NSW GOVERNMENT | The Treasury

Risk Management Toolkit for NSW Public Sector Agencies

Volume 2: Templates, examples and case study

Policy & Guidelines

TPP12-03c

August 2012 © Crown Copyright 2012
NSW Treasury
ISBN 978-0-7313-3569-5

General inquiries concerning this document should be initially directed to the Financial Management and Accounting Policy Branch of NSW Treasury.

This publication can be accessed from the NSW Treasury website: www.treasury.nsw.gov.au.
NSW Treasury reference: TPP12-03c

Copyright Notice
In keeping with the Government's commitment to encourage the availability of information, NSW Treasury is pleased to allow the reproduction of material from this publication for personal, in-house or non-commercial use, on the condition that the source, publisher and authorship are appropriately acknowledged. All other rights are reserved.

If you wish to reproduce, alter, store or transmit material appearing in the *Risk Management Toolkit for NSW Public Sector Agencies* for any other purpose, a request for formal permission should be directed to:

Mark Pellowe
Senior Director, Financial Management and Accounting Policy Branch, NSW Treasury,
Level 24, Governor Macquarie Tower, 1 Farrer Place Sydney NSW 2000.

Preface

NSW Treasury has developed this *Risk Management Toolkit for NSW Public Sector Agencies* (the Toolkit) to provide a comprehensive reference to the current international risk management standard, ISO 31000.

The Toolkit contains guidelines, templates and a case study based on a hypothetical agency. It may be particularly useful for those agencies that are just embarking on the risk management journey.

The Toolkit consists of two volumes:

- Volume 1 – Guidance for Agencies
- Volume 2 – Templates, examples and case study (this volume).

These two volumes are complemented by an Executive Guide which provides a navigation aid to the detailed guidance in the Toolkit.

I encourage departments and statutory bodies to familiarise themselves with the content of this volume and make use of the templates as appropriate.

Philip Gaetjens
Secretary
NSW Treasury

Treasury Ref: **TPP12-03c**
ISBN: **978-0-7313-3569-5**

Contents

Introduction **1**

PART 1: Templates **2**
1. Consequence table 3
2. Likelihood table 4
3. Risk matrix 5
4. Source–Pathway–Target methodology 7
5a. Risk assessment (portrait version) 9
5b. Risk assessment (landscape version) 10
6a. Risk register (option 1) 11
6b. Risk register (option 2) 12
7. Monitoring significant risks 13
8. Sample risk report 14
9. Maturity rating for risk management performance 15
10. Capability matrix 18
11a. Stakeholder analysis and communication planning 20
11b. Stakeholder analysis matrix 21
11c. External and internal stakeholders 22
11d. Risk management communication needs analysis 23
11e. Risk management communication strategy 24

PART 2: Case study
Southland Department of Law Enforcement **25**
Southland DLE organisational chart 26
Southland DLE risk management implementation plan 2012–14 27
Southland DLE risk management policy 34
Southland DLE stakeholder analysis matrix 36
Southland DLE capability matrix 37
Southland DLE consequence table 39
Southland DLE consequence table – for threats 40
Southland DLE likelihood table 42
Southland DLE risk matrix 43
Southland DLE risk register 44
Southland DLE risk profiles 50
Southland DLE risk profiles 51
Southland DLE risk profiles 53

Introduction

The *Risk Management Toolkit for NSW Public Sector Agencies* (the Toolkit) consists of two volumes that are complemented by an Executive Guide which provides a navigation aid to the detailed guidance in the Toolkit. This document is Volume 2 of the Toolkit.

Volume 2 provides practical assistance for implementing the concepts discussed in Volume 1 of the Toolkit. The information contained in this volume is presented in two parts.

Part 1: Templates and examples
Templates and examples are provided as a guide to help you practically apply the concepts explained in *Risk Management Toolkit for NSW Public Sector Agencies: Volume 1 – Guidance for Agencies*. These templates and examples can be tailored to suit your business.

Part 2: Case study – Southland Department of Law Enforcement
In addition to the templates provided in Part 1 of this volume, a case study based on a hypothetical general government agency, the Southland Department of Law Enforcement, has been used as the basis for selected worked examples.

Section	Template or sample	Page	Southland DLE case study	Page
Risk management process				
Consequence table	X	3	X	39
Likelihood table	X	4	X	42
Risk matrix	X	5	X	43
Source–Pathway–Target methodology	X	7	X	
Risk assessment	X	9,10		
Risk register	X	11,12	X	44
Risk profiles				
Risks affecting strategic objectives			X	50
Heat maps			X	51
Monitoring significant risks	X	13		53
Sample risk report	X	14		
Risk management framework				
Risk management policy			X	34
Risk management implementation plan			X	27
Maturity rating for risk management performance	X	15		
Capability matrix	X	18	X	37
Stakeholder analysis and communication plan	X	20		
Stakeholder analysis matrix	X	21	X	36
Risk management communication needs analysis	X	23		
Risk management communication strategy	X	24		

Part 1: Templates

The following templates are provided to get you started in documenting your risk management activities. They are intended to help you develop your own versions.

It is not necessary to use all of these templates. When developing your risk management tools, you should tailor the templates you decide to use to the specific needs of your agency.

You are not required to use these exact templates; for example, you may already have your own templates that achieve a similar purpose. What is important is to tailor the templates to the needs of your stakeholders.

Many of the templates are also available in Excel format for download from the Risk Management Toolkit page of the NSW Treasury website at www.treasury.nsw.gov.au.

1. Consequence table

A consequence table is a matrix in which consequence levels are described for different types of consequences. The three main steps for creating a consequence table are:

Step 1: Identify types of consequences that should be included in your table

Identify all the types of consequences that will affect your agency's ability to achieve its objectives. Some common consequence types include financial, service delivery, work health and safety, stakeholder satisfaction, reputation and image.

Step 2: Determine how many levels of consequences you need in your table

Determine the number of levels required to describe the severity that you anticipate for the consequence types identified in step 1, as shown below:

Consequence levels	
Consequence level	**Consequence level description**
Very high	
High	
Medium	
Low	

Step 3: Describe each consequence level for each consequence type

An example of step 3 is shown in the following table.

Consequence table – threats					
Consequence type		**Consequence level**			
		Low	**Medium**	**High**	**Very high**
	Financial loss	Does not exceed 0.1% of budget	Greater than or equal to 0.1% but less than or equal to 0.5% of budget	Greater than or equal to 0.5% but less than or equal to 2% of budget	Exceeds 2% of budget
	Service delivery	Service failure across a single service group's services that can be managed within the service group	A significant disruption to business continuity across a single service group's service requiring resources from other areas of your agency	A major disruption to business continuity across multiple services that your agency provides	A significant disruption in business continuity across all major services your agency provides

You can use a similar template for both threats and opportunities (refer to Volume 1, Section 4.3.3).

2. Likelihood table

A likelihood table can be used to describe the levels of likelihood for risks.

The three main steps for creating a likelihood table are listed below.

Step 1: Determine how many levels of likelihood you need in your table

Define sufficient levels so that each risk can be assigned an appropriate likelihood rating.

Step 2: Decide how to describe the likelihood

There are various ways you can describe the likelihood; they include probability and/or indicative frequency.

Step 3: Describe the levels of likelihood in a table

Each level on the likelihood scale should be described so it is easily understood and unambiguous and can be clearly distinguished from the level above or below it.

Likelihood table		
Likelihood level	**Frequency**	**Probability**
Almost certain	The event is expected to occur: – in most circumstances – frequently during the year	More than 99%
Rare		

3. Risk matrix

A risk matrix may be used to determine the level of a single risk by combining its consequence and likelihood. Below is an example of a 4 x 4 matrix with three escalation points. This can be adapted to your needs – for example, you may choose to use a 5 x 5 matrix with four escalation points. Note that it is not necessary to have the same number of consequence and likelihood levels.

Likelihood level	Consequence level: Low	Medium	High	Very high
Almost certain	10	11	15	16
Likely	4	9	13	14
Possible	3	7	8	12
Rare	1	2	5	6

Risk levels	
12–16	Extreme
5–11	Moderate
1–4	Low

A similar matrix can also be used to plot multiple risks to create a risk profile, such as a heat map. Refer to the worked example in Part 2. Note that the example in the case study uses four levels, instead of the three risk levels suggested here.

When you are designing your risk matrix, risks (or opportunities) can be divided into those that require no further action, those that may require action and those that demand action. You can also align these risks with the escalation actions required (see below for an example where three escalation levels have been described).

Risk actions and escalation points			
Group	**Group description**	**Action required for risk**	**Risk escalation**
12–16	Red–Extreme	Action required: risks that cannot be accepted or tolerated and require treatment	Escalated to the Head of Authority and executive Control strategy developed and monitored by the Head of Authority or Executive
5–11	Yellow–Moderate	Potential action: risks that will be treated as long as the costs do not outweigh the benefits As Low As Reasonably Practicable (ALARP)*	Managed at functional or service group level Escalated to the relevant direct report to the Head of Authority for information
1–4	Green–Low	No action: acceptable risks requiring no further treatment May only require periodic monitoring	No action required Monitoring within the functional area or business unit

Risk tolerance table		
Group	**Threat**	**Opportunity**
Action required (12–16)	Unacceptable risks Threats that your agency **cannot tolerate** at their current levels because their consequences coupled with their likelihoods are unacceptably high	Opportunities whose positive consequences, coupled with their likelihoods, are so large that your agency **must pursue** them because it cannot afford to forgo the benefits associated with them
Potential action (5–11)	ALARP risks Threats that your agency is **prepared to tolerate** at their current levels if the costs associated with implementing additional control measures outweigh the associated benefits	Opportunities that your agency **may wish to pursue**, as the benefits outweigh the costs associated with implementing the strategies required to realise the opportunity
No action required (1–4)	Acceptable risks Threats that your agency **can accept** at their current levels after existing controls	Opportunities that your agency will **give a low priority to**, as the benefits are not sufficient to expend resources on pursuing

* Refer to ISO 31010.

4. Source–Pathway–Target methodology

One of many techniques that can be used to identify risks is the Source–Pathway–Target methodology. This methodology can help you determine what sources of risk and types of risks affect particular assets in your agency. The methodology is based on the premise that where there is a source of risk and an asset (target) that may be affected by that source of risk, then the pathway between them is a risk. To protect their assets, organisations need to provide barriers (risk controls) against sources of risk.

To identify your risks using this methodology, you need to follow the three-step process set out below. You can use the template on the next page.

Step 1: Identify sources of risk in your agency

The PESTLE (political, economic, social, technological, legal and environment) approach provides a useful starting point for identifying sources of strategic risk. (You can add to the list as necessary.)

The PESTLE model is appropriate for identifying strategic risks. However, it may be less suitable when identifying sources of, for example, operational risks. In this case, it may be more appropriate to use the SABRE (safety, asset, business output, reputation and environment) model.

