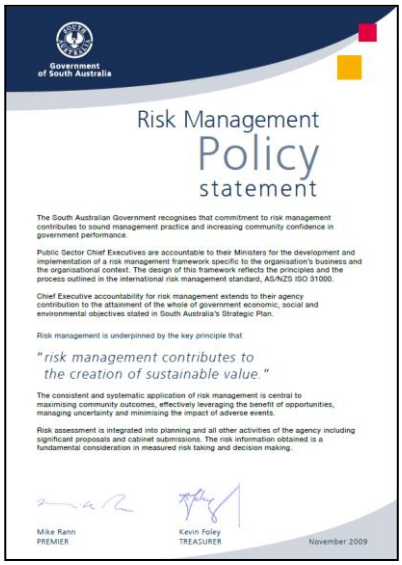
Risk Management Framework

Government of South Australia

Department for Communities and Social Inclusion

THIS PAGE INTENTIONALLY LEFT BLANK

Foreword


Government of South Australia

Risk Management Policy statement

The South Australian Government recognises that commitment to risk management contributes to sound management practice and increasing community confidence in government performance.

Public Sector Chief Executives are accountable to their Ministers for the development and implementation of a risk management framework specific to the organisation's business and the organisational context. The design of this framework reflects the principles and the process outlined in the international risk management standard, AS/NZS ISO 31000.

Chief Executive accountability for risk management extends to their agency contribution to the attainment of the whole of government economic, social and environmental objectives stated in South Australia's Strategic Plan.

Risk management is underpinned by the key principle that

"risk management contributes to the creation of sustainable value."

The consistent and systematic application of risk management is central to maximising community outcomes, effectively leveraging the benefit of opportunities, managing uncertainty and minimising the impact of adverse events.

Risk assessment is integrated into planning and all other activities of the agency including significant proposals and cabinet submissions. The risk information obtained is a fundamental consideration in measured risk taking and decision making.

Mike Rann
PREMIER

Kevin Foley
TREASURER

November 2009

The South Australian Government Risk Management Policy Statement 2009 advocates that consistent and systematic application of risk management is central to maximising community outcomes, deriving the benefit of opportunities, managing uncertainty and minimising the impact of adverse events.

Consistent with this policy the Department for Communities and Social Inclusion (DCSI) is committed to protecting itself, employees and others from situations or events that would prevent it from achieving its strategic goals and objectives. Risk management is an integral part of good management practice and the provision of safe workplace environments.

A systematic approach to managing risks and opportunities is more effective and efficient than allowing informal, intuitive processes to operate.

DCSI's adoption of a structured approach to risk management:

- defines a process for systematically managing the risk of all functions and activities in the organisation;
- encourages a high standard of accountability at all levels of the organisation;
- supports effective corporate and clinical governance systems and reporting mechanisms;
- encourages a high standard of efficient and effective client focused care and service delivery by taking advantage of opportunities for improvement; and
- allows the organisation to better meet its client and community demands.

It is everyone's responsibility to be involved in the identification, evaluation and treatment of risks and opportunities that could impact or influence outcomes for the organisation.

We trust this framework is useful in assisting you to integrate risk management into your role within the department.

Andrew Thompson
Executive Director
Financial Services

TABLE OF CONTENTS

Version 2.0
December 2012

1. Introduction

The purpose of this framework is to;

- define risk management;
- outline the department's risk management plan (Appendix 3);
- describe the approach to managing risks based on AS/NZS ISO 31000:2009 principles;
- outline guidance on the risk management process with a detailed context (Appendix 4);
- outline roles and responsibilities for risk management within the department; and
- explain the risk management recording and reporting requirements within the department.

Risk management is implemented in a manner consistent with three directive documents. They are:

AS/NZS ISO 31000:2009 Risk Management: Principles and Guidelines

The international risk management standard states that the success of risk management will depend on the effectiveness of the risk management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels. The framework;

- assists in managing the risks effectively through the application of the risk management process;
- ensures that the information about risks derived from the risk management process is accurately reported; and
- that the information is used as a basis for decision making and accountability at all relevant organisational levels.

(AS/NZS ISO 31000:2009)
Available at http://infostore.saiglobal.com
(Use of this reference material is subjected to copyright laws – DCSI can reproduce this document for internal use only)

Government of South Australia Risk Management Policy Statement

The Government of South Australia Risk Management Policy Statement 2009 states:

"risk management contributes to the creation of sustainable value"

> *'the South Australian Government recognises that commitment to risk management contributes to sound management practice and increasing community confidence in government performance'*

Further, the Risk Management Policy Statement indicates that the Chief Executive of the Department for Communities and Social Inclusion (DCSI) is accountable to the relevant ministers for the development and implementation of a risk management framework specific to the departments business and organisational needs.

The key principle which underpins this statement is that "risk management contributes to the creation of sustainable value".

(The Policy Statement is contained in Appendix 1)

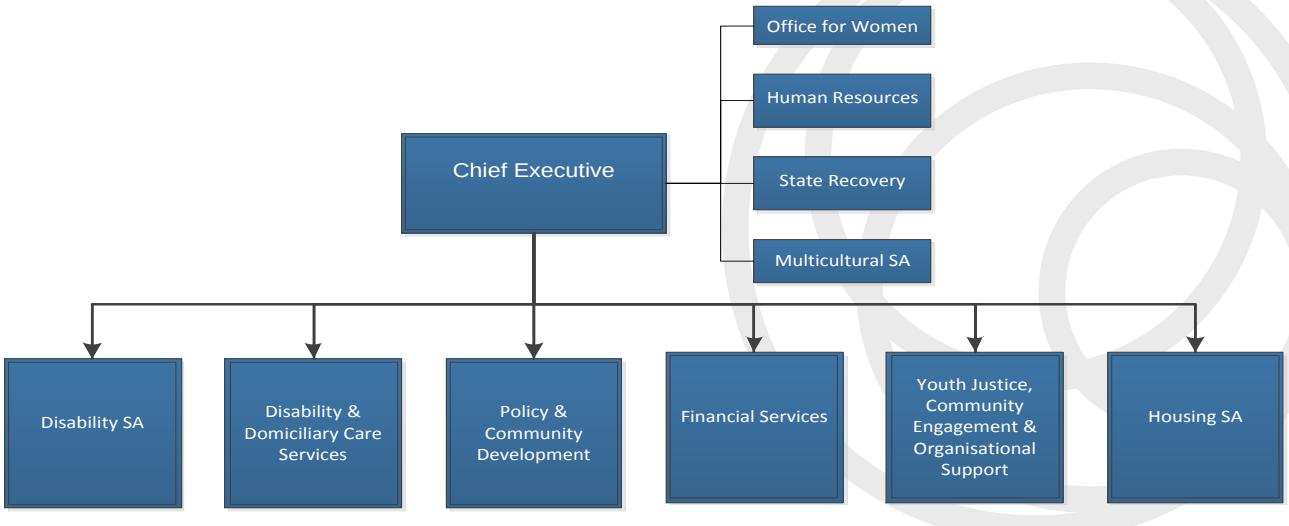
DCSI Risk Management Policy

The DCSI Risk Management Policy confirms the department's commitment to identify, assess and manage risks which may prevent the achievement of strategic goals and objectives. Risk management is regarded as an integral part of good management practice and the provision of safe workplace environments.

The policy directs that the department will integrate risk management into its culture, decision-making processes, programs, practices, business planning and performance reporting activities and will establish a safe working environment for its staff.

The DCSI Risk Management Policy is applicable to the whole of organisation as per organisational structure below:

(The policy is contained in Appendix 2)



2. What is Risk Management?

Risk management is about managing threats and opportunities.

AS/NZS ISO 31000:2009 describes risk as the

'effect of uncertainty on objectives'

When management of risks or opportunities is effective, it often remains unnoticed. When it fails, the consequences for clients and staff may be significant and politically high profile.

Having good risk management practice ensures that the department can undertake activities with the knowledge that measures are in place to maximise the benefits and minimise the negative effect of uncertainties on organisational objectives.

The risk management process is a "systematic application of management policies, procedures and practices to the activities of communicating and consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk". AS/NZS ISO 31000:2009

3. Risk Management Principles

Translating the AS/NZS ISO 31000:2009

The following table lists the principles identified in the AS/NZS ISO 31000:2009 standard which underpins effective risk management. The table provides a synopsis of what the principles mean to this department.

