vmia
Risk Management and Insurance

Guide

Risk Management

For Community Service Organisations

April 2010

Contents

Disclaimer

The information provided in this document is intended for general use only. It is not a definitive guide to the law, does not constitute formal advice, and does not take into consideration the particular circumstances and needs of your organisation.

Every effort has been made to ensure the accuracy and completeness of this document at the date of publication. VMIA cannot be held responsible and extends no warranties as to the suitability of the information in this document for any particular purpose and for actions taken by third parties. This document is protected by VMIA copyright. VMIA grants a non-exclusive right for this document on the condition it is not distributed for profit. VMIA encourages the free transfer and copying of the document if such activities support the purpose and intent for which the document was developed.

For more information on risk management, please visit www.vmia.vic.gov.au

1. Managing risk in community services

1.1. What is risk management?

Risk Management is an integral part of good management practice that should be embedded within all business processes.

A risk is defined by *ISO/IEC Guide 73:2009 Risk management – vocabulary* as “effect of uncertainty on objectives.”

Risks by their nature can be avoided, managed to acceptable levels, or shared to a third party. Community service organisations that manage risk effectively and efficiently are more likely to achieve their objectives.

Being part of corporate governance[1] – *the overall guidance system for achieving planned objectives* – risk management[2] develops treatment plans, controls and strategies associated with achieving objectives.

Controls provide reasonable assurance to the Board and Management that planned objectives will be achieved. They are processes, policies, or actions to minimise negative risk or enhance positive opportunities.

Compliance[3] and quality management ensures that organisational standards and requirements are met and these are part of the organisation’s controls.

1.2. Managing risk is about knowing your objectives

Everyone manages their own risk all the time, whether in the workplace[4] or at home. An example of managing risk on a daily basis is illustrated below:

Example – Planning a holiday to Asia		
Objective	**To get to the hotel safely**	
Risk	**Travel and transport**	
Description	**Illustration**	**Definition**
Risk	Potential car accident	Event that may impact your objective (Risk Rating = Consequence x Likelihood; Consequence – Impact of a risk event Likelihood – Probability of a risk occurring)
Risk factors	Speed; unfamiliar road system; car quality; traffic conditions	Factors that give rise to the risk
Controls	Avoid peak traffic; use a driver; understand traffic conditions	Policies, procedures and processes in place to address inherent risk
Residual risk	Low risk – injury	Risk remaining after risk treatment

[1] Australian Standard *AS 8000:2003 – Good Governance Principles* defined governance as a “system by which entitles are directed and controlled”.
[2] See *AS/NZS ISO 31000:2009 Risk management – principles and guidelines.*
[3] *Australian Standard AS 3806:1998 – Compliance Programs.*
[4] This is usually reflected in positions of staff.

Risk management is a whole-of-organisation approach to managing risks and prioritizing responses to risks to support the implementation of action plans and achievement of organisation and operational objectives.

An example of an objective for a community service organisation (CSO) is illustrated below.

Example – Establishing objectives

Strategic Objective for 2009 – 2009 is to improve their client satisfaction from 80% to 90%

Objectives should be SMART (specific, measurable, achievable, realistic and timed).

- Specific – Be precise about what you are going to achieve (e.g. achieving higher client satisfaction in the current financial year).
- Measurable – Quantify your objectives (e.g. 90% satisfied clients)
- Achievable – Are you attempting too much? (e.g. 100% satisfied clients)
- Realistic – Do you have the resources to make the objective happen? (e.g. people, money, machines and materials)
- Timed – State when and period by which you will achieve the objective (e.g. within one financial year, by June 2011).

Benefits in managing your risk include;

- improving organisational governance and performance
- effective planning, budgeting, reporting and strategy execution
- increasing the likelihood of achieving your objectives and meeting targets

1.3. Standard of risk management

AS/NZS ISO 31000:2009 consists of three major parts:

- Principles for managing risk (Clause 3) – To be most effective, CSOs should adhere to the 11 principles for managing risk
- Framework for managing risk (Clause 4)
- Process for managing risks (Clause 5) – this is same as the risk management process described in AS/NZS 4360:2004 (which has been superseded by AS/NZS ISO 31000:2009 from 20 November 2009).