Whichever model you choose, you should ensure that you still examine all sources of risk within the environment being assessed, from the perspective of all internal and external stakeholders.

Step 2: Identify your agency's assets

An agency's assets include, but are not necessarily limited to, the following:

- workforce
- hardware: infrastructure and equipment
- systems and processes
- data and information
- partnerships
- reputation.

Step 3: Identify each of your agency's objectives.

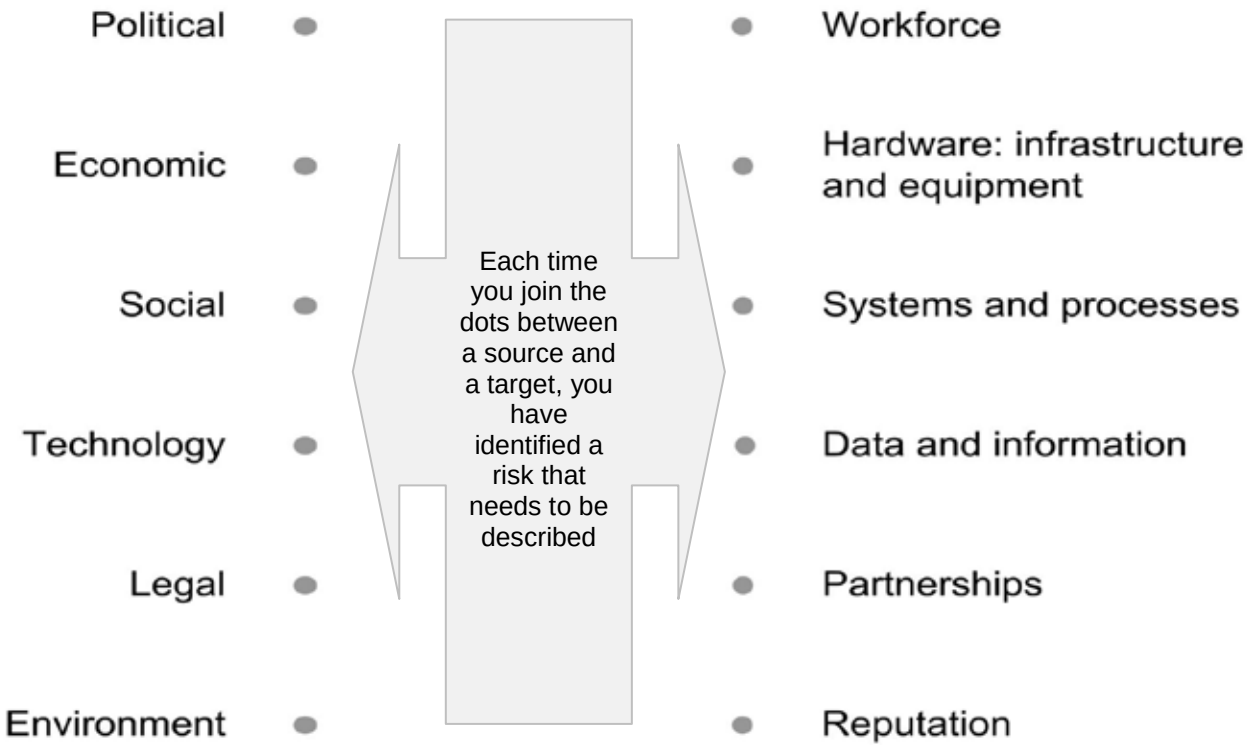
For each objective, identify connections between a source of risk and an asset. Describe each connection as a risk so that:

- the source, the event and the impact on your agency's objectives are consistently and clearly defined and differentiated
- those who were not involved in the assessment process can understand the risk.

You may wish to group risks into categories, such as financial, work health and safety, service interruption, community safety, stakeholder satisfaction and environmental impact.

Use a separate template for each objective being considered.

Agency objective: ……



5a. Risk assessment (portrait version)

All risk assessments should be clearly documented. You can use either Template 5a or Template 5b to document your assessment of a single risk at a divisional, operational or specific project level. Note that you should capture all your risks in your risk register (see Templates 6a and 6b)

Risk description Provide a brief description of the risk	**Objective(s) affected** Briefly list the objectives impacted by the risk	**Risk owner** Include name of the person managing the risk and the area of the agency he or she works in	**Stakeholders consulted** Include internal and external stakeholders

Worst case

Make an assessment of the risk based on the scenario where the current controls do not exist or completely fail. Refer to Template 5b for a risk ratings legend.

Consequence level Use your consequence table	**Likelihood level** Use your likelihood table	**Risk level** Use your risk matrix

Controls

List each current control and its effectiveness (substantially effective, partially effective or largely ineffective). (See Template 5b for the control effectiveness legend.)

Control(s) description	**Control effectiveness rating(s)**
1.	1.
2.	2.
3.	3.

Current risk

Make an assessment of the risk considering the effectiveness of current controls.

Consequence level	**Likelihood level**	**Risk level**

Treatment

List additional controls to be put in place if the risk is not acceptable/tolerable, including resources required for each (financial, physical assets, HR) and a schedule for implementation.

Treatment	**Resources required**	**Person responsible**	**Implementation schedule**
1.	1.	1.	1.
2.	2.	2.	2.
3.	3.	3.	3.

Residual risk: Make an assessment of the risk level remaining after risk treatment.

Consequence level	**Likelihood level**	**Risk level**

Monitoring and review

Outline the reporting protocols for the risk and when the risk and controls are to be reviewed.

Communicate and consult

Do you need to communicate the results of this risk assessment to any stakeholders? If so, what channel(s) will you use and what is the schedule?

Comments

Comment on any uncertainties or sensitivities – are the risks that you have identified making the achievement of your agency's objectives too uncertain?

Compiled by	**Branch/Division**	**Date** DD/MM/YYYY	**Reviewed by and date**

5b. Risk assessment (landscape version)

All risk assessments should be clearly documented. You can use either Template 5a or 5b to document your assessment of a single risk at a divisional, operational or specific project level. Note that you should capture all your risks in your risk register (see templates 6a and 6b in this volume)

Compiled by:..... Date:..... Division/Branch:.....

Reviewed by:..... Date:.....

Risk assessment															
Risk description	**Objective(s) affected**	**Worst case**			**Current controls**		**Current case**			**Treatment**	**Treatment effectiveness**	**Implementation schedule**	**Residual risk**		
		Consequence	Likelihood	Risk level	Current controls in place	Effectiveness	Consequence	Likelihood	Risk level	*Additional control* if the risk is not acceptable/ tolerable (include timeframe for treatment)			Consequence	Likelihood	Risk level

Risk owner

Include the name of the person managing the risk and the area of the agency he or she works in (if the person assigned to treat the risk is different to the risk owner, you may also include their details in brackets within this section).

Resources required for proposed treatment
For example: financial, physical assets, HR.

Stakeholders consulted
Include internal and external stakeholders.

Monitoring and review

Outline the reporting protocols for the risk and when the risk and controls are to be reviewed.

Communicate and consult
Do you need to communicate the results of this risk assessment to any stakeholders? If so, what channel(s) will you use and what is the schedule?

Comments
Comment on any uncertainties or sensitivities – are the risks that you have identified making the achievement of your agency's objectives too uncertain?

Risk ratings legend

Risk ratings	
Risk level	**Combined ratings for consequence and likelihood using your risk matrix**
Worst case	The risk if the current controls do not exist or completely fail
Current case	The risk as it is now
Residual risk	The risk level remaining after risk treatment

Control effectiveness legend

Control effectiveness			
Level	**Description and further action**	**Design effectiveness**	**Operating effectiveness**
Substantially effective	Existing controls address risk, are in operation and are applied consistently. Management is confident that the controls are effective and reliable. Ongoing monitoring is required.	Y	Y
Partially effective	Controls are only partially effective, require ongoing monitoring and may need to be redesigned, improved or supplemented.	N	Y
		Y	N
Largely ineffective	Management cannot be confident that any degree of risk modification is being achieved. Controls need to be redesigned.	N	N

6a. Risk register (option 1)

A risk register is a list of all the risks that your agency has identified and assessed using its risk management process. Templates 6a and 6b are two possible risk register designs that you could consider as a starting point. Information in your risk register should be tailored to the information needs of your stakeholders. This is an example of a more concise option. Your risk assessment documentation should form the basis for the information in your risk register.

Risk register										
Risk ID	**Risk description**	**Business area/risk owner**	**Date last assessed DD/MM/YYYY**	**Risk category**	**Current case risk level**	**Treatments**	**Control effectiveness**	**Residual risk level**	**Review and reporting requirements**	**Comments**
					The risk level after current controls	Proposed treatments	e.g Substantially effective Partially effective Largely ineffective	Expected level of risk remaining once additional treatments have been implemented	How and when are the risk and controls to be reviewed and reported?	Uncertainties or sensitivities – are the risks that you have identified making the achievement of your agency's objectives too uncertain? Resources required – financial, physical, human resources

6b. Risk register (option 2)

A risk register is a list of all the risks that your agency has identified and assessed using its risk management process. Your risk assessment documentation should form the basis for the information in your risk register.

Risk register															
Risk ID	Assessment		Risk description	Objective(s) affected	Consequence type(s)	Risk owner	Risk ratings				Accept risk?	Controls/risk treatment		Review and reporting requirements	Comments
	By	Date (DD/MM/YYYY)					Case	C	L	Risk level		Description	Control effectiveness		
					– Financial – Service delivery Note that these should be aligned to your consequence table.	Include the name of the person managing the risk and the area of the organisation he or she works in. If the risk owner is different to the person assigned to treat the risk, you should include the risk owner's details.	Worst case					Current controls		How and when are the risk and controls to be reviewed and reported?	Uncertainties or sensitivities – are the risks that you have identified making the achievement of your agency's objectives too uncertain? Resources required – financial, physical, human resources
							Current			Level of risk remaining after the application of existing controls	Is the risk acceptable/tolerable?	Additional treatment if the risk is not acceptable/ tolerable Timing			
							Residual			Expected level of risk remaining after risk treatments	Is the risk acceptable/tolerable?				

7. Monitoring significant risks

Significant risks are those that have been given a worst case risk level rated as high or above (i.e. they are in the red zone of your risk matrix).

Compiled by:..... Date:……

Reviewed by:..... Date:……

Division/Branch:……..

Significant risks										
Risk ID	**Risk description**	**Affects objective(s):**	**Risk levels**		**Date last assessed**	**Control or risk treatment**	**Risk owner**	**Monitoring mechanisms**	**Current status**	**Comments**
			Worst case	**Current case**						
			List risks that have a worst case level of high or above (i.e. they are in the red zone of your risk matrix).			Description of risk treatment Schedule of risk treatment	Include the name of the person managing the risk and the area of the organisation he or she works in.	How and when are the risk and controls to be reviewed and reported?		E.g. next steps, resources required

8. Sample risk report

You can design your own reporting templates, similar to this example, for summarising risk register information to present to key stakeholders.