Along with this departmental approach, the South Australian High Performance Framework Characteristics and the Australian Business Excellence Framework Principles have also been aligned to demonstrate a holistic technique in achieving best practice

ISO 31000: Principles of Risk Management	How these principles apply to DCSI	How it aligns to	
		SAHPFC	ABEF
Risk management creates and protects value	Risk management contributes to DCSI pursuing its primary objective of meeting the needs of the most disadvantaged in the community by the application of best practice in governance, human resource and asset management and the identification of opportunities to improve the value of DCSI services to clients.	**2**	**2**
Risk management is an integral part of all organisational processes	DCSI incorporates risk management into business planning and processes across all levels of the organisation and ensures consideration is given to financial, social and environment factors.	**9**	**1**
Risk management is part of decision making	Decisions made in DCSI by individuals, teams, units and divisions through to the Executive Leadership Team have regard to risk information and knowledge that is accurate, timely and complete.	**1**	**9**
Risk management explicitly addresses uncertainty	The recording and reporting of risks within DCSI is clear and concise and is responsive to organisational change.	**5**	**7**
Risk management is systematic, structured and timely	The risk management process exists within the DCSI Governance Framework with a reporting structure that reflects corporate needs and local circumstances.	**3**	**4**
Risk management is based on the best available information	DCSI has rich data sources that are fostered by open channels of communication, allowing the highest level of information to be conveyed effectively to stakeholders.	**6**	**6**
Risk management is tailored	The whole of DCSI, its divisions, and all of its business units, work with risk management procedures that are tailored to meet their specific needs.	**10**	**1**
Risk management takes human and cultural factors into account	Consultation on the development and implementation of risk management ensures policies; frameworks and practices in DCSI reflect the diversity of activities of the organisation, its staff and its clients.	**7**	**8**
Risk management is transparent and inclusive	Risk management in DCSI involves the engagement of internal and external stakeholders through respectful acknowledgement of their contribution to the communication & consultation and monitoring & reviewing processes.	**8**	**4**
Risk management is dynamic, iterative and responsive to change	Risk management in DCSI responds to the changing needs of the organisation, its staff and its clients by continually self-assessing, monitoring and reviewing business processes against the South Australia's Strategic Plan. Education and training within DCSI is tailored to the needs of Divisions and Business Units.	**4**	**5**
Risk management facilitates continual improvement of the organisation	In DCSI the identification and application of controls and treatments as a result of robust risk assessments, including refinement, leads to improved business practices and increased maturity of the risk management process.	**4**	**3**

SA High Performance Framework Characteristics	
These characteristics state that high performing organisations:	
1	Are well led
2	Are built on clear values
3	Are strategic
4	Are innovative and continually improving
5	Use information and knowledge effectively
6	Engage their workforce and stakeholders
7	Are customer and citizen focused
8	Are accountable
9	Manage to the triple bottom line
10	Focus on results

The Australian Business Excellence Framework Principles of leadership and management	
1	Clear direction and mutually agreed plans enable organisation alignment and a focus on the achievement of goals.
2	Understanding what customers and other stakeholders value, now and in the future, enables organisational direction, strategy and action.
3	All people work in a system; outcomes are improved when people work on a system and its associated processes.
4	Engaging people's enthusiasm, resourcefulness and participation improves organisational performance.
5	Innovation and learning influence the agility and responsiveness of the organisation
6	Effective use of facts, data and knowledge leads to improved decisions.
7	Variation impacts predictability, profitability and performance.
8	Sustainable performance is determined by and organisation's ability to deliver value for all stakeholders in an ethically, socially and environmentally responsible manner.
9	Leaders determine the culture and value system of the organisation through their decisions and behaviour

4. The Approach to Managing Risks

The department is committed to maintaining and continuously improving an enterprise wide system that manages risks at a strategic and operational level.

This system is designed to complement the strategic plan and promotes:

"...there is considerable value in linking risk management to business objectives and planning processes."

Risk management as part of the organisation's culture:

- a culture that is not risk averse but is prepared to manage risks within an appetite that is set and reviewed by the Executive Leadership Team (ELT);
- a culture of enquiry, learning, reflection and trust to anticipate and objectively assess risks and opportunities associated with managing directions, services, processes, competencies, values and behaviours;
- a culture with channels of communication that are open, ethical, and improve connectivity across the department;
- a culture which continually adds value to departmental governance structure and client outcomes;
- a culture which commits to a robust business planning and reporting cycle which is inclusive of risk management principles.

"…..the nature of risk is that it is unpredictable…."

Visible focus on managing strategic risk emergence and uncertainty:

- demonstrated by exercising risk leadership by example and communicating the risk culture;
- modelling behaviours based on principles outlined in this framework;
- overseeing and understanding the interdependence of risks;
- ensuring competencies by supporting professional development and risk management education and training; and
- aligning resources with managing risks and opportunities

Full accountability for managing and reporting significant risks at all levels of the organisation (strategic and operational):

- managing the uncertainty associated with strategic risks
- creating predictability and operational reliability
- implementing cost effective treatments to reduce risks and exploit opportunities
- ensuring risk management is considered in all new projects, initiatives, business cases and cabinet submissions
- risk information and knowledge that is accurate, timely and complete to be integrated into an effective decision making process

Recording and Reporting of Risks

"……preventing foreseeable problems and issues from occurring."

The department uses an electronic tool (DCSI Risk Register) to record and maintain its risks, controls and treatments. It is a requirement for all business units within the department to have their risks, operational or strategic, recorded on the register. Reporting of risks, controls and treatments occurs on a quarterly basis. These reports are subject to a quality review process that ensures there is a consistent approach and language used across the department. The results are then reported to the Chief Executive and members of the ELT and Audit Committees. The Project Officer in the Risk Management function of Quality Assurance, Risk & Business Improvement Branch (QARBI) of Financial Services Division is the administrator of the register and also assists the Risk Assessment Facilitators (RAF) in maximising use of the electronic risk register to record and report the information.

Risk control management (sometimes also called control self assessment):

- designing methods and procedures as controls to manage risks;
- reduces the likelihood of potential problems occurring and limits the impact if they do
- monitor and reviews the effectiveness of controls

Limitations of risk management

In acknowledging the limitations of risk management in isolation, the department will be better prepared to embed risk management in everything we do. To demonstrate this, the AS/NZS ISO 31000:2009 principles have been aligned to the department approach and then further aligned with the high performance framework and the business excellence framework.

5. The Risk Management Process

There are key elements in the risk management process that need to be considered and are addressed below.

- Risk, control and treatment owners are required to liaise with the RAF for their area, and if required, other owners to ensure all elements of the risk management process are considered.
- Risk, control and treatment owners can either be individuals or a specified group although it is recommended that an individual is designated as the owner.

Risk Owner

"Owners are able to manage and allocate resources….."

- Risks in the strategic risk register must be owned by either the Chief Executive or an Executive Director.
- All other risks are owned by a person in the business unit who has the overall responsibility of the risk, e.g. Director, Manager.
- Risk owners have the authority to manage and allocate resources to manage the risk.
- Risk owners understand when risks require escalation to the next management level and when they should be retired.
- Risks owners are accountable for the acceptance of risks that are outside the parameters set by the department. These parameters are identified in the risk matrix. When a risk has been accepted in these circumstances, the risk owner is required to provide a documented explanation as to why the risk has been accepted as it stands.

Control Owner

- Control owners are able to effectively and efficiently manage and allocate resources when implementing a control.
- Control owners are expected to review their controls on a quarterly basis and ensure the control is up to date and operating as intended. Any updates to controls should be advised to the RAF.
- If a control requires a treatment(s), the control owner will liaise with the treatment owner(s) to ensure appropriate actions are undertaken to modify and strengthen the control.

Treatment Owner

- Treatment owners are able to manage and allocate resources to ensure that the treatment they are responsible for is actioned and completed within the time frame specified.
- Any updates to the treatments are to be advised to the RAF when they occur or at the time of quarterly reporting.

Types of risk

Within this department, 3 types of risks are considered. They are;

"……a strategic risk is simply a risk that has the ability to impact on the achievement of strategic objectives."

- **Strategic** – Risks that are associated with the strategic objectives of the department. These risks don't often change and are coupled with long term goals. The PESTLE analysis is helpful in identifying these risks.
- **Operational** – Risks that are related to the ongoing procedures of the department. They are either long or short term risks, depending on the objective that it relates to. This type of risk can occur on a regular basis however, the impact on the organisation as a whole is often minimal. The SWOT analysis is also useful in identifying these risks.
- **Project** – Risks that are linked to projects and programs that exist within the department and are generally captured using the Project Management Office system. They are medium to long term risks and don't require much change, however when elements of a project or program do change, the risks, controls or treatments may require review. Project risks that remain once the project or program reaches the transition to operational phase; need to be entered on the appropriate risk register to facilitate continuing monitoring and review. The SWOT analysis is useful to identify these risks.

Controls and Treatments / Actions

"Communication is key….."

When the ownership of a control or treatment used to manage a risk lies outside the department, further controls or treatments may need to be implemented to ensure that the original control or treatment is effective. Communication is crucial in these situations and relevant stakeholders must be considered and engaged in this process.

