Government of South Australia
Department for Communities and Social Inclusion

Risk Management Framework

Quality Assurance Risk and Business Improvement

Contents	Page

Version	1.1
Date of Review	January 2018
Classification	FOUO (For Official Use Only)

1 Foreword

The South Australian Government Risk Management Policy Statement advocates that consistent and systematic application of risk management is central to maximising community outcomes, 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, its employees and others from situations or events that would prevent it achieving its strategic goals and objectives. Risk management is an integral part of good management practice and the provision of a safe workplace.

A systematic approach to managing risks and opportunities is more effective and efficient than allowing informal, intuitive processes to operate. DCSI's structured approach to risk management:

- Defines a process of systematically managing risk in all functions and activities in the organisation;
- Encourages a high standard of accountability at all levels of the organization;
- Supports effective governance systems and reporting mechanisms;
- Encourages a high standard of efficient and effective customer focused care and service delivery by taking advantage of opportunities for improvement;
- Allows the organisation to better meet its client and community demands.

It is everyone's responsibility to be involved in identifying, evaluating and addressing risks and opportunities that could impact the outcomes for our organisation. We trust this framework is useful in assisting you to integrate risk management into your role within DCSI.

Joslene Mazel

Chief Executive

2 The purpose of this framework is to:

- Define risk management;
- Outline the department’s risk management plan;
- 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;
- Outline roles and responsibilities for risk management, and
- Explain the department’s risk management recording and reporting requirements

Risk management is implemented in a manner consistent with three directive documents, namely,

- The Australian Standards AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines
- The Government of South Australia Risk Management Policy Statement’ and
- The Department for Communities and Social Inclusion Risk Management Policy.

2.1 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 risks;
- Ensures that the information about risks is accurately reported; and
- Ensures that the information is used as a basis for decision-making and accountability throughout the organisation.

2.2 SA Government Risk Management Policy Statement

The SA Government Risk Management Policy Statement states:

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

This Statement indicates that the Chief Executive of the Department for Communities and Social Inclusion (DCSI) is accountable to the Minister for the development and implementation of a risk management framework specific to the department’s business and organisational needs. The key principle which underpins this statement is that:

'Risk management contributes to the creation of sustainable value'

2.3 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 and the provision of safe work environments.

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

The DCSI Risk Management Policy is applicable to the whole of the organisation.

3 What is Risk Management?

Risk management is about managing threats and opportunities. The Australian Standard 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 high profile.

Good risk management practice ensure that the department can undertake activities confident that measures are in place to maximise the benefits and minimises the negative effect of uncertainties on organisational objectives.

Risk management 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'

4 Risk Management Principles

Translating the AS/NZS ISO 31000:2009 and acknowledging the 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 departmental approach and then further aligned with the high performance framework and the business excellence framework. This is shown in Tables 1 - 3 on pages 7 and 8:

- Table 1 lists the 11 principles identified in the AS/NZS ISO 31000:2009 Standard that underpin effective risk management. The table provides a synopsis of how these principles apply to DCSI;
- Table 2 lists the 10 South Australian High Performance Framework Characteristics (SAHPFC); and
- Table 3 lists the 9 Australian Business Excellence Framework (ABEF) Principles.

Table 1

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 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

Table 2

SA High Performance Framework Characteristics (SAHPFC)	
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

Table 3

The Australian Business Excellence Framework Principles of leadership and management (ABEF)	
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 an 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

5 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:

Risk management as part of the organisation's culture

DCSI is committed to a culture that is risk aware. The Executive Leadership Team works closely with the Risk Management team and key Risk Assessment Facilitators to strengthen our commitment to:

- 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 customer outcomes;
- A culture which commits to a robust business planning and reporting cycle which is inclusive of risk management principles;
- A culture where commitment to an annual risk management workshop results in an updated strategic risk register and risk assessment matrix.