Summary					
Key comments: Provide an overall summary of the major risks facing the organisation, including treatments.					
Date submitted: DD/MM/YYYY					
Report prepared by:					
	No major risks		**Major risks but treatment in place**		**Major risks – ineffective or no treatments**

Risk profile	**Risk 1**	**Risk 2**	**Risk 3**	**Risk 4**	**Risk 5**	**Risk 6**	**Risk 7**
This report							
Last report							

Risk 1

Risk description	**Objective(s) affected**	**Current risk rating**	**Control effectiveness**	**Treatment**	**Risk owner**	**Trend of risk**
		Determine using your risk matrix.	Refer to Template 5b for the control effectiveness legend.	Description schedule Resources required	Include the name of the person managing the risk and the area of the organisation he or she works in.	

Risk 2

Risk description	**Objective(s) affected**	**Current risk rating**	**Control effectiveness**	**Treatment**	**Risk owner**	**Trend of risk**
		Determine using your risk matrix.	Refer to Template 5b for the control effectiveness legend	Description schedule Resources required	Include the name of the person managing the risk and the area of the organisation he or she works in.	

9. Maturity rating for risk management performance

Continual improvement is a core component of your risk management framework. It means enhancing your risk management framework and moving to a higher level of risk maturity.

Your agency should regularly monitor your risk management maturity so the latter can inform your improvement strategies.

You can use the attributes of enhanced risk management described in Annex A of ISO 31000 to measure your risk management maturity by defining a set of success indicators for each attribute.

You can develop success indicators appropriate to your agency. An example is provided in this template.

You may wish to use the results of this matrix to prioritise improvement strategies and to inform your agency's attestation of compliance with Core Requirement 5 of TPP 09-05.

Maturity matrix rating scale	
Maturity rating	**Description**
Low (L)	There is no or minimal awareness across the agency of the need to manage risk and there are no processes in place.
Inconsistent (I)	There is organisational awareness of the importance of risk and some areas of the agency have processes in place.
Consistent (C)	There is clear organisational commitment and there are common processes used across the agency.
Fully addressed (F)	There is clear organisational commitment and there are common processes used across the agency. We routinely monitor our approach to check its effectiveness and make improvements as necessary.

Function: ..... Compiled by: ..... Date .....

Reviewed by: ..... Date: .....

Risk management performance: maturity matrix

		Maturity rating scale				
Attribute	**Success indicator**	**Documentary evidence**	**Low**	**Inconsistent**	**Consistent**	**Fully addressed**
A1. Continual improvement	Our organisational performance is measured against explicit performance goals. The performance of our staff is measured against explicit performance goals. Our organisational performance is communicated and published. We review our performance annually and follow this with a revision of processes and setting of revised performance objectives for the following period. Risk management performance assessment is included in our performance assessment (agency and individuals). Our risk management framework is formally reviewed periodically.					
A2. Risk accountability	All staff are fully aware of the risks, risk controls and tasks for which they are accountable. We define accountabilities in position descriptions and in our risk assessments and treatment plans. Risk management roles, responsibilities and accountabilities are defined in our induction program. We provide those with risk accountabilities with appropriate authority, time, training and skills to assume their responsibilities.					

Function: ..... Compiled by: ..... Date .....

Reviewed by: ..... Date: .....

Risk management performance: maturity matrix

		Maturity rating scale				
Attribute	**Success indicator**	**Documentary evidence**	**Low**	**Inconsistent**	**Consistent**	**Fully addressed**
A3. Risk-based decision making	Our committee minutes record explicit discussions on risks. Our risk management process is used when making key decisions. Soundly based risk management is seen within our agency as providing the basis for effective and prudent governance.					
A4. Risk communication	Communication with stakeholders is clearly regarded by staff as an integral and essential component of risk management. Communication with stakeholders takes place as part of all our risk management activities. Communication about risk is a two-way process so that informed decisions can be made about the level of risk and the need for risk treatment against properly established and comprehensive risk criteria. Comprehensive and frequent internal and external reporting on significant risks and on risk management performance contributes substantially to effective organisational governance.					
A5. Risk integration	Risk management is embedded in our planning processes, decision-making structures and operational procedures. Our managers regard effective risk management as essential for the achievement of all agency objectives.					

10. Capability matrix

An agency's executive, managers and staff all manage the risks related to their primary functions. Their risk roles are to:

§ contribute to achieving the agency's objectives for their nominated function

§ recognise the potential consequences and likelihood of risks that might impact on the achievement of agency objectives

§ monitor the design and operating effectiveness of relevant controls.

In addition to these major roles, the executive, managers and staff will also have roles in implementing your agency's risk management framework.

Your capability matrix should capture:

§ the risk roles undertaken, both in implementing the risk management framework and managing risks

§ the capability required to perform these roles

§ how to develop this capability, including induction and ongoing learning and development.

You can use the following matrix to compare the required capability with the current skill levels of staff. This gap analysis can inform your agency's risk management training plan.

Capability matrix			
Position	**Risk roles**	**Required capability**	**Training needs**
Head of Authority/risk sponsor			

Refer to Part 2 page 37 for a worked example of a capability matrix.

The following table lists points that you can consider in your gap analysis depending on your agency's current capability or internal capacity to provide resources for ongoing initiatives.

Example capability matrix			
	Examine	**Decide**	**Deliver**
Where are we now? Know the current workforce capability	Current roles and job categories in relation to required capability Critical workforce data for your agency (including skills audits if available) Effectiveness of organisational structure	Pivotal roles for delivering a successful risk management framework – now and in the future (focus your efforts) Availability of required skills to meet risk management challenges	Clear picture of the current state of the workforce in relation to risk management knowledge, experience and skills Analysis of how risk capability issues impact on the delivery of business outcomes
Where are we heading? Understand the context	External and internal operating environments – consider using SWOT analysis Planned or possible organisational change or restructure including changes in service delivery Agency performance and customer feedback Organisational culture	Capability-building objectives Skill-building approach (e.g. top down, bottom up, all or some business units) Goals and critical success factors to aid in evaluation The organisational- and business unit-specific skill requirements emerging from planned or possible change scenarios	A business case which reflects the agency's key priorities and indicates how improving risk management capability will tackle strategic challenges Planning framework for building risk management capability Change management, communication and evaluation strategies Shared understanding of the required risk management capability profile for pivotal roles
How are we going to get there? Enhance performance	Gaps or deviation in current capability Strategy options to build organisational and workforce capability Agency's effectiveness in making flexible use of its workforce and HR strategies Opportunities for cross-agency collaboration Current better practice	Risk and priority of identified capability challenges Integrated strategies to address each priority issue (adjustment of current/new practices) Resources required to implement the strategy Strategy review and evaluation mechanisms	Comprehensive plans tailored to specific areas of the agency (e.g. divisional, work group) Implementation plan and review strategy Integration and alignment of risk management capability and attract and retain strategies Ongoing dialogue with line managers on emerging risk issues

Where there is an obvious need to develop a program that builds the capability of the agency to manage risk, the following questions are pertinent:

- What factors might you examine to make positive capability development decisions?
- How do you identify the most useful information?
- How do you prioritise areas for action?
- How do you best establish a workforce that is capable for managing risks into the future?

11a. Stakeholder analysis and communication planning

It is critical to properly plan your intended stakeholder communication approach. The following templates/examples (11b-e) outline possible techniques you can use to:

1. Identify your audience

You can use the stakeholder analysis matrix (Template 11b) to develop a better understanding of your stakeholders (Template 11c), their level of influence and the impact that your agency has on them. It is most crucial to use this method when there are clearly identified key stakeholders or where an activity's impact is high.

2. Understand your audience's communication needs

You can use the communication needs analysis tool (Template 11d) to identify any special information needs relating to stakeholders with whom you will communicate.

3. Plan your communication strategy

You can use the risk management communication strategy template (Template 11e) to identify how you will communicate with your stakeholders and how to measure the success of the communication process.

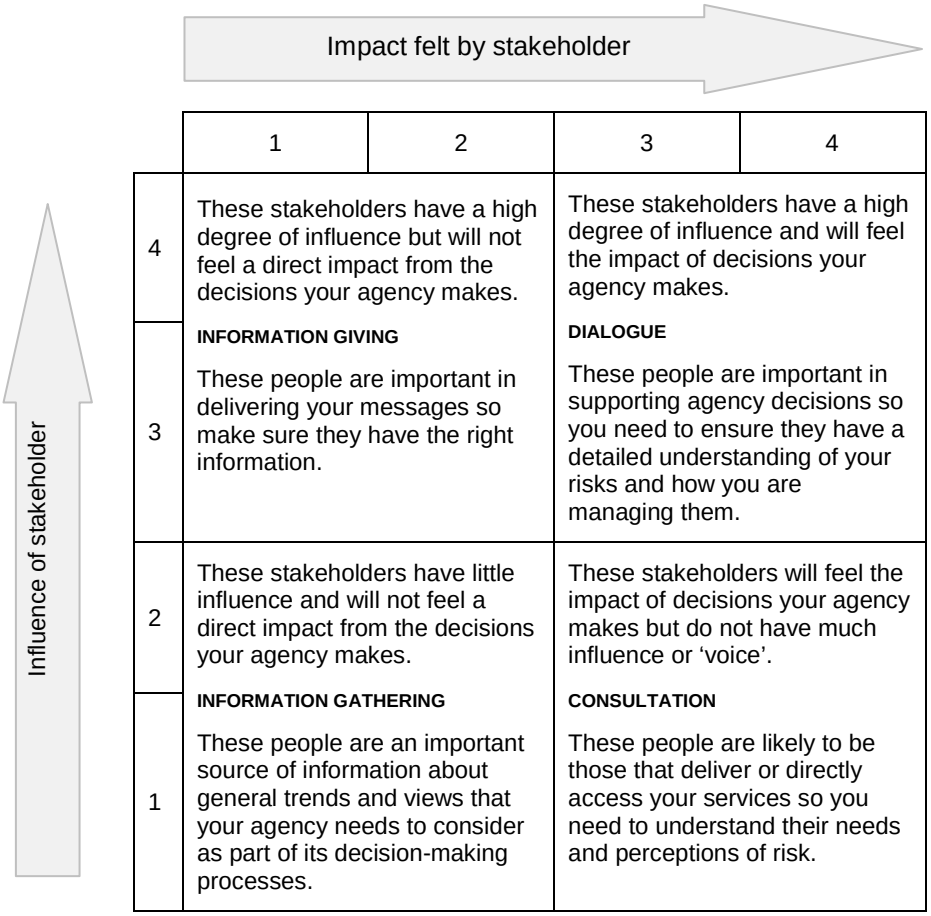
Your communication strategy should be reflected in your agency's risk management implementation plan and specific risk assessment plans.

11b. Stakeholder analysis matrix

The stakeholder analysis matrix provides a useful technique for assessing the importance and influence of key individuals and groups, and for determining how best to involve them in managing risks. This allows you to determine the level of engagement that you should aim for with them (information gathering, information giving, dialogue or consultation).