Controls and treatments can be linked to more than one risk and can be cross divisional or business unit e.g. a department policy can be a control to more than one division or business unit. However, the way one business unit may implement that policy might be different to another and therefore may create a treatment purely for its own use.

Risk Treatment / Action Plans

A treatment / action plan is put in place when either the current controls are ineffective or require improvement, or when no controls exist at all. Having no controls is unlikely in a government context.

Treatment plans comprise one or more actions that remedy identified issues or control weaknesses. When recording the treatment on the risk register, the description details who is doing what and what it is they are doing. Treatment plans may be generated from various business processes, including business plans, audit reports, action plans or simply in the risk register.

Key Stakeholders

Key stakeholders in the risk management process vary from executive level leaders, to management and frontline staff. These individuals may be allocated responsibility for individual risks, controls or treatments and are required to ensure information is accurate and up to date.

"Key stakeholders are critical to the risk assessment process….."

Executive Directors/Directors who are responsible for risk registers are responsible for the information contained in the quarterly reporting and are required to sign off that the information correct. RAFs are responsible for ensuring Executive Directors or Directors receive quarterly reports in a timely manner to ensure sufficient time to review the content.

Key stakeholders are critical to the risk assessment process as they provide fundamental knowledge and expertise when decisions are being made. It is the responsibility of all key stakeholders to understand and recognise who should be involved in the risk assessment process and ensure they are advised.

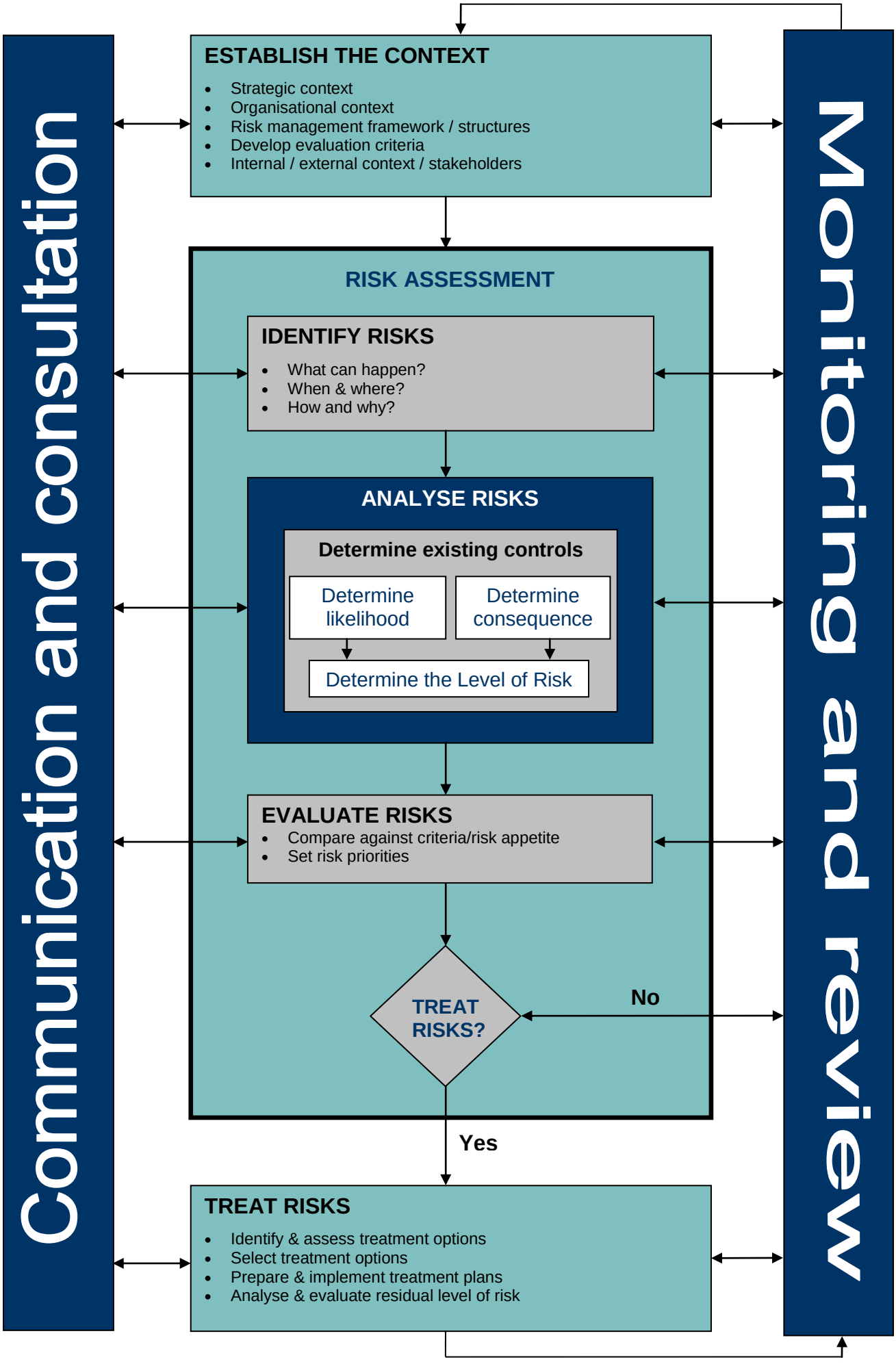
External stakeholders also need to be considered in the risk management process. These may included the Minister, members of Parliament, clients, other agencies, community groups, contractors, and volunteers.

Steps in the Risk Management Process

- Establish the context
- Identify the risks
- Analyse the risk
- Evaluate the risk
- Treat the risk
- Communication and consultation (this is a continual process)
- Monitoring and review (this is a continual process)

A diagram of the process is produced on the following page, and a detailed description of these steps can be found in Appendix 4.

The diagram below summarises the **Risk Management Process** (AS/NZS ISO 31000:2009)



6. Roles and Responsibilities

Informed and committed employees are the most important resource in implementing risk management successfully. An outline of the roles and responsibilities of staff is in the department's Risk Management Policy.

The following role profiles describe the resources available to support employees at all levels in the implementation of risk management.

Chief Executive

The Chief Executive is accountable to the Minister for the following:

"...enables better discussions with others who play a role in the mitigation of risk…"

- To establish and maintain a culture of risk awareness and intelligence;
- Ensure governance mechanisms effectively monitor risks and the way they are managed;
- Ensure employees receive support in fulfilling their responsibilities;
- Setting standards of best practice for risk management, based on the AS/NZS ISO 31000:2009; and
- Contribute to the attainment of whole of government economic, social and environmental objectives in the South Australian Strategic Plan.

Executives and Senior Management

Executive and Senior Management are required to:

- Demonstrate an understanding of and commitment to an integrated risk management system;
- Nominate influential and motivated team members to undertake the role of RAF;
- Support the RAF's professional development in risk management;
- Evaluate risks on a quarterly basis including relevance of risk, level of risk, effectiveness of existing controls, treatments and sign off as part of quarterly reporting process; and
- Undertake annual risk workshops as part of business planning process, incorporating fraud risk assessments.

Risk Assessment Facilitators (RAFs)

The role of the RAF requires that they:

- Promote local risk management awareness activities;
- Undertake competency based training and other risk management professional development;
- Facilitate quarterly reporting within their area of responsibility; and
- Facilitate annual risk workshop and ensure risk registers reflect outcomes.

Employees

- Actively support, report and contribute to the risk management process; and
- Maintain an awareness of the risks and opportunities that relate to their work group.

Risk Management

The risk management team is responsible to the Director, Quality Assurance, Risk & Business Improvement for:

- Developing, implementing and monitoring risk management policies and strategies;
- Providing expert advice, consultancy and recommendations on risk management; and
- Reviewing the department's risk management framework and monitoring its implementation.

The risk management team work with areas in the department to assist with the implementation of the Risk Management Policy and Framework, while providing training and support to Managers and the RAFs.

Internal Audit

"the internal audit program is risk-based…… "

The internal audit program is risk-based, consequently Internal Auditors, will consider the department's risk registers when developing annual audit plans and contribute to training of employees specifically around internal controls.

Risk Management and Audit Committees

The DCSI Risk Management and Audit Committee and South Australian Housing Trust (SAHT) Board Audit & Finance Committee monitor risk management within the department. The Committees;

- Assist the Chief Executive or SAHT Board in the identification of risks, determining priorities for action, and advise on developing and implementing strategies for effective risk management and ensuring accountabilities are met;
- Provide oversight of the risk management and internal audit functions of the department;
- Review and monitor the development and implementation of risk management principles across the department;
- Receive quarterly strategic risk management reports.