To be successful, risk management should function within a framework for managing risk that provides the necessary foundations and organisation arrangements that will embed risk management throughout the organisation at all levels and integrate risk management process within its overall governance, management, reporting processes, policies, philosophy and culture. This foundation can assist CSOs in managing risk effectively through the application of the processes for managing risk at varying levels and within specific contexts of the organisation.

There are five components of the framework for managing risk;

1. mandate and commitment
2. design of framework for managing risk
3. implementing the five processes for managing risk (see Section 1.7) :
   - communication and consultation
   - establishing the context

    - risk assessment
    - risk treatment
    - monitoring and review
4. monitoring and review of the framework
5. continual improvement of the framework.

1.4. Criteria for success

Generally, the main criteria for success are considered to be:

- Gaining total support from the top – without this, the process will fail and staff will not support the implementation with anything but lip service (risk champions at the CEO level are most effective)
- Incorporate risk management within the development and review of business plans and targets
- Follow through – tools, templates, training, self-checks and self-assessment, review, audit and confirmation are vital for the ongoing success of the risk management program
- Getting the message across that risk management is not just another fad but is something that can assist all staff and managers to be more effective
- A simple system that all staff can access and use on a regular basis.

1.5. Embedding and Integrating risk management

The framework for managing risk will form an overarching management foundation upon which other management frameworks can be implemented, such as:

- planning, reporting and budgeting processes
- quality and compliance program
- business continuity management program
- occupational, health and safety program

In implementing the framework for managing risk, you should consider the following:

- defining the appropriate timing and strategy for implementing the framework
- applying the risk management policy and plan to your organisation
- complying with legal and regulatory requirements
- documenting justified decision making, including the development and setting of objectives which are aligned with the outcomes of the risk management process
- conducting information and training sessions
- communicating and consulting with stakeholders to ensure that your framework and process for managing risk remains appropriate and effective.

1.6. Risk management policy and plan

A risk management policy clearly identifies your organisation's approach and attitude to risk management and the expected roles and responsibilities of individuals and committees, integrated with your overall policies and practices. It covers the following:

- objectives of the policy and the rationale for managing risk
- scope and coverage of the risk management policy

- links between the risk management policy and organisational objectives, goals, policies and the nature of its business
- accountabilities and responsibilities for managing risk and risk coordination
- organisation's risk appetite or risk aversion
- process, methods and tools to be used for managing risk
- resources available to assist those accountable or responsible for managing risk
- reporting protocols and the level of documentation required for various organisational levels, Management and the Board
- way in which risk management performance and indicators will be measured and reported
- commitment to periodic review and verification of the policy and framework, and its continual improvement.

A risk management plan defines how the process for managing risk is to be conducted throughout the organisation. It includes how the process is customised for and embedded into the organisation, its policies, procedures and culture. The plan covers the following:

- risk management definitions and language that promotes consistent understanding of risk management concepts and methodology
- relationship and integration with other management practices, integrated with and embedded into existing processes
- description of how each step of the process for managing risk will be applied within the organisation and activities
- risk reporting framework – content, format, frequency and recipients of risk reports and indicators
- risk assessment criteria – agreed criteria for assessment of risk likelihood, consequence, and overall level of risk
- risk register format.

A risk register is used for recording the risk management process for identified risks. This is further described in Section 2.7. The risk register includes:

- a description of the risk and risk owner
- existing risk controls that may minimize the likelihood of the risk occurring and/ or the consequence of the risk
- likelihood and consequences of the risk to the organisation
- level of risk rating based on risk rating matrix (high, medium, low, etc)
- assessment of whether the risk is acceptable or whether it needs to be treated (based on the organisation's risk appetite)
- clear prioritisation of risks and the development of a risk profile
- accountability for risk treatment as part of risk treatment plans
- time-frame for risk treatment.