Visible focus on managing strategic risk emergence and uncertainty

- 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)

An enterprise wide risk management system will promote full accountability for managing all risks (strategic and operational). The system will encourage a high standard of efficient and effective customer focused service delivery and:

- Provide a holistic approach to managing the uncertainty associated with strategic risks;
- Create predictability and operational reliability;

- Allow for the implementation of cost effective treatments to reduce risks and exploit opportunities;
- Ensure risk management is considered in all new projects, initiatives, business cases and cabinet submissions;
- Enable risk information and knowledge that is accurate, timely and complete to be integrated into an effective decision making process.

Recording and Reporting of Risks

The department uses an electronic tool (DCSI Risk Register) to record and maintain its risks, controls and treatments. All business units must 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, members of the ELT and audit committees.

The Project Officer, Risk Management, Quality Assurance, Risk & Business Improvement (QARBI), Financial and Business Services, 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)

Risk Controls reduce the likelihood of potential problems occurring and limits the impact if they do and are identified as part of the risk management process. Control Self-Assessment (CSA) is a key risk management process used to verify the adequacy and operational effectiveness of risk controls. CSA is a systematic process, which includes:

- Reviewing work processes and risk controls
- Designing methods and procedures as controls to manage risks
- Monitoring the adequacy and effectiveness of controls.

6 The Risk Management Process

There are key elements in the risk management process that need to be considered. 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 be either individuals or a specified group (although it is recommended that an individual be designated as the owner).

Risk Owner

- 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 above the recommended controlled level of risk. The Department's risk appetite at a controlled level is moderate to low.

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.

The risk owner will provide a documented explanation when a risk is accepted at a controlled level that is extreme or high. These risks will be reported to the Executive Leadership Team and require the endorsement of the Chief Executive.

Types of risk

Within this department, there are three types of risks to be considered. They are:

1) *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.
2) *Operational* – Risks that are related to the ongoing procedures of the Department. These are either long or short-term risks, depending on the objective. 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.

3) *Project* – Risks that are linked to projects and programs within DCSI are generally captured using the methodology contained in the DCSI Project Management Framework. Information and communication to relevant stakeholders is imperative, including status updates and the project risk register. When elements of a project change, the risks, controls or treatments should be reviewed.

If a project and associated risks are deemed by senior management or executive as extreme, high or are determined to have a strategic or operational impact that is above the Department's risk appetite then a project risk may be moved to the Department's risk register when it is still in its initial stage.

However, in most situations 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

When the ownership of a control or treatment used to manage a risk lies outside the department, further controls or treatments may be needed to ensure 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 are linked to risks, e.g., a department policy can be a control to more than one division or business unit.

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.

Treatment plans comprise one or more actions that remedy identified issues or control weaknesses. When recording the treatment on the risk register, the plan details who is doing what and what they are doing.

Key Stakeholders

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

Executive Directors/Directors are responsible for the information contained in quarterly reporting and are required to sign off that the information is correct. RAFs are responsible for ensuring Executive Directors or Directors receive quarterly reports in a timely manner with 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 important to identify who should be involved in the risk assessment process.