7. Recording and Reporting Requirements

Recording risk information that is concise, accurate and timely enables reports to be generated, which build corporate knowledge and contributes significantly to informed discussion on risk and uncertainty.

Executives and Senior Management

Formal risk assessments are to be undertaken as part of the annual business planning process.

"...ensure that reporting leads to actions…. That is identifying gaps and making sure we treat the gaps in a timely manner… "

Quarterly reporting demonstrates current timelines for assessment of control effectiveness and implementation of treatments.

The Divisions/Business Units of the department (through the Executive Director and ELT) shall provide information for reports to Audit Committees regarding risk registers and risk treatment plans.

Executives are required to report to the Audit Committees all key risks

- That are rated extreme/high at controlled or treated level of risk
- That may have an impact across other Divisions and / or Regions of the department.
- Where the action required to address the risk, requires a higher level of authority; and
- Risks deemed by executive to require higher level attention.

Risk Assessment Facilitators

Risk Assessment Facilitators will:

- Maintain up-to-date risk information for their Division/Business Unit using the DCSI Risk Register
- Assist in formal risk assessments undertaken when business plans are being developed.
- Facilitate reports to enable Directors to sign off on quarterly reports and forward them to Risk Management Unit.

Employees

All employees are expected to actively support and contribute to the recording and reporting of risks, through participation in risk assessment workshops when required and by discussing risks associated with their role with their RAF.

Risk Management

Risk Management will report quarterly on Strategic and Divisional risks, controls and treatments to Divisional Risk Management Committees and Housing Leadership Group meetings. Reports focus on matters arising, from new and emerging risks to the Department and work to be undertaken.

Internal audit

Internal Audit plans are developed to contribute to the assessment of the department's business processes and activities. Internal audits provide assurance to departmental executives regarding the identification of key risks, and the effectiveness of the control and management of those risks.

Risk Management and Audit Committees

The Committees report to the Chief Executive on any major risks or issues that are of continuing concern and ratify reports on activities and outcomes prepared by QARBI and Internal Audit for inclusion in the DCSI Annual Report as evidence of compliance with Government policy.

Risk Escalation Flowchart

This flowchart has been designed to demonstrate how risks are first identified and then recorded on the risk register. The flowchart illustrates how risks outside of the department's risk appetite are referred to senior management and executive. It should be noted that risks also can be downgraded. The flowchart is provided in Appendix 7.

Risk Management Reporting

"risk registers are maintained as living documents……. "

Risk reporting involves a structured process to record information at each stage of the risk management process. The department maintains a risk register via an electronic tool (DCSI Risk Register) which enables monitoring, review and prioritisation of risks. The risk register is based on the organisational structure and incorporates the strategic objectives. Currency of the risk register is the responsibility of the risk management team which supports RAFs on a needs basis and through formal training sessions. The risk register provides evidence of risks having been systematically identified, analysed and treated on a continuous basis by Divisions/Business Units. Risks may change regularly and without warning, so the registers should be maintained as a "living" database to accurately record the risk management process, effectiveness of internal controls and progress of risk treatments. Reports are submitted on a quarterly basis and are subject to a quality review process before being reported to ELT and the relevant committees.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDICES

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix 1 - SA Government Risk Management Policy Statement

Government of South Australia

Risk Management Policy statement

The South Australian Government recognises that commitment to risk management contributes to sound management practice and increasing community confidence in government performance.

Public Sector Chief Executives are accountable to their Ministers for the development and implementation of a risk management framework specific to the organisation's business and the organisational context. The design of this framework reflects the principles and the process outlined in the international risk management standard, AS/NZS ISO 31000.

Chief Executive accountability for risk management extends to their agency contribution to the attainment of the whole of government economic, social and environmental objectives stated in South Australia's Strategic Plan.

Risk management is underpinned by the key principle that

"risk management contributes to the creation of sustainable value."

The consistent and systematic application of risk management is central to maximising community outcomes, effectively leveraging the benefit of opportunities, managing uncertainty and minimising the impact of adverse events.

Risk assessment is integrated into planning and all other activities of the agency including significant proposals and cabinet submissions. The risk information obtained is a fundamental consideration in measured risk taking and decision making.

Mike Rann
PREMIER

Kevin Foley
TREASURER

November 2009

Appendix 2 – DCSI Risk Management Policy

Government of South Australia

Department for Communities and Social Inclusion

Risk Management Policy

Policy number:	RAL/137
Version:	2.1
Date of version:	March 2013
Applies to:	All DCSI staff
Implementation date:	Ongoing
Issued by:	Quality Assurance, Risk & Business Improvement (QARBI)
Delegated authority:	Jonathan Boyd, A/Director, QARBI
Policy custodian:	Brenda Head, Principal Risk Management Consultant
Due for review:	March 2014
Confidentiality:	C2: restricted internal
SA Strategic Plan:	T1.8

(See Notes below to complete table)

Intent

This policy describes the Department for Communities and Social Inclusion' (DCSI) responsibilities under the South Australian Government Risk Management Policy Statement: 2009

Context

The South Australian Government Risk Management Policy Statement 2009 (hereinafter referred to as Policy Statement: 2009) is based on the international standard AS/NZS ISO 31000:2009: Risk Management – Principles and Guidelines. The Policy Statement 2009 is explicit in asserting that "the consistent and systematic application of risk management is central to maximising community outcomes, effectively leveraging the benefit of opportunities, managing uncertainty and minimising the impact of adverse events".

In addition, the Premier's Declaration for Safety and Wellbeing in the Public Sector 2010 - 2015 outlines the requirement that all executives and managers are trained in risk management for the purpose of establishing integrated reporting systems.

Through this DCSI policy, the DCSI Risk Management Framework and supporting procedures, DCSI promotes a culture of enquiry, learning and trust to anticipate and assess risks and opportunities.

DCSI's assessment of risks associated with decision-making, business planning and practices and its performance reporting activities are fundamental to establishing a safe working environment.

This policy and the supporting Framework and Procedure documents are based on the principle that sound risk management enhances the agency's opportunities to achieve its goal to deliver better outcomes for the most vulnerable in the community.

Risk

This policy mitigates the risk that DCSI will not meet the obligations mandated for government agencies in the Policy Statement: 2009.

Failure to apply this policy would place in jeopardy the sound management of DCSI's extensive resources and the safe and secure management of its employees.

Reference Documents and Links

Directive Documents

- SA Government Risk Management Policy Statement Nov 2009
- Premier's Zero Harm Vision

- Premiers Declaration for Safety and Wellbeing in the Public Sector 2010 – 2015
- Chief Executive's Safety Commitment 2012
- WorkCover SA Performance Standards for Self Insured Employers April 2008

Supporting Documents
This document is to be used in conjunction with:

- DCSI Risk Management Framework (incorporating a glossary)

Related Documents and Resources

- AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines

Scope

This Risk Management Policy applies to all DCSI divisions, business units and agencies.

Definitions

Risk effect of uncertainty on objectives.

Risk Management coordinated activities to direct and control an organisation with regard to risk

Risk Management Framework is a set of information components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.

Policy Detail

Consistent with the international standard AS/NZS ISO 31000:2009 and Policy Statement:2009, DCSI is committed to maintaining and continuously improving an enterprise wide system that manages risks to protect itself, its employees and others from situations or events that would prevent the achievement of its strategic objectives.

DCSI will reduce its exposure to risk and optimise its opportunities by continuing to adopt a systematic and transparent approach to identification, analysis, evaluation and management of risks.

DCSI will create risk information and knowledge that is concise accurate, timely and complete, with clearly defined assumptions and limitations that support informed discussion on risks and opportunities across all of its functions, so that risks are clearly articulated, mitigated, monitored and reviewed.

DCSI will promote within business units consideration of risk in modifying behaviours or actions in the context of local needs and in consideration of the opportunities that might arise from different behaviours or actions being taken.

In DCSI, risk management will be a consideration in all initiatives and all project proposals.

Responsibilities:

The Chief Executive is "accountable to the Minister for the development and implementation of a risk management framework (based on the AS/NZS ISO 31000:2009: Risk Management – Principles and Guidelines) specific to the organisation's business and the organisational context". (SA Government Risk Management Policy Statement, 2009)

Executives and Senior Management are responsible for ensuring a systematic and integrated approach to risk management throughout their Division/Business Unit which complements the DCSI Policy and Framework.

Risk Assessment Facilitators (RAFs) are nominated by their Executive and Senior Management to assist with Divisional/Business Unit risk assessment workshops and quarterly reviewing of risks and promoting the integration of risk management throughout all business practices.

All staff are expected to have an awareness of the risks and opportunities within their work group and to actively support and contribute to the risk management system.