1.7. Process of managing risk

The process for managing risk is the systematic application of management policies, procedures, and practices to the task of communicating, consulting, establishing the context, identifying, analysing evaluating, treating, monitoring and reviewing risk, as shown below:

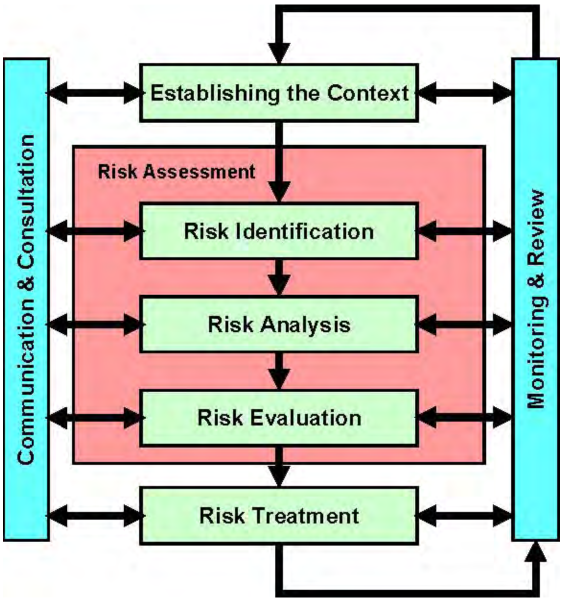


Figure 1: Process for managing risk

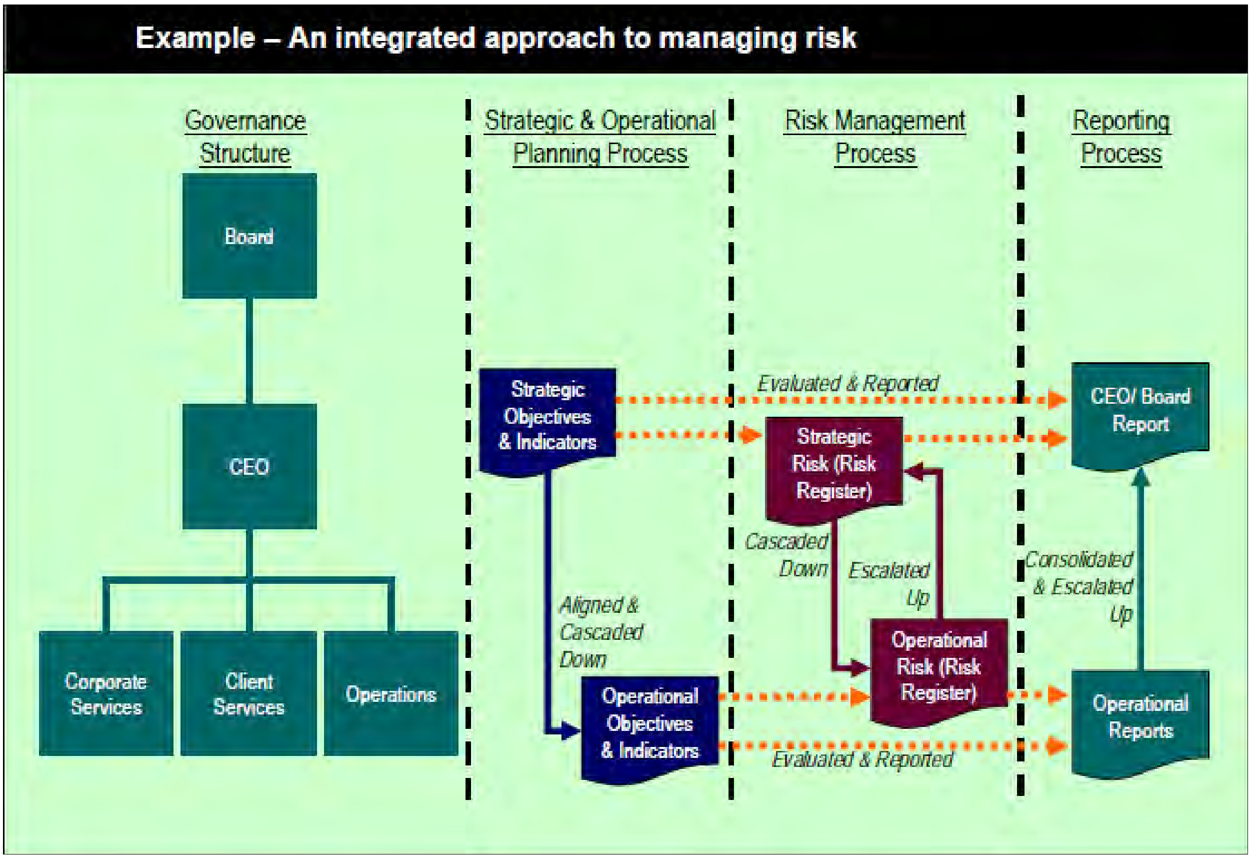
Key elements of the risk management process are:

- Effective communication and consultation is intrinsic to the process for managing risk and should be considered at every step of the project, process, or activity
- Establish the context by understanding your operating environment, objectives, and SMART indicators and targets
- Identify risks by generating or brainstorming a “shopping” list of relevant risks that could prevent the achievement of your objectives
- Analyse and quantify the likelihood of a risk event occurring and its consequence using pre-established likelihood and consequence rating tables. Evaluate control effectiveness using a control effectiveness rating table where possible. This is further explained in section 2.5. All controls identified must be actionable by an assigned control owner
- Evaluate the level of risk and prioritise your risks using a risk matrix
- Treat the risk by selecting cost-effective risk responses (or risk controls), and incorporating them into your risk register and risk treatment plans
- Monitor and review your risk register, risk treatment plans and the framework and process for managing risk on a regular basis.

2. Implementing your risk management program

2.1. Aligning risk management to achieving objectives

An example of an integrated approach to managing risk is illustrated below:


Example – An integrated approach to managing risk
Governance Structure
Strategic & Operational Planning Process
Risk Management Process
Reporting Process
Board
CEO
Corporate Services
Client Services
Operations
Strategic Objectives & Indicators
Aligned & Cascaded Down
Operational Objectives & Indicators
Evaluated & Reported
Strategic Risk (Risk Register)
Cascaded Down
Escalated Up
Operational Risk (Risk Register)
Evaluated & Reported
CEO/ Board Report
Consolidated & Escalated Up
Operational Reports

Based on the CSO's governance structure, and strategic and operational planning process, strategic objectives and indicators are determined at the organisational-level and cascaded down as operational objectives and indicators into various business units like Corporate Services, Client Services and Operations. Strategic risks are linked to the achievement of the CSO's strategic objectives and indicators. Likewise, operational risks are linked to the achievement of operational objectives and indicators.

There should be objective criteria in the risk management policy for:

- escalating operational, new or emerging risks bottom-up from operations to management and/or Board
- cascading down strategic risk for operational line manager's attention.

The organisation's risk register would include both strategic and operational risks.

Regular operational reports will report on the progress of operational risk treatment plans and any potential new operational risk. Operational reports are consolidated upwards whereby the nature and volume of risk information required to be reported at various organisational levels (including the Board level) and from various geographical locations are determined. For example, the Board may receive the top 15 organisation/ strategic risks.

2.2. Specifying performance indicators

SMART indicators specify how the achievement of objectives will be measured and answers the question – “How do I know whether or not the organisations plans are being achieved, or have been achieved?”. An understanding of indicators is therefore an essential pre-requisite to understanding risks and controls required.

Examples of performance indicators and targets from which risk could be identified are illustrated below.

Example – Strategic objectives, indicators and targets

Strategic Objectives	Performance Indicator	Performance Targets
Continuously improve quality and safety	Number of injuries	5 per quarter
Continuously improve services and facilities	Number of adverse client feedback about client services	90% high client satisfaction score (yearly) for 80% of client base
Achieve a financially sustainable service	Finance reserves	$1.0 million by June 2009

In the example below, strategic objectives and indicators can be cascaded and aligned throughout various parts of the organisation, using tools like the balanced scorecard.