Method for completing the matrix

1. Identify your key stakeholders (see Template 11c on the next page for examples).
2. Rate each stakeholder's influence on your agency's ability to achieve its objectives from 1 (least) to 4 (most).
3. Rate the impact that the agency's objectives has on each stakeholder from 1 (least) to 4 (most).
4. Position each stakeholder on a grid using the results of 2 and 3 above. Document the results.



11c. External and internal stakeholders

Examples of external and internal stakeholders include but are not limited to those shown in the following example.

External	Internal
The community, including taxpayers	Head of Authority (risk sponsor)
Minister, ministerial office	Audit and Risk Committee
Regulatory authorities	Business unit managers
The media	Agency risk management champion(s)
Non-government organisations	Chief Audit Executive and internal audit teams
Interest groups: employer groups, industry groups, unions	Agency staff and contractors
Other government agencies (e.g. cluster/principal department, shared services providers)	
Clients	
Suppliers	
Representatives from Treasury and the Department of Premier and Cabinet	

11d. Risk management communication needs analysis

This tool enables you to note any special needs relating to communication activities with your stakeholders that you have identified using your stakeholder analysis tool.

Function: ..... Compiled by: ..... Date: .....

Reviewed by: ..... Date: .....

Risk management communication needs analysis					
Project or activity objective:	**Statement of project or activity objective (or risk)**				
	Internal stakeholders		**External stakeholders**		
Issues to consider communicating with stakeholders	**Stakeholder**	**Stakeholder**	**Stakeholder**	**Stakeholder**	**Stakeholder**
A recently identified risk management project, activity or risk					
Your agency's risk management project/activity, or risk assessment objectives					
A single or set of risk management project/activity or risk decision(s) and/or recommendation(s)					
Issues arising when evaluating controls, process for seeking feedback related to a specific risk management project/activity or risk					
Ongoing monitoring and reporting on a risk management project/activity or risk					

11e. Risk management communication strategy

Function: ..... Compiled by: ..... Date: .....

Reviewed by: ..... Date: .....

Risk management communication strategy						
Project objective	Short summary of the project/activity/risk					
Communication step	New activity, project or risk Objectives of project, activity or risk assessment Communication recommendations Evaluation or feedback					
Communications objective	**Audience or key stakeholders**	**Message content**	**Frequency**	**Communication channel**	**Measures and evaluations**	**Officer responsible for communicating the message**
A statement of the objectives, principles and key messages	Who will you communicate with and what are their priorities?	What is the key message(s)?	Is the communication: § ad hoc (before a particular event, after a particular event)? § regular? Have stakeholders been given adequate time to respond to communications if required?	How will you communicate with each group? Consider: § face to face, such as workshops, seminars, meetings or community forums § written forms, such as brochures, media releases, interpretive materials or direct mail § electronic forms, via e-mail, websites, blogs, social media, TV, radio, etc. § networks, such as peer-group networks, pressure-group networks and educational forums.	How will you evaluate the success of the communication method?	

Part 2: Case study

Southland Department of Law Enforcement

The Southland Department of Law Enforcement (DLE) provides community-based policing at more than 100 law enforcement stations. The DLE is a general government budget–dependent agency. In 2012–13, the DLE's total expenses are estimated to be $497 million.

The DLE is governed by the *Law Enforcement Act 1999* which sets outs out its principal objectives as:

- protect the community from crime
- reduce the incidence of crime in the community
- ensure that justice is served.

The government has allocated $40 million over four years for the establishment and full operation of a new E-Security Response Centre by December 2016.

Southland DLE aims to achieve the following goals:

- safe roads
- reduced rates of crime, particularly violent crime
- people feeling safe.

The department delivers the following key programs that contribute to the above goals:

- road safety
- crime prevention and community safety
- crime response and community support
- investigation and judicial support.

Southland DLE organisational chart

Southland DLE risk management implementation plan 2012–14

This plan was as at March 2012.

1. Corporate plan (risk management)

Corporate objective	To manage risk effectively and thereby improve our ability to meet our objectives	**Corporate strategy**	Embed risk management into all organisational systems and processes Develop an organisational culture that is risk aware

2. Risk management strategy

Objective	Strategy	Initiatives
1. Embed risk management in all organisational activities	Risk management needs to form part of all of Southland DLE's systems and processes. We need to establish mechanisms to support the implementation of risk management at all levels.	a) Identify our risk management objectives b) Identify risk management roles c) Integrate governance and risk management d) Integrate audit and risk management e) Integrate planning and risk management
2. Develop a common understanding of our risks and their management	We need to ensure that our approach to managing risk is well understood and applied consistently at all levels in Southland DLE. This requires: § an approach that meets the needs of Southland DLE § strong leadership § effective communication about risk.	a) Understand our internal and external operating environment as it relates to managing our risks b) Establish our risk leadership team consisting of Executive and other risk champions c) Understand our risk culture and identify any barriers to the implementation of our risk management framework d) Develop our risk capability e) Develop and implement our risk management policy f) Develop our risk management communication strategy

Objective	Strategy	Initiatives
3. Measure, control and monitor our risks	We need to ensure that our process for managing risk is clearly defined, repeatable and based on appropriate information.	a) Identify our risk tolerances b) Develop our risk process, including the rules for risk escalation and risk reporting c) Develop our risk information strategy d) Identify, assess and control our strategic risks e) Cascade our risk management process into all levels of planning f) Develop a process for identifying and managing project risks g) Develop a process for identifying and managing ad hoc risks h) Develop our risk management reporting strategy
4. Continue to improve our risk management practice	We need to understand what level of risk management maturity is current in Southland DLE and what level is required, and develop a strategy to close the gap.	a) Identify what constitutes an appropriate level of risk management maturity for Southland DLE b) Develop our risk management assurance program to monitor the effectiveness of our risk management framework and risk management maturity

3. Risk management action plan

Note: Activities and tasks completed as part of the 2011–12 plan are included to provide a comprehensive view of the development and implementation of the risk management framework.

Initiatives		Tasks	To be completed by	Responsibility
1a	**Identify risk management objectives**	§ Set the scope and purpose for risk management	Completed	
1b	**Risk management roles**	§ Identify those with accountability and responsibility for roles associated with developing and implementing the risk management framework	Completed	
		§ Identify those with accountability and responsibility for roles associated with identifying and managing risk	Completed	
		§ Revise position descriptions to reflect risk management roles	June 2012	Human Resources
		§ Revise delegation manual to reflect risk management roles	June 2012	Governance
		§ Review committee charters to ensure risk management responsibilities are clearly articulated	Completed	
		§ Ensure roles are articulated in the risk management policy	Completed	
1c	**Integrate governance and risk management**	§ Review governance framework and structure to incorporate risk management	December 2012	Governance and Chief Risk Officer (CRO)
1d	**Integrate audit and risk management**	§ Review Audit and Risk Committee (ARC) charter for compliance with TPP 09-05	Completed	
		§ Clarify audit and risk management roles and responsibilities	June 2012	Chief Audit Executive (CAE)
		§ Establish risk-based audit methodology	December 2012	CAE
1e	**Integrate planning and risk management**	§ Embed risk management into the planning framework and all planning activities, including project planning	December 2013	Strategic Planning and CRO
2a	**Context**	§ Identify Departmental objectives where risk needs to be managed	Completed	
		§ Identify legislative and compliance requirements	Completed	
		§ Undertake environmental scans (external and internal) to identify potential sources of risk	Completed	
		§ Undertake stakeholder analysis	Completed	
		§ Understand potential impacts of these sources of risk to identify the types of risk that we need to manage	Completed	

Initiatives		Tasks	To be completed by	Responsibility
2b	**Risk Leadership Team (Executive risk champion and other risk champions)**	§ Communicate Director General's commitment to risk management	Ongoing	Director General
		§ Identify membership of risk leadership team	Completed	
		§ Ensure risk leaders are familiar with TPP 09-05 and AS/NZS ISO 31000 and encourage them to read the Treasury *Risk Management Toolkit for NSW public sector agencies*	Ongoing	CRO
		§ Hold a risk management framework information session with the risk leadership team	Completed	
2c	**Risk culture**	§ Undertake a risk climate survey to establish the current (baseline) risk culture	Completed	
		§ Perform a gap analysis between baseline and the culture that we are aiming for	Completed	
		§ Identify strategies to close the gap	June 2012	CRO
2d	**Risk management capability**	§ Develop our risk management capability matrix	Completed	
		§ Identify learning needs	Completed	
		§ Review training program and revise to meet risk management training needs	December 2012	CRO
2e	**Risk management policy**	§ Develop risk management policy	Completed	
		§ Review other risk-related policies for consistency	Completed	
		§ Review by Executive and ARC	Completed	
		§ Director General's endorsement for the policy	Completed	
		§ Publish and communicate policy	Completed	
		§ Review risk management policy and practice	Annually	CRO and ARC
2f	**Risk management communication strategy**	§ Identify communication needs using results of the stakeholder analysis (see 2a)	October 2012	CRO and Communications Manager
		§ Develop communication strategy for implementing the risk management framework	November 2012	CRO and Communications Manager
3a	**Risk attitude and risk tolerances**	§ Develop our risk tolerances for each type of risk (see 2a) to reflect our overall attitude to risk	Completed	
		§ Develop a risk escalation process based on our risk tolerances	Completed	
		§ Identify how tolerances and risk escalation will be reflected in our consequence tables and risk matrix (see 3b)	Completed	

Initiatives		Tasks	To be completed by	Responsibility
3b	**Risk management process**	§ Identify how many risk assessment processes we need to cover all areas of our business (strategic, operational, project, etc.)	Completed	
		§ Research available risk assessment tools to identify appropriate methodologies for risk identification, analysis, treatment, etc.	Completed	
		§ Develop our consequence table(s), likelihood table(s) and risk matrices for the assessment of threats	Completed	
		§ Develop risk assessment facilitation and support strategy	Completed	
		§ Develop risk assessment and treatment guidelines, including templates	Completed	
		§ Monitor use of risk process for consistency	Ongoing	ARC, Internal Audit and CRO
		§ Develop review/revision plan for risk process	August 2013	CRO
		§ Revise risk policy and process, including expanding our risk tables and matrix to consider positive risk (opportunities)	June 2013, then annual	CRO
3c	**Risk information strategy**	§ Identify stakeholder information needs	July 2013	CRO
		§ Develop our risk register (Microsoft Excel-based initially)	Feb2013	CRO
		§ Develop our risk profiles (Microsoft Word/Excel-based initially)	Feb 2013	CRO
		§ Investigate future options for risk information management system	July 2013	CRO
		§ Develop a medium- to long-term risk information plan	September 2013	CRO
3d	**Strategic risk assessment**	§ Undertake a risk assessment of our corporate objectives as an integral part of the strategic planning cycles to identify strategic risks and their treatment	March 2013 and ongoing	Executive team facilitated by Strategic Planning and CRO
		§ Use the assessment to inform our internal audit plan	March 2013 and ongoing	Internal Audit and CAE
		§ Report on risks in our strategic risk register and risk profile	March 2013 and ongoing	CRO
		§ Develop and implement a monitor/review process for our strategic risks	March 2013 and ongoing	CRO