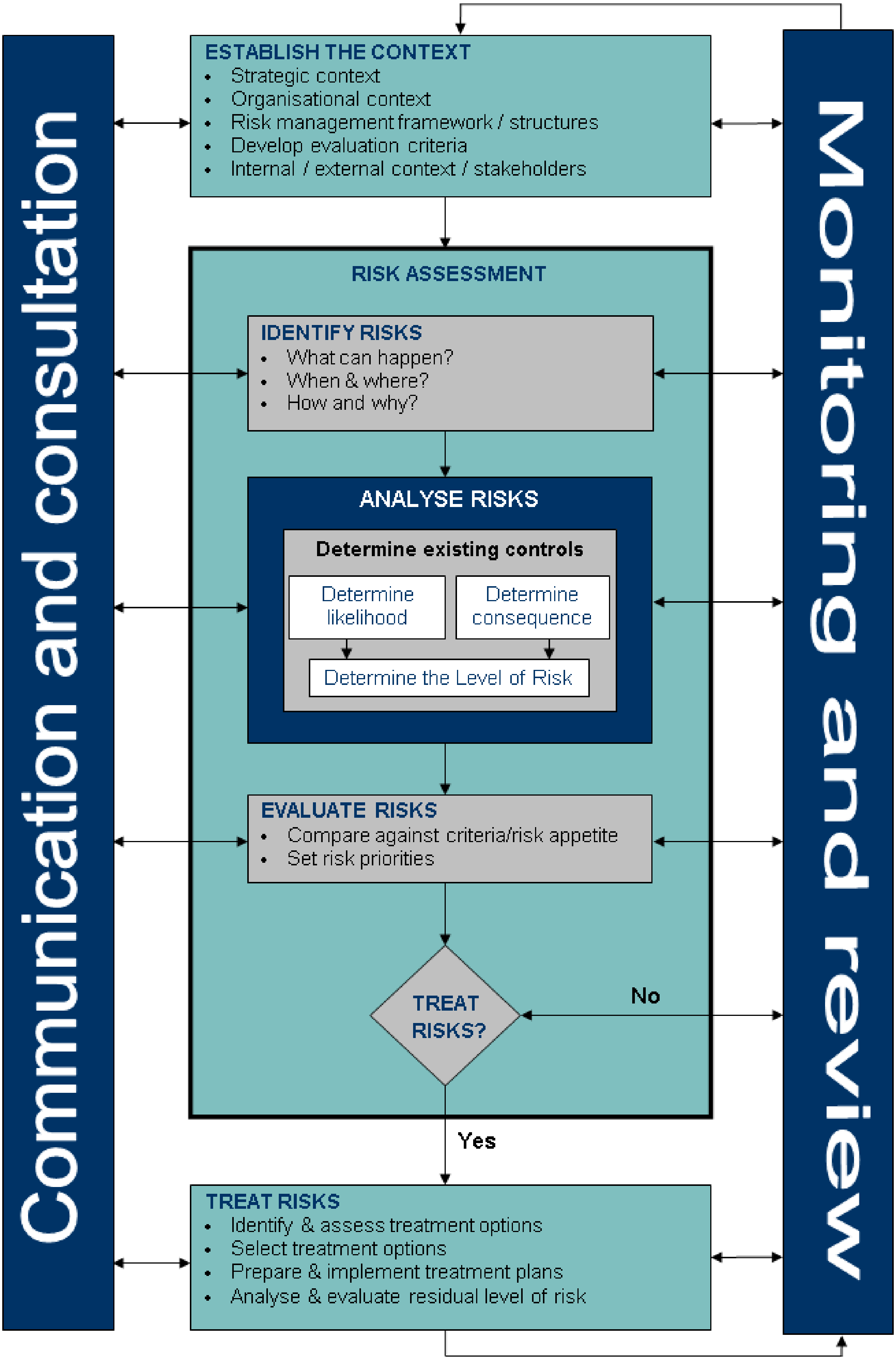
External stakeholders also need to be considered in the risk management process. These may include the Minister, customers, other agencies, community groups, contractors, and volunteers.

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 this framework.

6.1 Risk Management Process Flowchart



7 Roles and Responsibilities

Informed and committed employees are the most important resource in implementing risk management successfully. Roles and responsibilities are outlined below:

Chief Executive

The Chief Executive is accountable to the Minister for:

- Establishing and maintaining a culture of risk awareness and intelligence;
- Ensuring governance mechanisms effectively monitor risks and the way they are managed;
- Ensuring employees receive support in fulfilling their responsibilities;
- Setting standards of best practice for risk management, based on the AS/NZS ISO 31000:2009; and
- Contributing to the attainment of whole-of-Government economic, social and environmental objectives in South Australia's Strategic Plan.