Example – Cascading strategic objectives into operational objectives and indicators

Strategic Objectives	Corporate Services	Client Services	Operations
Continuously improve quality and safety		√	√
Continuously improve services and facilities		√	√
Achieve a financially sustainable service	√		

Client Services together with Corporate Services and Operations would then have its own risk management process (at the operational level) to identify operational risk that may impact upon their achievement of the own operational objectives, in addition to allocated strategic objectives that have been cascaded down.

2.3. Integrate risk management with reporting

Integrate and embed risk management into your reporting framework by developing a standardised reporting format that includes the following:

- performance and variance reporting – reporting on the achievement of objectives and adherence to budgets
- reporting on new and/or emerging risk, including changes and updates to the risk register
- status report of agreed risk treatment plans

Monthly operational reports will have information on the achievement of operational objectives and updated to the operational risk register. These operational reports will be consolidated at the CEO/ Board level. Board reports would include information on the achievement of strategic objectives and updates to the strategic risk register.

2.4. Communication and consultation

An important aspect of risk management is to ensure appropriate communication and consultation with stakeholders, including audit and risk committees (or equivalent). Communication and consultation throughout the entire process for managing risk is vital to ensure that

- risks have been accurately identified
- controls for identified risks are adequate and effective
- "buy-in" from risk and control owners is secured
- all stakeholders are engaged and committed to the risk management process
- the risk management process is effective and well embedded within the organisation, and its culture and processes.

2.5. Risk assessment

The risk assessment process consists of three steps :

- identifying risk
- analysing their likelihood and consequences
- ranking the level of risks against pre-established priority criteria

For each objective, the organisation uses the risk management process to :

- identify performance indicators, quantifiable targets and corresponding risk
- analyse and quantify the level of risk in terms of the likelihood (L) of a risk event occurring (using a likelihood rating table) and the consequence (C) of its impact on the organisation if the risk did occur (using a consequence rating table)
- identify and assess any cost effective controls (e.g. policies, procedures, checklist) that are actionable by the organisation (using a control effectiveness rating table)
- estimate and prioritise the level of risk (using a risk matrix), all based on the organisation’s risk appetite, or willingness and ability to take appropriate risk.

Both risk appetite and risk tolerance set boundaries in relation to how much risk an organisation is prepared to accept. Risk appetite is a high-level statement of risks that the Board and management accept. Risk tolerance is narrower and describes the acceptable level of variation around objectives. Risk tolerance operationalises risk appetite.

For example, an organisation that says that it does not accept risk that could result in a significant loss of its funding base is expressing its *risk appetite*. When the same organisation says that it does not wish to accept risks that would cause funding from its top-five funding providers to decline by more than 15%, it is expressing its *risk tolerance.*

Risk appetite and risk tolerance are represented in the risk management plan and are included in the following:

- likelihood rating table
- consequence rating table
- control effectiveness rating table
- risk matrix
- risk treatment policy

Examples of three point likelihood and consequence rating tables, based on risk appetite and risk tolerance are illustrated below.

Example – Likelihood rating table (three point scale)

Likelihood Rating	Probability of Occurrence
Almost Certain	Event will almost certainly occur – once a year or more frequently
Possible	Event might occur at some time – once in 2 years
Rare	Event may only occur in exceptional circumstances – once in 5 years

Example – Consequence rating table (three point scale)

Consequence Rating	Clinical	Financial	Publicity	Efficiency	Quality / Performance	Service Disruption
Extreme	Death	>$50,000	Adverse Reputation Damage	Non-Achievement of Objectives	>50% Variation	> 1 Month
Moderate	Disability	$1,000 to $50,000	Moderate Reputation Damage	Moderate Impact on Achievement of Objectives	10% to 50% Variation	1 Day to 1 Month
Minor	Injury	<$1,000	Insignificant Reputation Damage	Insignificant Impact on Achievement of Objectives	<10% Variation	< 1 Day

Whether it is a five, four or three point scale depends on organisational preference (e.g. guided by financial delegation limits, organisational maturity and culture, historical information…etc).

Controls are effective when your processes are operating in a manner that provides reasonable assurance that the organisation's objectives will be achieved. An example of a control effectiveness rating table is illustrated below.