The Director Quality Assurance, Risk & Business Improvement (QARBI) is responsible for ensuring that the Risk Management Team work collaboratively with Executive, Senior Management and staff to assist with the implementation of the Risk Management Policy and Framework, and in providing advice, training and support to the Risk Assessment Facilitators.

DCSI Risk Management and Audit Committee and SAHT Board Audit & Finance Committee monitor risk management within DCSI and provide oversight of the functions of the Risk Management Unit. The Committees assist the Chief Executive in developing and implementing strategies for effective risk management and ensuring accountabilities are met.

Policy Approval

• ***Content Author:***	• **Delegated Authority***: (Director or authorised delegate)*	• **Executive***: (if required)*
• *Date:*	• *Date:*	• *Date:*
Name Brenda Head Position Principal Risk Management Consultant	Name Jonathan Boyd Position A/Director, Quality Assurance, Risk & Business Improvement	Name Andrew Thompson Position Executive Director Financial Services

Appendix 3 - DCSI Risk Management Plan

Element	Description	When	Who
Define scope and objective of business activities	Risk management will be incorporated into normal business activities including planning, decision making and operational processes, leading to the achievement of organisational goals.	Biennially	All staff
Risk Management Policy	Policy review is every year. This allows for any updates and organisational changes to be incorporated into the policy and keep the information as contemporary as possible.	Annually	QARBI
Risk Management Framework	A review every two years of the framework allows the organisation to continually improve its processes without deviating too far from the policy and procedures.	Biennially	Risk Management
Risk Assessments	Formal risk assessment workshops are to be undertaken as part of the annual business plan cycle, new initiatives, budget bids, cabinet submissions etc.	Annually	All Business Units/Divisions
Roles and responsibilities	Roles and responsibilities are reviewed on a quarterly basis during the reporting cycle. If responsibilities for risks, controls or treatments have changed, it will be reflected in the report.	Quarterly	All Business Units/Divisions
Training and education	The Manage Risk Course, Risk Awareness to Action Workshops and Business Development packages and presentations will be presented.	Bi-annually	Risk Management
Risk Management Reporting Process	RAFs, Directors and Executive Directors review risk registers on a quarterly basis. The Chief Executive is then provided with a memo outlining the results of the compliance program undertaken from the quarterly reporting process. Risk Management Committees, HLG and the ELT are then provided with reports outlining the results. Any feedback from these groups is then incorporated into the RMAC and SAHTBAF reports.	Quarterly	All Business Units/Divisions
Escalation process (Appendix 7)	Any risks that have a high or extreme controlled level of risk OR have controls rated as less than effective require treatment plans. If the treatment plan does not reduce the level of risk or increase control effectiveness, the risk is required to be escalated to management for further attention or authority to issue additional action. Management determines if the risk should be escalated further through to the Executive Director. The ELT review the risk and determine whether the risk is to be on the directorate or strategic risk register.	As required	All Business Units/Divisions
Risk treatment plans	Risk treatment plans exist where a risk has been rated as either extreme or high, or the control effectiveness has been rated as less than effective. These treatment plans are reviewed on a regular basis by the risk, control and treatment owners however are only reported on a quarterly basis.	Quarterly	All Business Units/Divisions
Compliance and testing	Quarterly declarations are submitted every three months and undergo a testing process to determine the quality of the report and the level of compliance.	Quarterly	Risk Management
Communication	Communication and consultation occurs on a regular basis to ensure key stakeholders (both internal and external) are consulted, engaged and actively involved throughout the risk management process. This promotes a consolidated awareness of the department's risk management system and influences behavioural shifts in relation to management of risks. The department has a risk management site which allows all staff to easily access information, tools (i.e matrix, control descriptors etc), manuals and templates. The department also has regular RAF forums to allow networking and sharing of information and experience relating to risk management.	Continually	All Business Units/Divisions
Monitor and review	This allows for lessons learned to be identified and applied to continuously improve upon the DCSI risk management framework and associated practices. This encourages and increases the successful achievement of strategic and business objectives.	Quarterly	All Business Units/Divisions

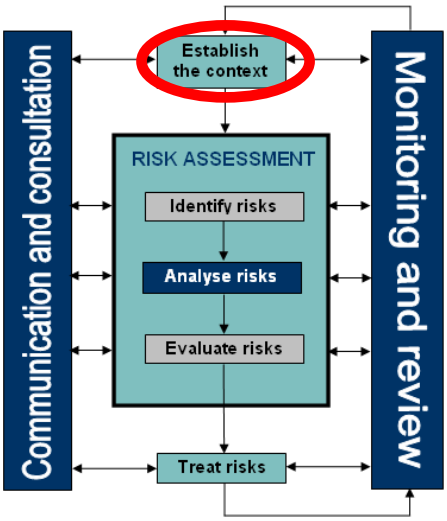
RAF (Risk Assessment Facilitator) **ELT** (Executive Leadership Team) **DCSI** (Department of Communities & Social Inclusion)
RMAC (Risk Management & Audit Committee) **HLG** (Housing Leadership Group) **QARBI** (Quality Assurance, Risk & Business Improvement
SAHTBAF (South Australian Housing Trust Board Audit & Finance Committee

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix 4 - Detailed Risk Management Process

(this is an excerpt from the RAF manual)

Establish the context



To establish the context of the work environment, relevant stakeholders must meet to determine what the objectives are and understand what the internal and/or external environment is eg. legal, cultural, political, socio-economical, physical and day to day aspects of an organisation's functions.

When the internal and external context is understood, the risk management context, or what it is that we are going to do, can then be established. The scope and boundaries of where the risk management process will be applied must be clearly defined, taking into consideration both the costs and benefits of risk management. For example, it is not good introducing a state of the art risk management initiative if it fails to support the organisations goal and objectives, or the organisation simply cannot afford to implement the initiative.

Key questions to ask when establishing the context may include:

(These questions can relate to Department, Division, business unit or even a particular team.)

External

- What is the Purpose/Mission/Objective/s of our business unit?
- What threats do you see that may affect the achievement of our business unit's goals and objectives?
- What opportunities do you see that could enhance the achievement of our business unit's goals and objectives?

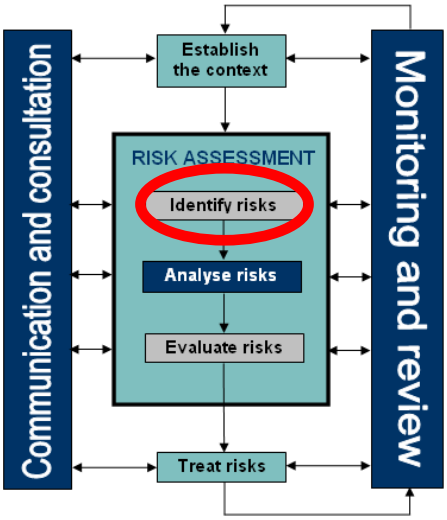
Internal

- What are the strengths and weaknesses of our business unit?
- Who are our internal and external stakeholders?
- How is our unit accountable to our stakeholders?

Sources and categories of risk, which is included in Appendix 5 also provides assistance in establishing the context. When considering the environment which risks will be identified, the basis from where a risk initiates it an important element in controlling and treating that risk.

Appendix 4

Identify the risks



This step is the first step of the risk assessment.

To identify risks, a list of potential things that could stop the organisation from achieving its goals must be developed.

This list should always be wide-ranging as unidentified risks can cause major losses through missed opportunities or adverse events occurring. 'Brainstorming' will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are considered to be the subject experts when considering potential risks to the objectives of the work environment and should be included in all risk assessments being undertaken. Key risks to the organisation/unit can then be identified and captured in the risk assessment worksheet

The sources and categories of risk template can be useful again in this step to determine which area the risk falls under. There may be more than one area that the risk effects.

When identifying risks, consider the following:

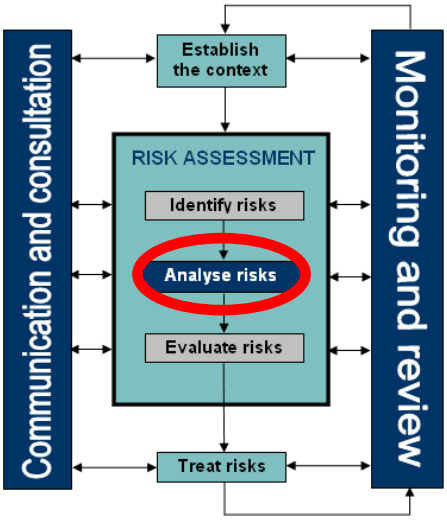
- What can happen
- Why will it happen
- Where will it happen
- When will it happen
- How will it happen

This step also is where opportunities for enhancement or gain across the organisation can be found.

Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

Appendix 4

Analyse the risk



The second step in the risk assessment is to analyse the risk. This means to understand the essence of the risk and determine the causes and consequences and to identify any existing controls.