Executives and Senior Management

All Executive and Senior Managers 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 that risk registers reflect outcomes.

Key Risk Assessment Facilitators (RAFs)

Key RAFs are highly experienced RAFs who have oversight at a divisional level and assist with RAFs in business units within their division. A Key RAF:

- Assists with the quarterly requirements at a strategic level;
- Supports Managers / Directors on nominations for new RAFs;
- Encourages and supports other RAFs in learning opportunities.

Employees

Employees actively support, report and contribute to the risk management process. Employees also maintain awareness of the risks and opportunities that relate to their work group and discuss risk management with RAFs, Managers and the Risk Management.

Risk Management Team

The risk management team is responsible to the Director, Quality Assurance Risk & Business Improvement (QARBI) 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 works across the department to assist with the implementation of the Risk Management Policy and Framework, and provides training and support to RAFs and Managers.

Internal Audit

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

Risk Management and Audit Committees

The DCSI Risk Management and Audit Committee monitors risk management within DCSI. The South Australian Housing Trust (SAHT) Board Audit & Finance Committee monitors risk management within Housing SA and the relevant functions within Renewal SA. The Committees:

- Assist the DCSI 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 that accountabilities are met;
- Provide oversight of the risk management function of DCSI, Housing SA and relevant functions within Renewal SA;
- Review and monitor the development and implementation of risk management principles across DCSI, Housing SA and relevant functions within Renewal SA;
- Receive quarterly strategic risk management reports.

8 Recording and Reporting Requirements

Risk information should be recorded in a way that is concise, accurate and timely thus enabling reports to be generated. This builds 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. Quarterly reporting identifies the current timelines for the 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 the DCSI Risk Management and Audit Committee regarding risk registers and risk treatment plans.

Executives are required to report to the DCSI Risk Management and Audit Committee all key risks:

- That are rated extreme/high at controlled or treated level of risk;
- That may have an impact across other divisions/business units of the department;
- Where the action required to address the risk requires a higher level of authority; and
- Are determined 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 when business plans are being developed;
- Facilitate reports to enable directors to sign off on quarterly reports and forward them to the Risk Management team.

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 (if required).

Risk Management

The Risk Management team will report quarterly on strategic and divisional risks, controls and treatments to divisional risk management committees and Housing and Homelessness Leadership Group (HHLG) meetings. Reports focus on matters arising from new and emerging risks to the department and work to be undertaken.

Internal Audit

Internal audits 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.

DCSI Risk Management and Audit Committee

This Committee reports to the Chief Executive on any major risks or issues that are of continuing concern and ratifies reports on activities and outcomes prepared by QARBI 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 can also be downgraded.

Risk Management Reporting

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 department's strategic objectives.

The accuracy of the risk register is the responsibility of the risk management team which continuously support RAFs through formal training sessions, specific risk assessments, RAF Forums, workshops and as requested by the RAF or senior personnel.

The risk register provides evidence of risks having been systematically identified, analysed and treated on a continual 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, the 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 DCSI Risk Management and Audit Committee

9 Appendices

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

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 and Business Development packages and presentations will be presented in conjunction with the College for Learning and Development.	Bi-annually	Risk Management
Risk Management Reporting Process	Risk Assessment Facilitators (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, Housing Leadership Group (HLG) and the Executive Leadership Team (ELT) are then provided with reports outlining the results. Any feedback from these groups is then incorporated into the Risk Management Audit Committee (RMAC) and South Australia Housing Trust Board Audit and Finance Committee (SAHTBAF) reports.	Quarterly	All Business Units/Divisions

DCSI Risk Management Plan

Element	Description	When	Who
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 a controlled level of risk 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 (e.g. matrix, control descriptors), 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

Detailed Risk Management Process

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 e.g. 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 Organisation's goals and objectives, or the Organisation simply cannot afford to implement the initiative.