Initiatives		Tasks	To be completed by	Responsibility
3e	**Cascade risk management process**	§ Undertake risk assessments of our operational objectives as an integral part of business planning cycles to identify operational risks and their treatment	April 2013 and ongoing	Service Group managers facilitated by Strategic Planning and CRO
		§ Escalate operational risks as per strategy defined in risk matrix	April 2013 and ongoing	Service Group managers
		§ Use the assessments to inform our internal audit plan	April 2013 and ongoing	Internal Audit and CAE
		§ Report on risks in our operational risk register(s) and risk profile (where relevant)	April 2013 and ongoing	Service Group managers and CRO
		§ Develop and implement a monitor/review process for our operational risks	April 2013 and ongoing	CRO
3f	**Project risks**	§ Undertake risk assessments of our project objectives as an integral part of project planning to identify project risks and their treatment	April 2013 and ongoing	Project teams facilitated by CRO
		§ Escalate project risks as per strategy defined in risk matrix	April 2013 and ongoing	Project managers
		§ Use the assessments to inform our internal audit plan as appropriate	April 2013 and ongoing	Internal Audit and CAE
		§ Report on risks in our project risk register(s) and risk profile (where relevant)	April 2013 and ongoing	Project managers and CRO
		§ Develop and implement a monitor/review process as part of our project governance framework	April 2013 and ongoing	CRO
3g	**Ad hoc risks**	§ Develop a process for dealing with ad hoc risks (risks that are identified outside of planning and project work), including: - analysis - treatment - escalation - communication, reporting and inclusion in risk registers - monitoring and review	April 2013 and ongoing	CRO

Initiatives		Tasks	To be completed by	Responsibility
3h	**Risk management reporting strategy**	§ Understand external reporting requirements	Completed	
		§ Understand ARC and Executive reporting requirements	Completed	
		§ Develop risk management report template	Completed	
		§ Develop and implement risk management reporting plan	Completed	
		§ Review/revise risk management reporting strategy as part of the review of our risk management framework	June 2014	CRO/ARC
4a	**Risk management maturity**	§ Establish a methodology for determining our organisational risk maturity	Completed	
		§ Undertake the maturity analysis to identify our current (baseline) maturity	June 2012	CRO
		§ Review our maturity at 12 months from first assessment	June 2013	CRO
		§ Use the results of the review to inform our risk management improvement strategy	July 2013	CRO
		§ Review our risk management maturity methodology	March 2014	CRO
4b	**Risk management assurance**	§ Develop and include risk management framework KPIs in our performance management framework	November 2012	CRO and Strategic Planning
		§ Develop review/revision plan for our risk management framework	Completed	
		§ Review our risk management framework	June 2014	CRO

Southland DLE risk management policy

Southland DLE provides community-based policing to ensure safe roads and safe communities. Risk management is concerned with understanding and managing uncertainty. We recognise that by embedding risk management into all organisational systems and processes, we optimise our ability to meet our organisational objectives.

We have developed a Risk Management Framework consistent with AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, to guide and support consistency in our approach to risk management and decision making. Our framework includes a tailored risk management process to ensure we identify and analyse risks consistently across all functions and that risk evaluation is linked to practical and cost-effective risk controls that are appropriate to our business. We record all key risk management decisions.

The Risk Management Policy sits within Southland DLE's broader policy framework. We incorporate suitable risk management activities into our business planning, development of new policies and programs, operations, and contract and project management.

Risk management is a continuous process that demands awareness and proactive behaviour from all staff, contractors and external service providers to reduce the possibility and impact of accidents and losses, whether caused by the Department or external sources, and improve our ability to respond to opportunities.

Risk management is a core responsibility for all managers. In addition to the assessment of risk, their roles include:

- ensuring our staff have the appropriate capability to perform their risk management roles
- prioritising and scheduling risk control improvements
- reporting to the Executive on the status of risks and controls
- identifying and communicating potential improvements in the Department's risk management practices to the Department's Chief Risk Officer.

All staff are responsible for identifying and managing risk within their work areas. In undertaking their responsibilities, we expect our staff to be familiar with, and understand, the Department's Risk Management Framework including the Department's risk reporting protocols. We expect our staff to be able to differentiate between those risks that are within their responsibility and authority to manage and those that they should escalate through their management structure for further consideration and management.

The Department's Chief Risk Officer is available to support staff in undertaking their risk management activities.

All committees need to consider relevant risks and their management as a regular item of all meetings. Our Audit and Risk Committee is responsible for reviewing our:

- risk management process and procedures
- risk management strategies for major projects or undertakings
- control environment and insurance arrangements
- business continuity planning arrangements
- fraud control plan.

The Department will publish a summary of its risk management performance in its Annual Report. Our challenge for the future is to create a culture where we integrate risk management into our everyday service delivery operations and those of our contractors and partners. Everyone's involvement and support is critical to achieving our goals and departmental objectives.

We have developed a common risk vocabulary to use when we talk about risk and risk management. This is available on our intranet site along with risk management tools, processes and procedures.

The Department is committed to continually improving its ability to manage risk. We will review this policy and our Risk Management Framework at least annually to ensure that it continues to meet our requirements.

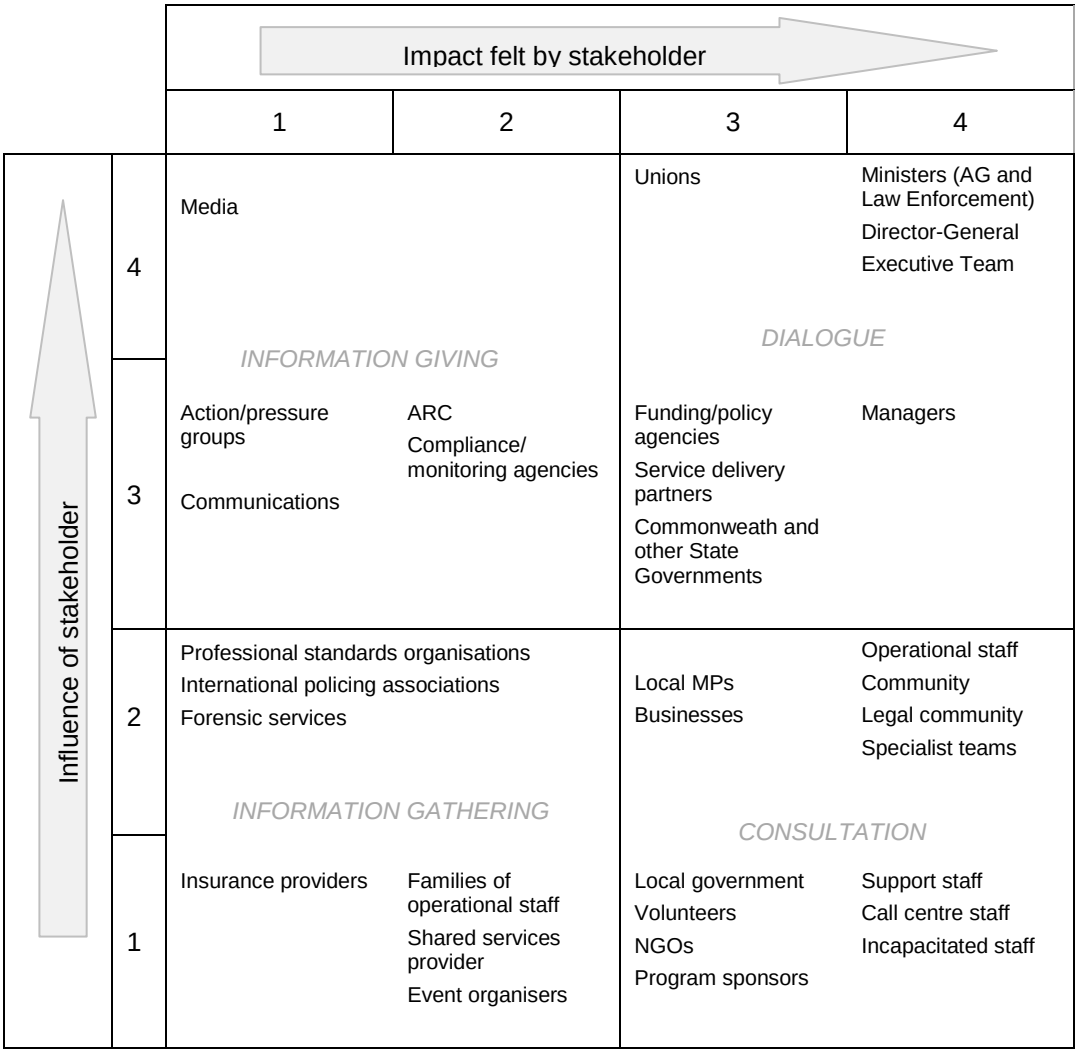
For further information on Southland DLE's Risk Management Policy, Framework and Process, contact the Department's Chief Risk Officer, <officer name> on email address <email contact> or by phone <contact number>.

Signed

Director-General, Southland DLE

Southland DLE stakeholder analysis matrix

Southland DLE undertook a stakeholder analysis facilitated by the Communications Manager and the CRO. The results are shown below.



Southland DLE capability matrix

In Southland DLE, the responsibility for developing and managing the risk management framework resides with the dedicated Chief Risk Officer (CRO).

This position reports to the Assistant Director-General Corporate Services. This Assistant Director-General is seen as the 'risk specialist' on the Executive and has been designated the Executive's risk champion. In addition, each Assistant Director-General has nominated a risk champion from their service group.

All staff are responsible for managing the risks within their areas of operations and for identifying and escalating those risks that are beyond their delegated authority to manage.

The agency's capability matrix is shown in the following table.