Existing controls are things that are already in place such as policies, procedures, training programs etc. These controls require rating as either effective, requires improvement or ineffective.

Once this has occurred, the level of risk can be ascertained. This is done by using the risk assessment matrix. *(Appendix 6)*

The department has created a risk assessment matrix based on its '**risk appetite**' and what is and isn't acceptable within the organisational structure. The department has determined that it is not prepared to accept a controlled level of risk above moderate and therefore anything above that rating must have controls recorded as less than effective and have a treatment plan put in place.

However, there are circumstances where a high or extreme level of risk is not treated due to the financial impact and therefore remains at this level. Should this occur, an explanation from the risk owner is then required.

Risk descriptions – describe what the risk is, the cause of the risk and the consequences. As the risk description is only meant to be a short, contextual statement, the causes and consequences that are included should centre on the context that the risk is seen in.

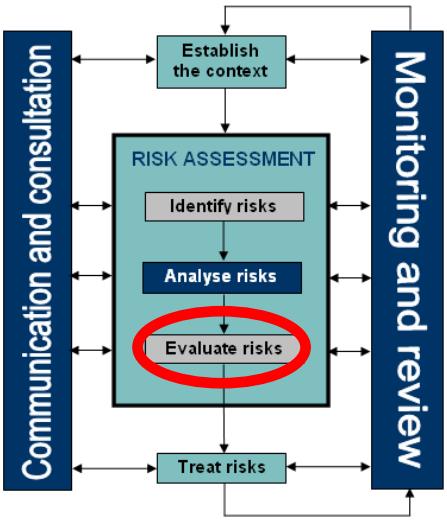
Control descriptions – describe what the control is, what it does, who performs it and how it is done. If the control is a process or task performed by a particular role (committee, unit or person), they must be named in the control description as the control owner is not always the person undertaking the process or task. Not every control will require every component; however, the description must reflect exactly how the control is working. If it requires improvement, the weakness of the control is also captured on the risk register.

Treatment descriptions – describe what the treatment is, what action is required and who performs the task. As with controls, the person undertaking the task is not always the treatment owner and therefore must be identified in the description.

Appendix 4

Evaluate the risk

Risk evaluation uses the information obtained during the analysis to make decisions about whether the risk is acceptable in its current state or whether further action needs to be taken to mitigate the risk.



Decisions regarding whether treatments need to be implemented are required and then the priority of those treatments is established.

To evaluate the risk, the departmental risk assessment matrix (Appendix 6) is used to determine the levels of risk at the inherent and controlled stages. The control effectiveness is also considered at this point and plays a part in the decision whether treatments are then required.

The Department has ascertained that:

- Any risk where controls are less than effective require a treatment plan
- Risks that are rated at the controlled level of risk as extreme or high must have controls rated as less than effective and therefore require a treatment plan
- Risks that are rated at the controlled level of risk as either moderate or low can be accepted and monitored. *(Provided that the controls have been assessed as effective)*

Some risks outside of the departments risk appetite may need to be accepted with ongoing review because the cost of treatment is not feasible. However, if this is the case, an explanation from the risk owner is required.

An accepted risk does not mean that the risk is insignificant, rather that:

- the inherent or controlled LoR is low/moderate and does not warrant using resources to treat it
- no treatment is available
- treatment costs are prohibitive
- opportunities significantly outweigh the threats

The departments risk appetite has been determined as below.

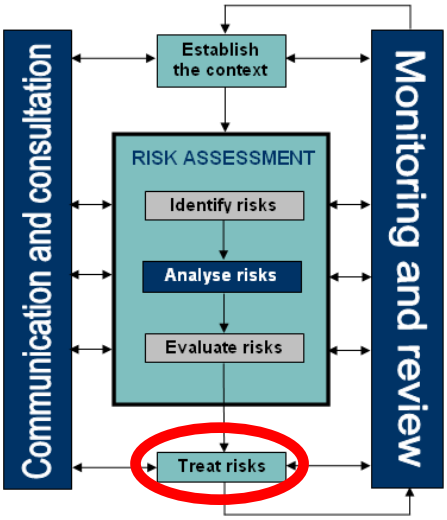
Risk Appetite

Action required when rating is at **controlled** level of risk

Extreme:	Immediate action required and commitment of senior management
High:	Senior management attention required and remedial action planned
Moderate:	Management responsibility must be specified & accountability defined
Low:	Managed by routine procedures such as quality management systems

Appendix 4

Treat / action the risk



Treating / actioning the risk involves selecting measures that contribute to either mitigating the risk or strengthening current controls.

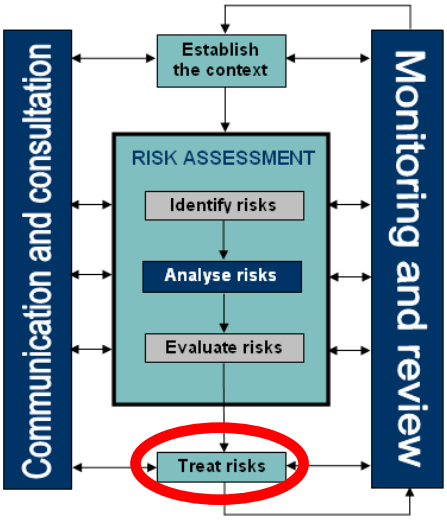
It is probable that a combination of options will be required to treat complex risks. The most suitable risk treatment / action options are generally identified as:

- Risk Acceptance:
  When all treatment options have been explored and there is no course of action likely to be effective or, the option will cost more than the benefits gained. It could also be when the risk is of low consequence and unlikely to occur, then it is appropriate to accept the risk. (this may require an explanatory note from the risk owner if the controlled level of risk is rated at extreme or high)
- Risk Retention:
  When after careful analysis of the risk, it cannot be avoided, reduced or transferred, or where the cost to do so is not justified.

  (this requires an explanatory note from the risk owner stating the situation and they are aware of the current status of the risk)
- Risk Avoidance:
  This is when stopping or not proceeding with the activity, or choosing an alternative, eliminates the risk. This is not often an option in the Public Sector.
- Risk Transfer:
  This is when the risk is transferred to other parties. This includes taking out insurance policies, outsourcing activities or moving operations to a better equipped part of the department that can handle the risk. In some cases, liability cannot be transferred as contractors may cap their level of liability and therefore responsibility remains with the Government.
- Risk Control (reduce the likelihood and/or consequence of the event):
  This is where the majority of effort is generally required in managing risk. Management processes such as audit and compliance programs, preventative maintenance, training of employees etc are some of the methods that will reduce the likelihood of risks being realised. Ensuring that controls are in place such as contingency plans, evacuation procedures or structural barriers, may reduce the consequences.

Appendix 4

Treat / action the risk (cont)



This element also incorporates evaluating the options, preparing treatment / action plans and implementation of those plans. The treatment plan may incorporate one or more of the above options and will document how chosen treatment options will be implemented.

Information that needs to be included in treatment plans are as follows:

- the name of the selected treatment
- treatment / action owner and those responsible for implementing the plan;
- what will be happening;
- when will it happen
- the original due date and the current due date (which can either be brought forward or go beyond the original date)

Treatment / action plans should be integrated with the risk management reporting process of the business unit and discussed with appropriate stakeholders.

Decision makers and other stakeholders need to be involved in determining the treated level of risk – which is the level of risk after the treatment / action, has taken place. The treated level of risk is recorded on the electronic risk register and is subjected to monitoring, review and, where appropriate, further treatment / action.

(examples can be found in the RAF Manual)

Further, treatment / action plans can be implemented by management through recommendations provided by internal audit following a review.

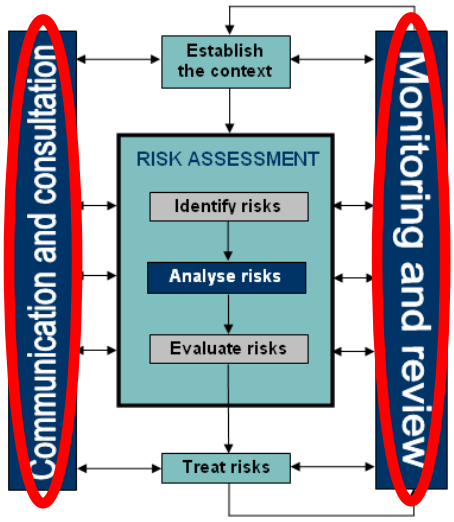
Appendix 4

Two ongoing themes are constant throughout the risk management process, these are:

Communication and consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk, and those with a vested interest, understand the basis on which decisions are made and why particular treatment / action options are selected or the reasons to accept risks have changed.