Questions are useful when establishing the context. Questions can relate to Department, Division, business unit or even a particular team and their function. Key questions to ask when establishing the context may include:

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 also provide assistance in establishing the context.

Identify the risks

Identification is the first step in the risk assessment process. 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. 'Brainstorming' will always produce a broad range of ideas and all should be considered.

Relevant stakeholders are considered to be the subject experts when considering potential risks and should be included in all risk assessments being undertaken. Key risks can then be identified and captured.

The Sources and Categories of Risk template can be useful in this step to determine which area the risk falls under. When identifying risks, consider:

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

During this step, opportunities for enhancement or gain across the organisation may also be identified. Risks may emerge through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

A formal risk assessment is not the only process through which risks are identified.

Analyse the risk

The second step in the risk assessment process is to analyse the risk. This means understanding the essence of the risk and determining the causes and consequences, as well as identifying any existing controls.

Existing controls are things already in place such as policies, procedures, training programs etc. These must be rated as either effective; requires improvement; or ineffective. Once this has occurred, the level of risk can be ascertained using the risk assessment matrix.

The Department has created a risk assessment matrix based on its 'risk appetite' and what is and isn't acceptable within the organisational structure. DCSI 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 risk with a controlled, high or extreme level of risk is not treated due to the financial impact and therefore the risk will remain at this level. Should this occur, an explanation from the risk owner must be recorded.

Risk descriptions describe the risk, its causes and its consequences. The risk description is a short, contextual statement; the causes and consequences should centre on the context of the risk.

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. 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 should also be 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.

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. A decision must be made regarding whether treatments need to be implemented and then the priority of treatments established.

The departmental **Risk Assessment Matrix** should be used to determine the levels of risk (LoR) 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 the **control effectiveness** rated as **'requires improvement'** or **'not effective'** and therefore a treatment plan;
- Risks that are rated at the controlled level of risk as either moderate or low can be accepted and monitored, if the **control effectiveness** has been assessed as **'effective'**.

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 department's risk appetite has been determined as below.

DCSI Risk Appetite

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

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

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:

1) *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. Risks may also be accepted when the risk is of low consequence and unlikely to occur. This may require an explanatory note from the risk owner if the controlled level of risk is rated at extreme or high.

2) *Risk Retention:*

When, after careful analysis, it is identified the risk cannot be avoided, reduced or transferred, or where the cost to do so is not justified, it is retained as a risk. This requires an explanatory note from the risk owner stating the situation and awareness of the status of the risk.

3) *Risk Avoidance:*

Risk avoidance occurs 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.

4) *Risk Transfer:*

Risks may be transferred to other parties. This may include, for example, taking out insurance policies, outsourcing activities or moving operations to an area of the department better placed to handle the risk.

5) *Risk Control (reduce the likelihood and/or consequence of the event):*

Controlling risk is where the majority of effort is generally required. Management processes, such as audit and compliance programs, preventative maintenance and training of employees are some methods that reduce risks. Ensuring that controls are in place, such as contingency plans, evacuation procedures or structural barriers, may reduce the consequences.

This element also incorporates evaluating the options, preparing treatment / action plans and implementing these 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 includes:

- 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 i.e. the level of risk after the treatment / action has taken place. The treated level of risk must be recorded on the electronic risk register and subjected to monitoring, review and, where appropriate, further treatment / action. Treatment / action plans can also be implemented following recommendations provided by internal or external audit following a review.

Iterative steps in the risk management process

There are 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, for example, why particular treatment / action options are selected.

Monitoring and review

Monitoring and review is essential.

During the quarterly reporting process, management must review risks within their area and follow up on controls and treatments / action that are mitigating these risks. Any action that is out of date and requires further attention can thus be identified. As well, completed treatments could be converted to controls; levels of risk confirmed and risks may be retired or escalated.