Position	Risk roles	Required capability	Training needs
Agency Head of Authority and Executive	Sign off on risk management policy and framework Provide risk leadership, including communicating about risks and their management Undertake strategic planning Participate in critical incident debriefs	Good understanding of risk management principles Strong understanding of the agency's external, internal and risk management context Understanding of governance, risk management and compliance (GRC) principles	Executive briefings by CRO and risk champion
Executive Risk Champion: Assistant Director-General, Corporate Services	Support the Executive in undertaking risk activities Promote benefits of risk management to all staff Champion and support the activities of CRO Represent agency on ARC (non-independent member)	As above plus: Skills and expertise in risk management Well-developed communication skills	External training in risk management and risk analysis External training in security and business continuity principles Mentoring by CRO
Risk champions	Support their service group in undertaking risk activities Promote benefits of risk management to all staff Champion and support the activities of CRO	As above	External training in risk management Mentoring by CRO
CRO	Develop, implement and monitor the risk management policy, framework and risk management plan Manage the agency's risk information including risk register and risk profile Provide updates to the Executive and ARC on the status of risks and controls Liaise with Internal Audit on control assurance requirements and activities Facilitate strategic and operational risk analysis Provide risk consultancy and mentoring to staff	Detailed expertise in risk management and risk assessment Good understanding of the agency's external, internal and risk management context Strong facilitation skills Strong technical and report writing skills	External training in risk management and risk analysis External training in security, business continuity, incident management, etc. Access to risk management publications and standards Membership of professional risk management body Facilitation training Access to external mentoring

Position	Risk roles	Required capability	Training needs
Business unit managers	Undertake business unit planning and risk analyses Understand and abide by the agency's risk policy Understand and use operational risk information Report on hazards Undertake operational incident debriefs	As above plus: Understanding of links between risk management and planning Good understanding of the agency's operational and risk management context	As above plus: Incident investigation training
Operational staff	Understand and abide by organisational policies and procedures Understand and use operational risk information Report on hazards Participate in operational debriefs	Understanding of agency's approach to risk management Ability to use hazard reporting system	Induction to include risk management policy and hazard reporting process Internal operational risk assessment training

Southland DLE consequence table

Step 1: Identify types of consequences that should be included in your table

Southland DLE has identified the following consequence types:

- financial
- work health and safety
- community impact – injury or property damage caused by inappropriate staff actions (including inaction)
- legal and regulatory
- service delivery disruption – caused by either a loss of a critical system/facility or insufficient staff to provide services
- service performance
- reputation and image.

Step 2: Determine how many levels of consequences you need in your table

Southland DLE has decided to use four consequence levels in our consequence table. We have defined these levels in terms of the level of management resources that would be involved.

Consequence levels	
Consequence level	**Consequence level description**
VERY HIGH	Affects the ability of DLE to achieve its objectives and may require third-party intervention
HIGH	Affects the ability of DLE to achieve its objectives and requires significant coordinated management effort at the Executive level
MEDIUM	Affects the ability of a single business unit in DLE to achieve its objectives but requires management effort from areas outside the business unit
LOW	Affects the ability of a single business unit in DLE to achieve its objectives and can be managed within normal management practices

Step 3: Describe each consequence level for each consequence type

Southland DLE has aligned our consequence descriptions for each consequence type to the consequence level based on management resources to ensure that they are consistent and unambiguous.

Southland DLE consequence table – for threats

(Southland DLE uses a similar consequence table for opportunities.)

		CONSEQUENCE LEVEL			
CONSEQUENCE TYPE		**LOW**	**MEDIUM**	**HIGH**	**VERY HIGH**
	FINANCIAL (FIN)	*The financial impact…*			
		Does not exceed 0.1% of Southland DLE budget	More than or equal to 0.1% of Southland DLE budget but less than or equal to 0.5% of that budget	More than or equal to 0.5% of Southland DLE budget but less than or equal to 2% of that budget	Exceeds 2% of Southland DLE budget
	WORK HEALTH AND SAFETY (OH&S)	*An unsafe work environment or act causes…*			
		1 staff member or contractor lost-time injury	1–5 staff members or contractor lost-time injuries	1 or more staff member or contractor permanent disability injury and/or 5–25 staff or contractor lost-time injuries	Fatality and/or More than or equal to 5 staff member or contractor permanent disability injuries and/or More than or equal to 25 staff member or contractor lost-time injuries
	SERVICE DELIVERY DISRUPTION (DISRUPT)	*Loss of access to critical systems or facility causes…*			
		Service failure across a single service group's services that can be managed within the service group	A significant disruption to business continuity across a single service group's service requiring resources from other areas of Southland DLE	A major disruption to business continuity across multiple Southland DLE services	A significant disruption in business continuity across all major Southland DLE services
	LEGAL/ COMPLIANCE (LEG)	*Breach of legislation, law and/or government policy requirements causes failure to…*			
		Fully comply with requirements, which can be corrected without consequence	Fully comply with requirements, resulting in legal action of internal investigation	Comply with requirements, resulting in civil damages, criminal penalties or government investigation	Meet requirements, resulting in significant civil damages, serious/extreme criminal penalties or government remedial action

CONSEQUENCE TYPE		CONSEQUENCE LEVEL			
		LOW	**MEDIUM**	**HIGH**	**VERY HIGH**
	SERVICE PERFORMANCE (PERF)	*Inability to meet service delivery performance requirements causes…*			
		Changes to service delivery strategies managed within the service group	Significant changes to a single group's service delivery, requiring some realignment of resources within Southland DLE	Significant realignment of service delivery strategies across several service groups	Imposition of significant service delivery reforms by government
	REPUTATION AND IMAGE (REP)	*Management of issue(s) causes…*			
		Temporary loss of confidence in Southland DLE in some sections of the community and/or Ongoing individual concerns	Major impact on public confidence in Southland DLE (days) and/or Concern expressed by Minister in Southland DLE activities	Considerable and widespread impact on public confidence in Southland DLE (days/weeks) and/or Issues raised in Parliament	Significant impact on public confidence in Southland DLE (months) and/or Potential parliamentary enquiry

Southland DLE likelihood table

Step 1: Determine how many levels of likelihood you need in your table

Southland DLE has decided to use four likelihood levels: almost certain, likely, possible and rare.

Step 2: Decide how to describe the likelihood

Southland DLE has decided to define likelihood:

§ in general terms, using words such as expected, could occur and may occur, and

§ with indicative frequencies based on the chance of occurrence in the coming year.

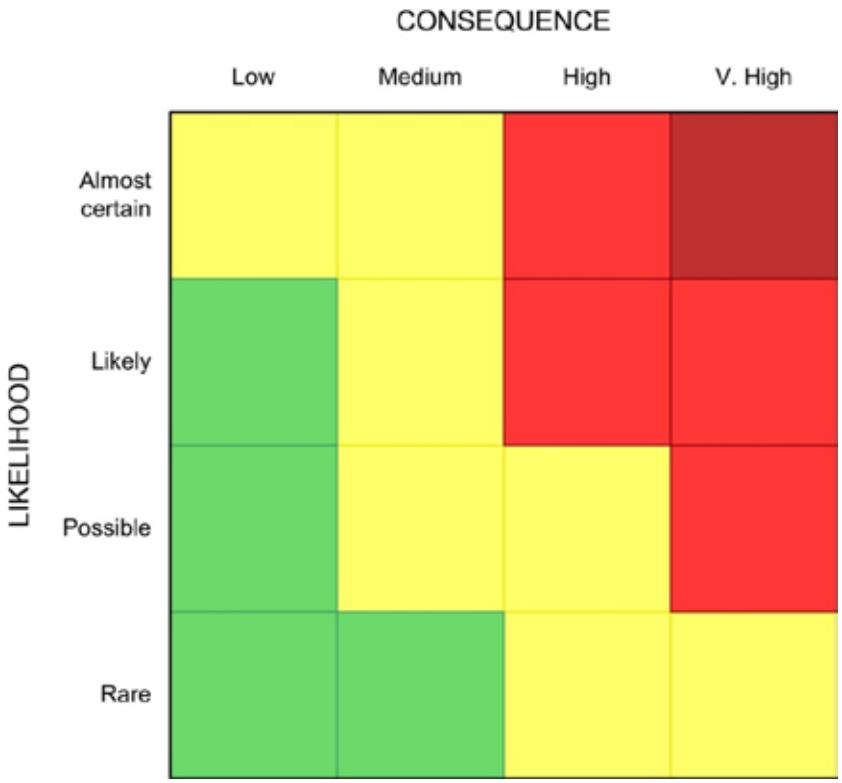
Step 3: Describe the levels of likelihood in a table

Likelihood table			
Likelihood descriptor	**General descriptions**		**Indicative frequency**
Almost certain	Is expected to occur in most circumstances	The event will occur on an annual basis – within the short-term (e.g. budget) planning cycle	Will occur within this year
Likely	Could occur in some circumstances	Is likely to happen to Southland DLE within the long-term (10-year) planning cycle	1 chance in 10 of occurring this year
Possible	Could occur but would not be expected	Has happened in the Australian law enforcement sector	1 chance in 200 of occurring this year
Rare	May occur only in exceptional circumstances	Could happen in the global law enforcement sector	1 chance in 1,000 of occurring this year

Southland DLE risk matrix

Southland DLE currently only considers threats when undertaking risk assessments. However, we have designed our risk tables and matrix in a way that also enables opportunities to be considered.

Southland DLE has defined four groups for its risk matrix: extreme, major, moderate and minimal. Risks rated extreme and major are unacceptable; risks rated as moderate are in the ALARP (As Low As Reasonably Practicable)[1] group and risks rated as minor are acceptable.



Southland DLE has linked its risk communication and risk ownership strategies to its risk escalation points as shown in the table below.

EXTREME	Immediate escalation to the Executive Control strategy developed and monitored by the Executive
MAJOR	Escalation to the Executive at next meeting Ownership of risk assigned to a member of the Executive
MODERATE	Managed at functional/service group level Escalated to relevant Assistant DGs for information
MINIMAL	Managed within functional area/service group

[1] Refer to ISO 31010.

Southland DLE risk register

Note: This register was prepared as at March 2012

ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
A2	Exec Team	3/12	Government response to changing community needs causes a mismatch between Southland DLE's organisational capability and new service delivery requirements, resulting in negative impact on all Southland DLE objectives	SERVICE PERFORMANCE	Comm.	Worst case	V High	Likely	Major	No	Forward workforce planning Targeted recruitment strategies Training matrix for workforce Review and revision of training needs (SUP HRM)	Yes	Review the effectiveness of the controls through annual frontline officer and specialist roles skills audit
						Current	Med	Likely	Mod	Yes			
						Residual							
A3	Exec Team	3/12	Ageing and obsolete IT infrastructure causes IT systems to be hacked, resulting in inappropriate use and loss of sensitive information	LEGAL/COMPLIANCE REPUTATION AND IMAGE FINANCIAL	ADG CS	Worst case	V High	AC	Ex	No	Firewall and virus software User access controls User ID and password policy Routine penetration testing (MAN Exec Res and Inf)	No	Quarterly reporting to the Executive of progress against project milestones and budget Reporting of firewall breaches to ADG CS
						Current	V High	Pos	Major	No	Upgrade IT Systems (ADG CS)	Yes	
						Residual	V High	Rare	Mod				

ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
A4	Exec Team	3/12	Findings of widespread corruption in other jurisdictions creates a negative association for Southland DLE as a law enforcement agency, resulting in loss of reputation, heightened scrutiny and lower internal morale	REPUTATION AND IMAGE	Comm.	Worst case	Med	Likely	Mod	No	Recruit psychological testing program, induction program, governance (incl. whistleblower) programs (MAN Educ Serv)	Yes	Quarterly report to the Executive on reported incidents of suspected fraud or corruption, and/or access to whistleblower program
						Current	Low	Likely	Min	Yes			
						Residual							
A5	Exec Team	3/12	Questions about the performance and effectiveness of Southland DLE's activities raised by the Parliamentary Accounts Committee causes a perception that the Department does not present good value to the community, resulting in an adverse impact to our budget position	REPUTATION AND IMAGE FINANCIAL	ADG CS	Worst case	High	Likely	Major	No	Performance management systems in place to monitor outputs against objectives on a quarterly basis. Performance measures are reviewed and updated annually Executive monitoring of budget against performance criteria (crime statistics, road safety, community measure, etc.) Twice-yearly assessment to identify opportunities for improvement and/or reallocation of resources (DIR Strat. Plan.)	Yes	Reporting as directed through the strategic plan, reporting as directed through community performance metrics
						Current	Med	Pos	Mod	Yes			
						Residual							

ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
A6	Exec Team	3/12	Increasing age of frontline officers and an imbalance between retirements compared to recruitments causes a skill shortage across frontline policing roles, resulting in the inability to provide frontline policing	SERVICE PERFORMANCE	ADG CS	Worst case	V High	Likely	Major	No	Development of workforce-planning strategy to bring forward recruitment numbers and reskill non-frontline officers to frontline positions Targeted recruitment strategies to include socially diverse groups (SUP HRM)	Yes	Report quarterly to the Executive on workforce-planning strategy progress Report quarterly to the Executive on workforce retention statistics
						Current	V High	Pos	Major	No	Consider and develop incentive schemes (SUP HRM)	Yes	
						Residual	V High	Rare	Mod	Yes			
A7	Exec Team	3/12	Poor communication has led to a mismatch between the community's perception of public safety and real crime rates, resulting in a drop in Southland DLE's reputation as an effective policing authority	REPUTATION AND IMAGE	ADG FO	Worst case	Med	Pos	Mod	No	Community education and communication strategy about serious crime rates and impact (DIR PA)	No	Review community education strategy annually Report to the Executive on communication strategy performance every six months Report to the Executive on community safety measures following each survey
						Current	Med	Pos	Mod	No	Improve communication of strategy to stakeholders Monitor community response and modify strategy accordingly	Yes	
						Residual	Med	Rare	Min	Yes			
1.2	Exec Team	3/12	Poorly delivered road safety awareness campaign causes the road safety education program to fail, resulting in Southland DLE missing road safety improvement targets	SERVICE PERFORMANCE	ADG RS	Worst case	High	Pos	Mod	No	Service provider agreement with performance metrics in place Independent program evaluation to assess effectiveness (DIR PA)	Yes	Review service provider agreement performance criteria annually Report to the Executive quarterly on road safety performance statistics
						Current	High	Rare	Mod	Yes			
						Residual							

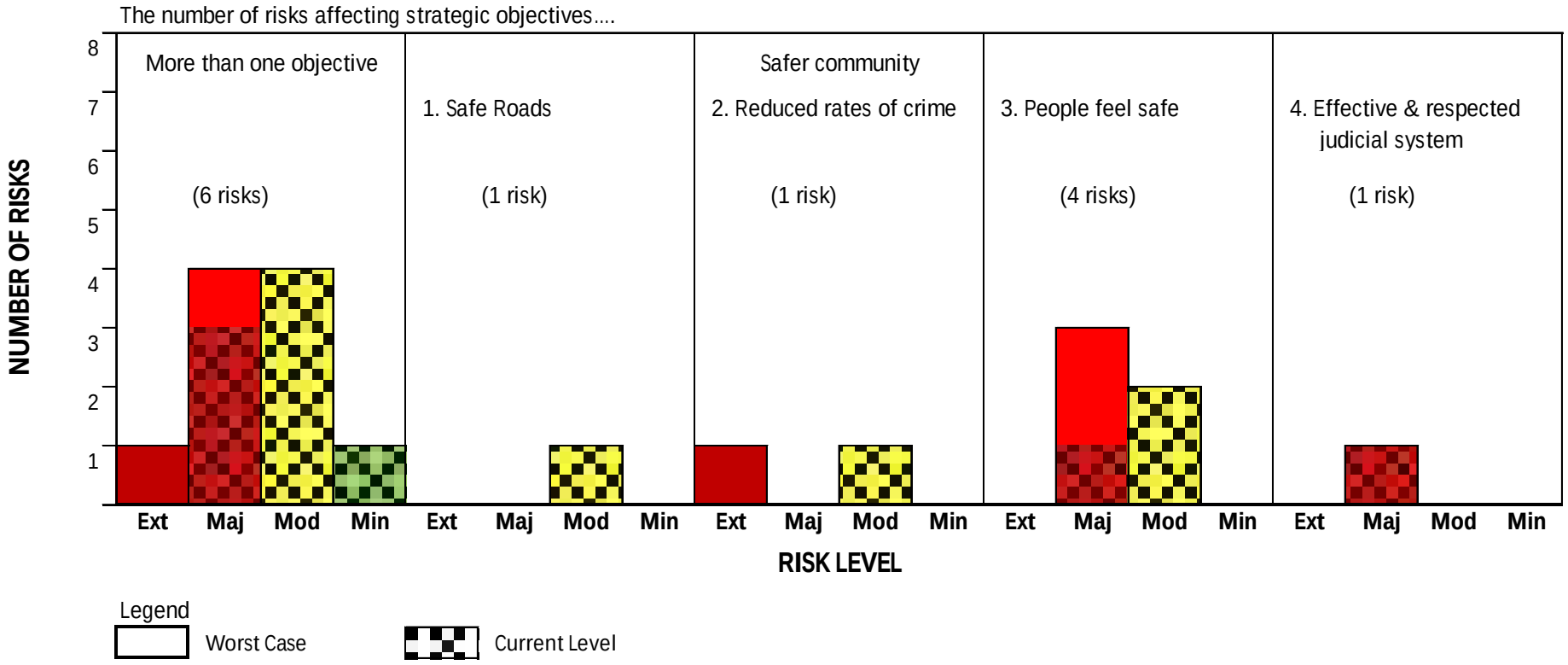
ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
2.1	Exec Team	3/12	Southland DLE's inability to fill specialist analyst roles causes a new or emerging threat, e.g. cybercrime, to be overlooked, resulting in greater community concern about potential incidents	REPUTATION AND IMAGE SERVICE PERFORMANCE	ADG SO	Worst case	V High	AC	Ex	No	Staff access to national training programs, formal and/or informal sharing of information across jurisdictions (ADG SO)	Yes	Monthly emerging threat assessment report to the Executive Report on progress in establishing specialty units, and national/international alliances
						Current	V High	Pos	Major	No	Establishment of specialty units with skill and experience in emerging threats such as cybercrime Develop alliances with national and international assessment and investigation bodies (ADG SO)	Yes	
						Residual	V High	Rare	Mod	Yes			
3.1	Exec Team	3/12	Ageing IT infrastructure causes Southland DLE's communication systems to fail and they are non-operational for a number of hours, resulting in the inability to deliver effective policing services to the community	SERVICE DELIVERY DISRUPTION	ADG FO	Worst case	High	AC	Major	No	Southland DLE Business Continuation Plan (CRO)	No	Report on annual BCP testing Quarterly reporting to the Executive on progress against project milestones and budget Reporting of communication systems failures to ADG Corporate Services
						Current	High	AC	Major	No	Reduce the level of risk through an investment in upgrading the IT system for communications (ADG CS)	Yes	
						Residual	High	Rare	Mod	Yes			

ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
3.2	Exec Team	3/12	The inability to gain government support for the policy allowing volunteers to 'police' school crossings causes greater strain on frontline policing resources, resulting in a reduction in policing services to the community	REPUTATION AND IMAGE SERVICE PERFORMANCE	ADG FO	Worst case	Med	AC	Mod	No	Undertake stakeholder focus group meetings throughout affected community (DIR CE)	No	Report from project steering group to the Executive on status of project quarterly Report to the Executive on alternative strategies
						Current	Med	Pos	Mod	No	Investigate alternative policies that allow a transfer of school crossing duties to non-uniformed officers or other strategies that do not require changes to legislation	Yes	
						Residual	Med	Pos	Mod	Yes			
3.3	Exec Team	3/12	Changes in population demographics across Southland, which are not considered in DLE's policing strategy, result in Southland DLE frontline policing becoming ineffective for local communities	REPUTATION AND IMAGE SERVICE PERFORMANCE	ADG FO	Worst case	High	Likely	Major	No	Workforce-planning strategy assesses socio-demographic changes in the community (SUP HR)	Yes	Report quarterly to the Executive on workforce planning strategy progress Report quarterly to the Executive on workforce retention statistics Annual report to the Executive on Southland's demographic mix and changes by specialist
						Current	High	Pos	Mod	No	Implement mobile policing into regional areas Undertake recruitment programs within socially diverse groups Offer incentives for officers to relocate to regional areas (SUP HR)	Yes	
						Residual	Med	Pos	Mod	Yes			

ID	Assessment		Risk description	Impacts (consequence type)	Risk owner	Ratings					Controls/risk treatment		Review and reporting requirements
	By:	Date (M/YR):					C	L	RISK	Accept ?	Description (Owner)	Effect	
3.4	Exec Team	3/12	Lack of community understanding about the role of the '000' emergency hotline causes an increase in non-urgent calls, resulting in an increase in emergency call receipt times	SERVICE PERFORMANCE REPUTATION AND IMAGE	ADG FO	Worst case	V High	Pos	Major	No	Public education campaign on emergency and non-emergency numbers Regular testing of technology for redirecting calls and updating as required Staff training and development for handling calls	Yes	Report quarterly to the Executive on call receipt statistics
						Current	Med	Pos	Mod	Yes			
						Residual							
4.2	Exec Team	3/12	Insufficient skills and budget to increase levels of skilled staff and retrain staff in new forensic technology division causes a failure to take advantage of improvements in forensic technology, resulting in an increase in challenges over quality of trial evidence, poor judicial outcomes, reduced morale, and the inability to attract and retain incident investigation and forensic evidence staff	SERVICE PERFORMANCE REPUTATION AND IMAGE	ADG SO	Worst case	High	AC	Major	No	Resource forensic specialists and provide training to current forensic and investigations staff in leading-edge technologies (DIR Foren.Inv.Unit)	No	Report to the Executive on progress in creating and filling staff specialist roles Report to the Executive on strategic partnerships as they are agreed to
						Current	High	Likely	Major	No	Seek strategic partnerships with high-performing forensics organisations (DIR Foren.Inv.Unit)	Yes	
						Residual	High	Pos	Mod	Yes			