Monitoring and review



It is essential to monitor and review the management of risks as changing circumstances may result in some risks increasing or decreasing in significance. By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, we can determine if the organisations resources are being put to the best use possible.

During the quarterly reporting process, management are required to review any risks within their area and follow up on controls and treatments / action that are mitigating those risks. This allows them to identify any action that is out of date and requires further attention

It is also the time when completed treatments can be converted to controls, levels of risk are confirmed and the retirement or escalation of risks is implemented.

Monitoring and the reviewing of risks, controls and treatments also applies to any actions / treatments to come out of an internal audit. The audit report will provide recommendations that effectively are treatments for controls and risks that have been tested during an internal review.

- Retiring a risk

  Retirement of a risk occurs when the organisation no longer considers the risk relevant, in existence or has mitigated it to a point where the risk has been accepted. However, this can only be when the controlled level of risk is either moderate or low.

  Risks are retired for a variety of reasons can be reactivated should there be a change in the organisational objectives or its internal/external environment.

  Retired risks are not deleted from the risk register but may be archived after a period of time.

Appendix 5 - Risk Categories and Potential Sources of Risk

Best practice in risk identification requires the categorisation of risks. Each risk/opportunity identified in the Department will be classified into one of the risk categories that define business activity. If a risk has aspects that relate to more than one category, the predominant category is recorded on the risk register

This list is not conclusive & indicates only some examples of potential sources of risk

Risk Category		Examples of Potential Sources of Risk	
1	Leadership & Strategic Planning	• Political environment • Leadership and management processes • Government involvement and directions • Ministerial processes • Parliamentary processes and requirements • Financial requirements and conditions	• Strategic, divisional & business unit planning & reporting • Corporate practices • Protective security • Business continuity and disaster response
2	Knowledge Management / Information Technology	• Business continuity and disaster response • Procurement • Legal compliance • Protective security	• Records management • Business continuity and disaster response • Advancement in technology
3	Partnerships / Stakeholder (Working Together)	• Client and stakeholder relationships • Organisational relations (internal & external) • Government collaborations	• Peak bodies and various groups • Communications
4	Customer Service	• Specific client needs • Promulgation of information to clients	• Evaluation and feedback • Economic value of service
5	Asset & Facility Management	• Policies & procedures • Legal and financial requirements • Assets, development and maintenance	• Business continuity and disaster response • Protective Security
6	Legal Compliance	• Legislative requirements • Legal and governance obstructions • Industry regulations and standards	• Legal liabilities • OHS&W • Departmental guidelines
7	Procurement & Contract Management	• Policies and procedures • Financial management • Contractual agreements • Contract specifications	• External, outsourced functions • Asset management • Resource availability • Transparency & dispute resolution
8	Human Resource Management	• Managerial responsibilities • Policies & Procedures • Legislative requirement • Recruitment and allocation of resources	• Workforce and succession planning • Staff recognition & dispute resolution • Ethical and Professional conduct
9	OHS&W	• Governance and legal requirements • Policies and procedures	• Injury management & response • Incident management and documentation
10	Finance	• Policies and procedures • Financial management	• Legislative & industry requirements • Legal costs
11	Project Management	• Project Management Framework compliance • Project Management Office requirements	• Skilled resources
12	Clinical / Practice	• Policies & procedures • Safety & quality • Direct client care • Informed consent • Adverse events	• Privacy & confidentiality • Resource allocation • Training & credentialing of clinicians /practitioners • Documentation
13	Fraud & Corruption	• Policies & procedures • Control breakdown • Protective security	• Procurement & contract management • Illegal activity

Appendix 6 - DCSI Risk Assessment Matrix

RISK ASSESSMENT MATRIX

Risk Likelihood and Consequence Matrix

	5 - Catastrophic	4 - Major	3 - Moderate	2 - Minor	1 - Insignificant
5 - Almost Certain	Extreme	Extreme	High	High	High
4 - Likely	Extreme	High	High	Moderate	Moderate
3 - Possible	High	High	Moderate	Moderate	Low
2 - Unlikely	High	Moderate	Moderate	Low	Low
1 - Rare	Moderate	Moderate	Low	Low	Low

Risk Appetite

Action required when rating is at **controlled** level of risk

Extreme: Immediate action required and commitment of senior management

High: Senior management attention required and remedial action planned

Moderate: Management responsibility must be specified & accountability defined

Low: Managed by routine procedures such as quality management systems

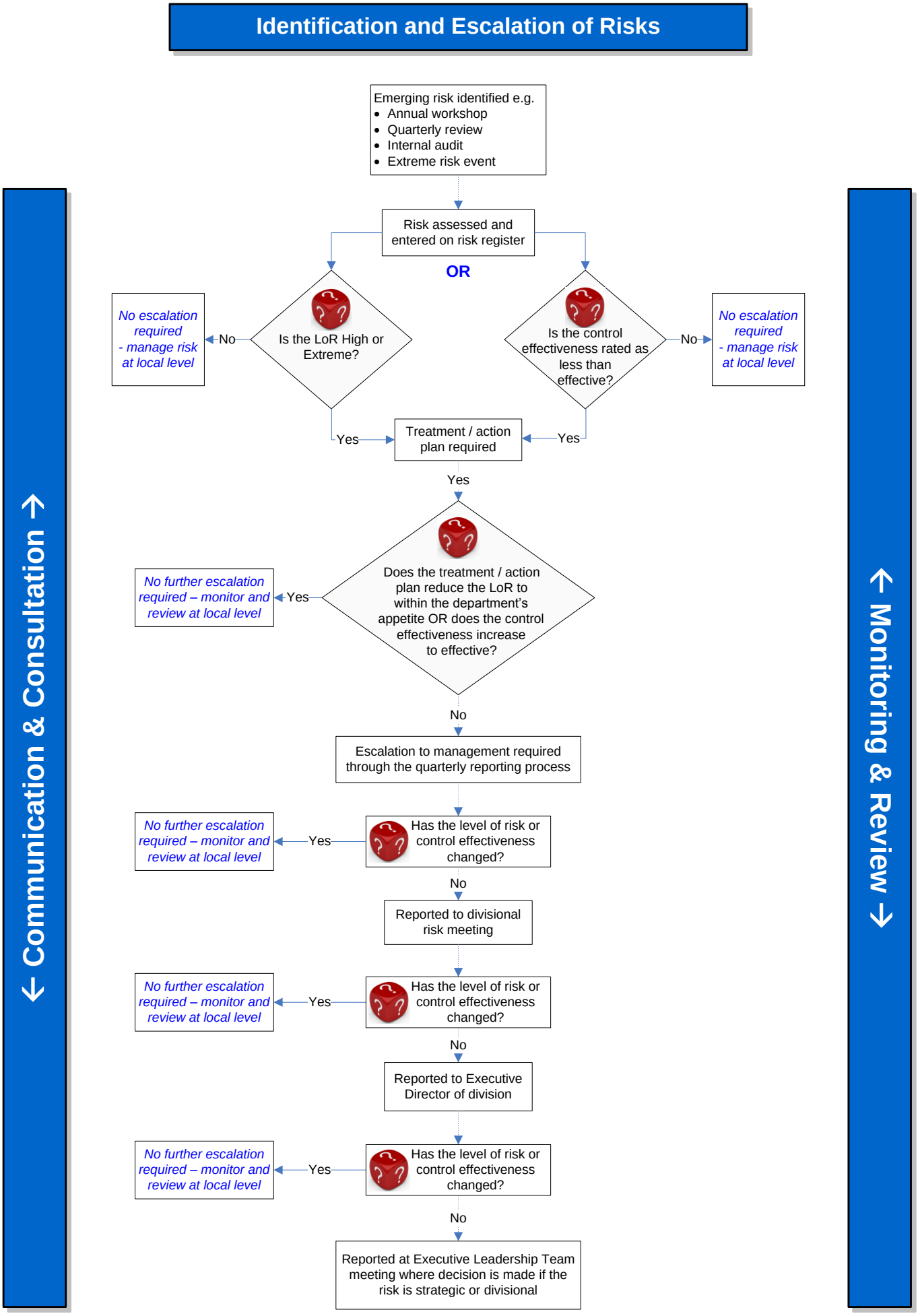
Risk Likelihood Descriptors

Level	Descriptor	Indicators (Choose one only)		
		Qualitative	Quantitative	Quantitative
5	Almost Certain	Expected to occur in most circumstances	Daily To Weekly	90 -99% certainty of occurrence
4	Likely	Will probably occur in most circumstances	Monthly To Six Monthly	70 -89% probability of occurrence
3	Possible	Could occur at some time	Annually	30 - 69% probability of occurrence
2	Unlikely	Unlikely in the foreseeable future	Once in 5 Years	10 - 29% probability of occurrence
1	Rare	Occurrence requires exceptional circumstances	Once in 10 Years	1-9 % probability of occurrence