Monitoring and reviewing risks, controls and treatments also apply to any actions / treatments from 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 mitigated to a point where the risk is accepted. However, this can only occur when the controlled level of risk is either moderate or low.

Risks are retired for a variety of reasons and can be reactivated should there be a change in the organisational objectives or internal/external environment. Retired risks are not deleted from the risk register but may be archived after a period of time.

Risk Categories and Potential Sources of Risk

Best practice in risk identification requires the categorisation of risks. Each risk/opportunity identified 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. The following list is not conclusive and indicates only some examples of potential sources of risk.

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
Knowledge Management / Information Technology	• Procurement • Legal compliance • Protective security	• Records management • Business continuity and disaster response • Advancement in technology
Partnerships / Stakeholder (Working Together)	• Client and stakeholder relationships • Organisational relations (internal & external) • Government collaborations	• Peak bodies and various groups • Communications
Customer Service	• Specific client needs • Promulgation of information to clients	• Evaluation and feedback • Economic value of service
Asset & Facility Management	• Policies & procedures • Legal and financial requirements • Assets, development and maintenance	• Business continuity and disaster response • Protective Security
Legal Compliance	• Legislative requirements • Legal and governance obstructions • Industry regulations and standards	• Legal liabilities • Work Health & Safety • Departmental guidelines
Procurement & Contract Management	• Policies and procedures • Financial management • Contractual agreements • Contract specifications	• External, outsourced functions • Asset management • Resource availability • Transparency & dispute resolution
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
Work Health and Safety	• Governance and legal requirements • Policies and procedures	• Injury management & response • Incident management and documentation
Finance	• Policies and procedures • Financial management	• Legislative & industry requirements • Legal costs
Project Management	• Project Management Framework compliance • Project Management Office requirements	• Skilled resources
Clinical	• Policies & procedures • Safety & quality • Direct client care • Informed consent • Adverse events	• Privacy & confidentiality • Resource allocation • Training & credentialing of clinicians /practitioners • Documentation
Fraud & Corruption	• Policies & procedures • Control breakdown • Protective security	• Procurement & contract management • Illegal activity

