almost Certain Expected to happen/ commonly repeating/ occurs weekly	**MEDIUM**	**HIGH**	**HIGH**	**EXTREME**
Likely Will probably occur/ occurs monthly	**LOW**	**MEDIUM**	**HIGH**	**EXTREME**
Possible May happen at some time, say yearly/ has a one in twenty chance of occurring	**LOW**	**MEDIUM**	**MEDIUM**	**EXTREME**
Unlikely Little chance that this event could happen/ less than a 5% chance of occurring	**LOW**	**LOW**	**MEDIUM**	**HIGH**

Information Risk Register Template

Risk	Something which has the potential to threaten the agency	**Change**	Has the priority level of the risk changed since it was last addressed? * indicates that a new risk has been identified ↓ indicates that the risk has been decreased since the last assessment ↑ indicated that the risk has increased since the last assessment -- indicates no change
Cause	The trigger that causes the risk to occur (helps determine likelihood)	**Date of previous review**	This helps the reviewer understand the success (or failure) of any previous risk mitigation activities
Result or Impact	The effect the risk could have (helps determine consequence)	**Control**	Any existing Records Management controls
Likelihood	Probability that a threat will emerge or event will occur	**Cost/Resource**	Details of any specific resource requirements (and costs)
Consequence	The seriousness/impact if it does occur	**Treatment Actions**	Pre-emptive mitigation actions to reduce the risk level
Risk Level	The priority level of the risk based on the likelihood and consequence (risk matrix)	**Work plan**	Is treatment included in the Treatment Action Plan or the Records Management work plan?

ID	**Risk**	**Caused by**	**Result / Impact**	**Likelihood**	**Consequence**	**Risk Level**	**Change**	**Date of previous review**	**Control**	**Treatment Actions**	**Cost/ Resource**	**Work plan**
<#>	[Short statement that describes the risk]	[The trigger that causes the risk to occur]	[The effect the risk could have]	L	M	H	*	[Date of last review]	[Specify any existing Records Management controls]	[Planned mitigation strategies: Preventative (implement immediately) or contingency (implement if/when risk occurs).]	[Specify any costs or specific resourcing requirements]	[Specify responsibility and timeline for mitigation action(s) or if included in Work plans]

<Agency Name> Information Risk Register

ID	Risk	Caused by	Result / Impact	Likelihood	Consequence	Risk Level	Change	Date of previous review	Control	Treatment Options	Cost/ Resource	Work plan
1	[Agency records kept in multiple locations on shared drives and personal drives]	No business rules around document and version control]	[Agency copy of contract differs from the other party's version, causing increased legal fees, and possibility of losing case.]				*	[Never]	[Policy and Procedures Records Management System]	[Develop and implement policy and procedures around version control. Lock down share drives. Implement an EDRMS to will enforce version control.]	[TBC]	[Records Manager - by end 2014]
2	[Project records stored in cloud-based commercial applications are more likely to be subject to cyber-attack.]	[Agency has no control over other users or the types of information stored in the application.]>	[Application's developers accept no liability or responsibility for deleted, lost or corrupted data. Sensitive agency information will be made public]				*	[Never]	[Policy and procedures]	[Staff ordered to remove all business records from the application. IT staff regularly monitor use of the application and enforce this policy]>	[TBC]	[Records manager IT Manager - needs immediate implementation]
3	[Records storage not compliant with standards (Physical storage of State records Guideline 11)]	[Agency stores permanent records in shipping container in flood prone area.]	[Mould forms on records. Vital records are damaged. Mould spores cause illness of staff member with existing respiratory problems]				*	[Never]	[TBC]	[Purchase mould treatment equipment Move records to another storage with environmental controls in place Outsource to an approved records storage provider]	[Quote for mould treatment equipment to be obtained]	[Facilities Manager - action to be completed by July 2015]

ID	Risk	Caused by	Result / Impact	Likelihood	Consequence	Risk Level	Change	Date of previous review	Control	Treatment Options	Cost/ Resource	Work plan
4	[Information security models not applied to emails]	[Staff not trained to use information security classification scheme.]	[Sensitive information is leaked to the media, causing embarrassment and damage to agency's reputation.]				*	[Never]	[Communication & training]	[Induction includes awareness of information security and employee responsibilities regarding classification of information]	[TBC]	[Records Manager - by end November 2014]
5	[Legacy systems can't be switched off because the records in them cannot be legally disposed of]	[Critical recordkeeping metadata isn't identified in the migration process and doesn't get migrated over to new system]	[Agency incurs additional costs to keep legacy system operational. Records staff spend additional time carrying out legacy searches. Staff don't trust the data in the new system.]				*	[Never]	[Retention and Disposal Schedules]	[Implement retention and disposal schedule in system Engage database migration specialists before retiring legacy system.]	<TBC>	<Records Manager - commence R&DS development in next 3 months>