Revised December 2011

	Impact Categories					
	Client	**OHS**	**Human Resources**	**Organisational**	**Reputation & Image**	**Financial**
Insignificant	• Near miss, no injury • No increase in care • Non-essential item affected not likely to result in injury or medical treatment being required	• Incident report or first aid treatment required	• Minor local workforce disruption • Loss of continuity of staff knowledge	• Business unit work plans delayed • Some delay in divisional business objectives • Some impact on normal operations within division • Reduced organisational efficiency in business unit	• One off negative reporting in media • Unresolved complaint resulting in dissatisfaction/ frustration	• Negligible financial loss or over expenditure within cost centre • Requires monitoring and corrective action within existing cost centre budget
Minor	• Increase level of care/monitoring • Some services to customers are delayed • Essential item affected may result in a minor injury or medical treatment being required	• Lost time injury (less than 5 working days)	• Local and temporary poor morale • Skill mix issues • Temporary loss of some of the business unit's workforce • Loss of staff continuity requiring recruitment	• Business unit work plans will not be achieved • Divisional business objectives delayed • Some impact on normal operations across several divisions • Significantly reduced organisational efficiency across business units • Some non-mission critical activities suspended/cease	• Temporary negative impact on reputation • Some negative reporting in media • Unresolved complaint leading to external investigation	• Minimal financial loss or over expenditure within cost centre • Requires some redistribution of existing business unit/divisional budget
Moderate	• Permanent decline of physical ability • Increased dependency • Some services not delivered to customers • Some major departmental services to customers delayed • Potential exposure to a hazard that may result in injury requiring a minor operation	• Lost time injury greater than 5 working days • Single non conformance from WorkCover evaluation resulting in financial penalties and administrative controls • SafeWork SA intervention due to non compliance with legislation, regulations or codes requiring a Default Notice and leading to the issuing of an Improvement Notice	• Widespread morale issues. • Industrial disputations affecting specific groups • Temporary loss of some of the Divisional workforce • Loss of key staff with specific knowledge and skills • Impact on recruitment capacity as an employer of choice	• Divisional business objectives will not be achieved • Departmental strategic objectives delayed • Significant disruption to operations across DCSI • All non-mission critical activities suspended/cease	• Temporary breakdown in key relationship • Widespread negative reporting in media • Premier or Ministerial involvement • Prosecution of a staff member	• Some financial loss or overrun of business unit/divisional budget • Requires significant redistribution of existing divisional budget
Major	• Death unrelated to natural course of life • Increased long term dependency • Requires hospitalisation • Some major Departmental services to customers cease • Exposure to an immediate hazard that may result in injury requiring significant medical treatment or death	• Hospitalisation, Dangerous Occurrence, Notifiable Work related injury/illness/death • Multiple non conformances from WorkCover evaluation leading to financial penalties and stringent administrative controls • SafeWork SA intervention due to non compliance with legislation, regulations or codes leading to the issuing of multiple Improvement Notices	• Entrenched severe morale problems • Inability to recruit employees with necessary skills • High employee turnover and significant industrial disputation	• Some departmental strategic objectives will not be achieved. • Reduced ability to deliver strategic outcomes • Some mission critical activities cease	• Ongoing widespread negative reporting in media • High-level independent investigation with adverse findings • Department being sued/prosecuted	• Significant financial loss or overrun of divisional budget • Requires significant additional funding, or redistribution of departmental budget or termination and/or reduction of other initiatives
Catastrophic	• Multiple Deaths unrelated to natural course of life • All Departmental services to customers cease • Exposure to an immediate hazard that may result in multiple deaths	• Multiple deaths • SafeWork SA intervention due to non compliance with legislation, regulations or codes leading to the issuing of a Prohibition Notice or prosecution	• Loss of a majority of departmental workforce • Inability to replace critical services	• All departmental strategic objectives will not be achieved. • Threatens ongoing existence of the department • Strategic outcomes unachievable • All mission critical activities cease	• Total loss of community confidence in DCSI and with the Government • Class action	• Extensive financial loss or over overrun of business unit/ divisional budget • No capacity to seek additional funding • Funding exhausted due to mismanagement or misappropriation

Appendix 7 - DCSI Risk Escalation Flowchart



Appendix 8 - DCSI Risk Management Glossary

TERMS & DEFINITIONS

Client Risk Management: An approach to improving the quality and safety of delivery of care to clients by placing special emphasis in identifying circumstances that put clients at risk of harm and acting to prevent or control those risks.

Clinical Governance: The system by which the governing body, managers and clinicians share responsibility and are held accountable for consumer care, minimising risks to clients and for continuously monitoring and improving the quality of clinical care. Ensure accountability structures are in place to manage performance issues.

Control: The process designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The process is affected by leadership, management and all involved staff.

Control Owners: The owners of a control process that mitigates an identified risk. Where controls are evaluated as "requiring improvement" or "not effective", the control owner will participate in developing a treatment to ensure the effectiveness of the control.

Corporate Governance: For the Public Sector there is a very broad coverage including how an organisation is managed its corporate and other structures, its culture policies and strategies and the way it deals with its various stakeholders.

Good governance is important to provide adequate accountability to the many stakeholders and to encourage performance improvement while satisfying control and compliance requirements.

External Context: The external environment in which the organisation seeks to achieve its objectives (i.e. **P**olitical, **E**conomical, **S**ocio-**E**conomical, **T**echnological, **L**egislative and **E**nvironmental aspects).

Hazard: A source of potential harm.

Incident: An unplanned and unexpected event (including a near miss). It may or may not result in an injury or illness to a person or damage to an asset/property.

Risk Event: The occurrence of risk. The risk may occur as a once off event or may continue to occur as an ongoing event.

Internal Context: The environment in which the organisation seeks to achieve its objectives (i.e. **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats).

Level of Risk (LoR): The magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

- **Inherent LoR:** The level of risk before existing risk controls are considered or existing controls fail (lose effectiveness)
- **Controlled LoR:** The current level of risk with controls in place.
- **Treated LoR:** The projected level of risk whilst treatments are being implemented. The controlled level of risk should be revised as treatments are completed.

TERMS & DEFINITIONS

Quarterly Declarations: Quarterly review of strategic and divisional risks with declaration statement attached to maintain a historical record of risk registers by respective Divisions/Business Units that may be subject to future audits.

Resilience: Capacity of an organisation or individual to resist being affected by an event/incident.

Risk: Effect of uncertainty on objectives

Risk Acceptance: Form of risk treatment when there is an informed decision to take a particular risk.

Risk Aggregation: A process to combine individual risks to obtain a more complete understanding of risk

Risk Analysis: Process used to understand the nature of risk and to determine the level of risk.

Risk Assessment: Process of risk identification, risk analysis and risk evaluation.

Risk Appetite: The amount and type of risk that an organisation is prepared to pursue, retain or take – this is illustrated by the risk assessment matrix

Risk Aversion: Attitude to turn away from risk.

Risk Avoidance: Form of risk treatment where there is a decision not to be involved in, or to withdraw from, an activity based on the level of risk.

Risk Criteria: Terms of reference against which the significance of a risk is evaluated.

Risk Description: A short statement using the formula Risk Name due to Cause results in Consequences.

Risk Evaluation: Process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable.

Risk Financing: Form of risk treatments involving budgetary arrangements to meet the financial costs should a risk occur.

Risk Identification: Process of finding, recognising and describing risks.

Risk Management: Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Framework: Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.

Risk Management Process: Systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Assessment Matrix: The tool for ranking and displaying risks by defining ranges for likelihood and consequence.

Risk Mitigation: Measures taken to reduce/treat an undesired consequence.

TERMS & DEFINITIONS

Risk Owner: Person or entity with the accountability and authority for managing the risk and any associated risk treatments.

Risk Register: A set of identified risks, controls and treatments (also known as Risk Profile).

Risk Retention: Form of risk treatment where there is acceptance of the benefit of gain, or burden of loss, from a particular risk.

Risk Sharing: Form of risk treatment involving the agreed distribution of risk with other parties.

Risk Source: Anything which alone or in combination has the intrinsic potential to give rise to risk.

Risk Tolerance: An individuals or organisation's readiness to bear the risk after risk treatments in order to achieve its objectives.

Risk Transfer: Move the liability for the risk to another party or share the risk (contracting, outsourcing, insuring)

Risk Treatment / Action: Process of selection and implementation of measures to modify risk

Stakeholder: *(Internal and External)* Any person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Treatment / Action Owners: Treatment owners are responsible for the implementation of treatments. Treatment owners should agree the treatment design, resourcing and agree timeframes for implementation with Directors, Risk owners, and possibly Control owners.