DCSI Risk Assessment Matrix

DCSI Risk Assessment Matrix

DCSI Risk Likelihood and Consequence Matrix

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

DCSI Risk Appetite

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

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

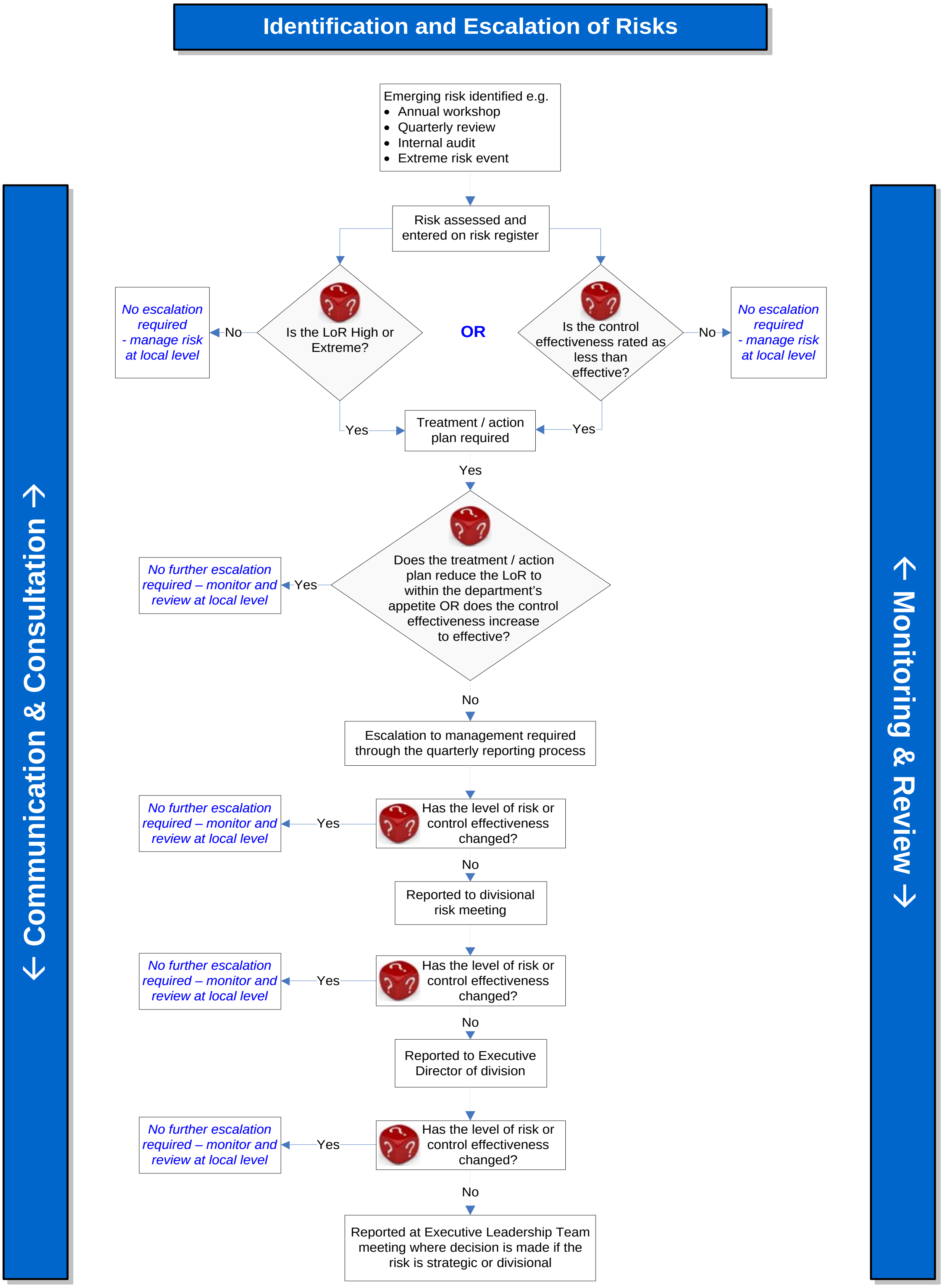
DCSI Risk Likelihood Descriptors

Level	Descriptor	Indicators (Choose one only)		
		Qualitative	Quantitative	Quantitative
5	Almost Certain	Expected to occur in most circumstances	Daily to Weekly	90 – 99% probability 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 January 2016

	Impact Categories					
	Client	**Health & Safety**	**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 or increased dependence • Some services delayed or not delivered to customers • Missing person • Potential exposure to a threat that may result in injury requiring a minor operation	• Lost time injury greater than 5 working days • SafeWork SA intervention due to non-compliance with legislation, regulations or codes requiring a Provisional Improvement Notice (PIN) and/or 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 • Unplanned hospitalisation • Some major Departmental services to customers cease • Exposure to an immediate threat that may result in injury requiring significant medical treatment or death • Missing child	• Hospitalisation, Dangerous Occurrence, Notifiable Work related injury/illness/death • DCSI duty to provide suitable work or wages as per Section 58B – Workers Rehabilitation & Compensation (WRC) Act 1986 • 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 • Prosecution and/or litigation	• 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 threat 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

Risk Management escalation flowchart



Terms & Definitions

Clinical 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. Political, Economic, Socio-Economic, Technological, Legislative and Environmental 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. Strengths, Weaknesses, Opportunities and Threats).
Levels 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.
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	The 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 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	Set of components that provide the foundations and organisational

framework	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.
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 individual's 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	Any person or organisation (internal and external) 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 on the treatment design, resourcing and agree timeframes for implementation with directors, risk owners and, possibly, control owners.