Southland DLE risk profiles

Profile of risks affecting strategic objectives

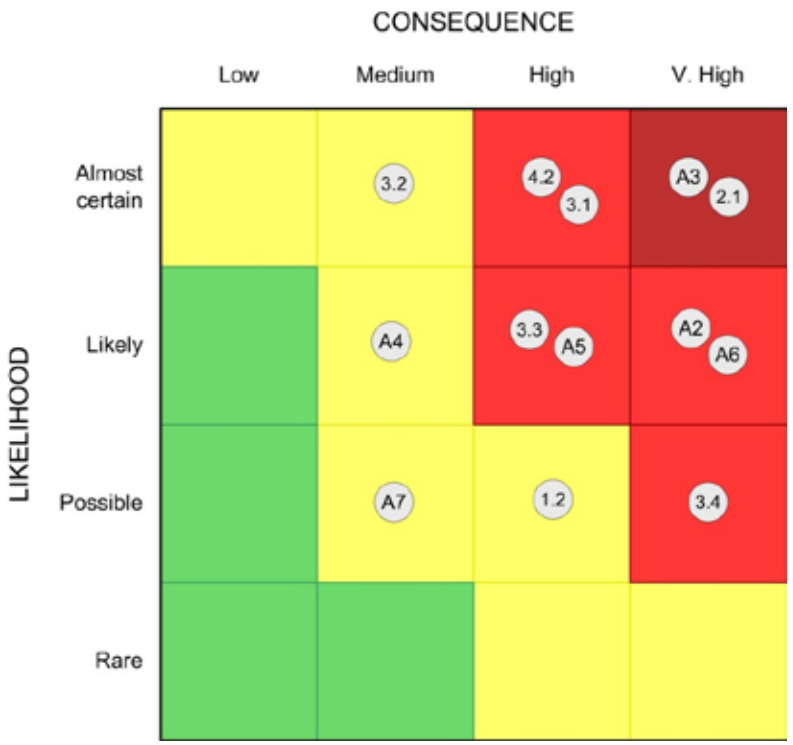


(Tabled at Executive team meeting held 7 March 2012.)

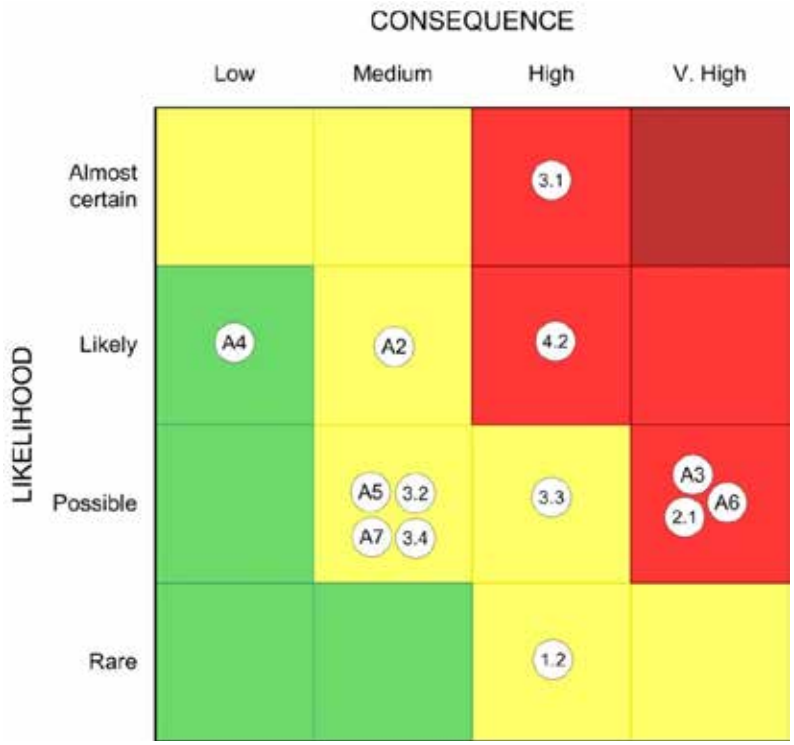
Southland DLE risk profiles

Heat maps

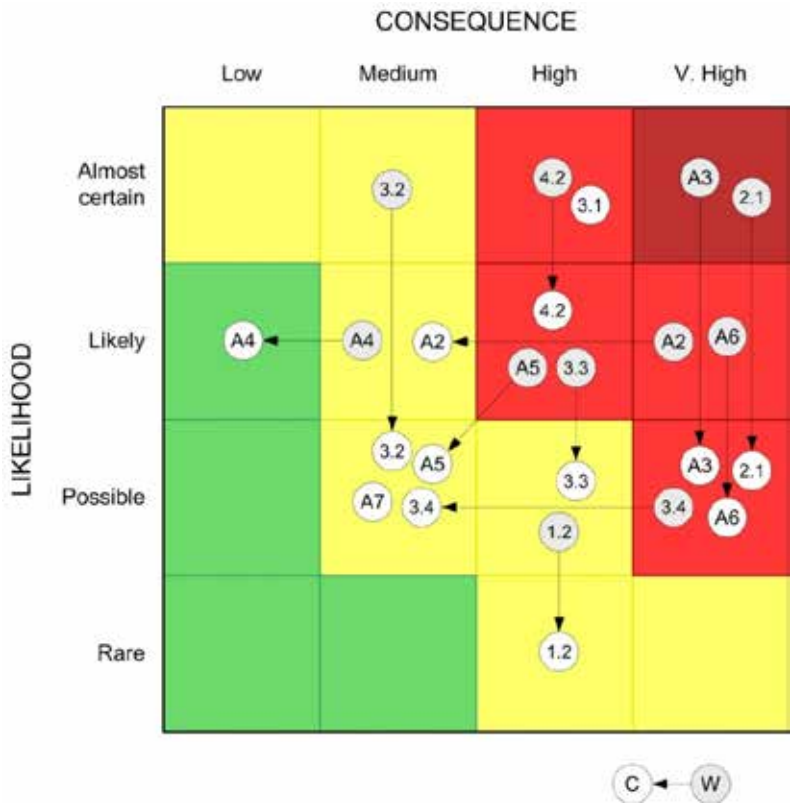
Southland DLE has mapped the combined consequences and likelihoods of risks in the risk register (page 44) on four different heat maps to represent the different ways risks can affect Southland DLE's objectives.



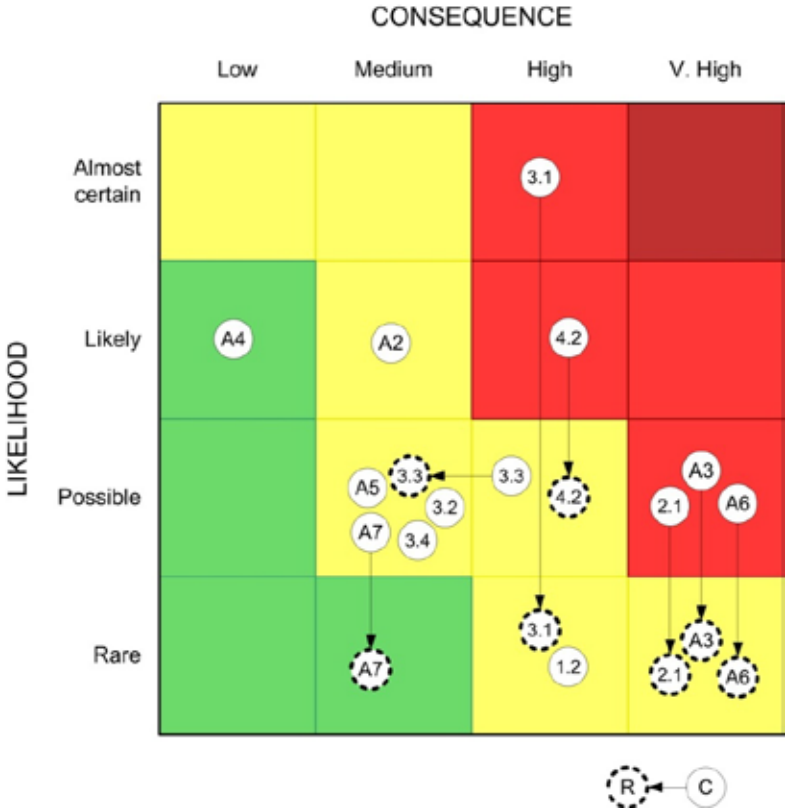
Risks affecting strategic objectives: worst case risk ratings



Risks affecting strategic objectives: current risk ratings



Risks affecting strategic objectives: comparison of worst case and current risk levels (for risks where only one symbol is shown, the current controls for the risk are non-existent or ineffective)



Risks affecting strategic objectives: comparison of current and residual risk levels (for risks where only one symbol is shown, the risk is acceptable/tolerable at its current level)

C	Current risk level
W	Worst case risk level
R	Residual risk level

Southland DLE risk profiles

Monitoring significant risks

Southland DLE considers significant risks to be those with a worst case risk level rated as extreme or major (where the consequence rating is very high).

Risk ID	Risk description	Impacts (consequence type)	Risk levels		Last assessed (date)	Risk owner	Monitoring mechanisms	Current status
			Worst case	Current				
1. Extreme risks								
A3	Ageing and obsolete IT infrastructure causes IT systems to be hacked, resulting in inappropriate use and loss of sensitive information	LEGAL/COMPLIANCE REPUTATION AND IMAGE FINANCIAL	Extreme	Major	March 2012	ADG CS	Reporting of firewall breaches to ADG CS	Month to end March 2012: three attempted breaches, none successful
2.1	Southland's inability to fill specialist analyst roles causes a new or emerging threat, e.g. cybercrime, to be overlooked, resulting in greater community concern about potential incidents	REPUTATION AND IMAGE SERVICE PERFORMANCE	Extreme	Major	March 2012	ADG SO	Monthly emerging threat assessment report to Exec Team	Month to end March 2012: no emerging threats identified

Risk ID	Risk description	Impacts (consequence type)	Risk levels		Last assessed (date)	Risk owner	Monitoring mechanisms	Current status
			Worst case	Current				
2. Major risks with a consequence rating of very high								
A2	Government response to changing community needs causes a mismatch between Southland DLE's organisational capability and service delivery requirements, resulting in negative impact for all Southland DLE objectives	SERVICE PERFORMANCE	Major	Moderate	March 2012	Comm.	Monitor government service delivery priorities	Priorities have not changed since release of last whole of government service delivery strategy (new strategy is due for release in September 2012)
A6	Increasing age of frontline officers and an imbalance between retirements and recruitments causes a skill shortage across frontline policing roles, resulting in the inability to provide frontline policing	SERVICE PERFORMANCE	Major	Major	March 2012	ADG CS	Report quarterly to Executive team on workforce retention statistics	Workforce retention statistics for quarter ending March 2012 will be tabled at May 2012 meeting
3.4	Lack of community understanding about the role of the '000' emergency hotline causes an increase in non-urgent calls, resulting in an increase in emergency call receipt times	SERVICE PERFORMANCE REPUTATION AND IMAGE	Major	Moderate	March 2012	ADG FO	Report quarterly to Executive team on call receipt statistics	Call receipt statistics for quarter ending March 2012: Calls received: 44,326 ñ Attended within 10 mins: 83% ó Non-urgent: 27% ñ