Example – Control effectiveness rating table (three point scale)

Control Rating	Description of Control
Effective	• Controls are well designed, documented, operating and address the risk • Controls are effective and reliable.
Satisfactory	• Controls are designed, documented, operating and addresses most of the risk • Controls are not always effective or reliable
Unsatisfactory	• Controls in place do not adequately address the risk

The level of risk is the magnitude of risk measured in terms of the combination of likelihood (L) and their consequences (C), where:

- likelihood = probability or frequency of a risk event occurring, or chance of something happening
- consequence = the effect on the organisation of a risk event occurring expressed qualitatively or quantitatively, or change in circumstances affecting the achievement of objectives.

Risk matrix is a tool for ranking and displaying risks by defining risk categories, levels of likelihood and ranges for consequences. An example of a risk matrix is illustrated below.

Example – Risk matrix (three-by-three matrix)

Likelihood	Almost Certain	Medium	High	High
	Possible	Low	Medium	High
	Rare	Low	Low	Medium
		Minor	Moderate	Extreme
		Consequence		

Risk ranking is used to categorise the risk based on the level of risk. A risk should be rated "high" if the risk is likely to occur and/ or its consequence is rated "high". Classification of "red", "amber" and "green" ratings are customisable and are dependent on your risk appetite.

Using the risk matrix to rank risk promotes identification and prioritisation of which risk will be:

- cascaded-down as operational risk (lower-level "green" risk) for operational managers to monitor
- escalated-up as strategic risk (higher-level "amber" or "red" risk) for senior management or Board attention.

The criteria for risk to be cascaded-down or escalated-up must be clearly defined in the organisation's risk treatment policy. Risk treatment develops and implements measures to modify risk.

An example of a risk treatment policy is illustrated below.

Example – Risk treatment policy (three point risk rating)			
Risk Rating	**Control Response**	**Management Response**	**Responsibility**
High	• May prevent achievement of objectives • Controls require detailed planning and decision making at Board or Management level.	• Needs regular management • Risk treatment plans must be established and implemented • Risk rated "high" at the operational level is escalated up and reclassified as strategic risk in the risk register	Risk is to be managed, monitored and reported at the Board or Management level, with individual risk owners identified.
Medium	• Management control responsibility must be specified • Further management measures / controls may be considered, if economic	• Needs regular monitoring • Risk should be monitored in conjunction with a review of existing control procedures	Risk is to be managed, monitored and reported by Management, with specific risk owners identified.
Low	• No major concern and can be managed by routine controls and procedures	• No major concern • Significant management effort should not be directed towards these risks • Risk rated "low" at the strategic level is cascaded down and reclassified as operational risk in the risk register	Risk is to be managed, monitored and reported at the operational level, with specific risk owners identified.

2.6. Risk treatment

Risk treatment planning consists of the identification of feasible but cost effective risk treatments. Options include:

- **Avoiding the risk** – Where the level of risk is unacceptable and the means of risk control are either not viable or not worthwhile or not actionable, risk could be eliminated by not proceeding with the activity that could generate the risk. For example, changing your business activity, process or objective so as to avoid the risk.
- **Changing the risk likelihood** – Undertake actions aimed at reducing the probability of the risk occurring. For example, using concrete rather than wood for buildings.
- **Changing the risk consequence** – undertake actions aimed at reducing the impact of the risk. For example, installing fire sprinklers to control a fire
- **Retaining or accepting the risk** – Accept the risk as it is. This is appropriate where the rating of a risk is sufficient to justify other potential risk treatment options, or when it is not possible or uneconomic to treat the risk, or when the risk level is within your risk tolerance. For example walking on a pedestrian crossing.
- **Sharing the risk** – Responsibility for treating the risk can be transferred or allocated to parties best able to manage it. For example, using insurers or contractors.

The general principle of risk management is that risk should be the responsibility of those best able to control or manage them (e.g. risk owner, control owner and/or task owner). Control activities must be regularly tested or reviewed by independent parties like auditors to ensure that there are no material weaknesses or significant deficiencies. Risk treatment options involve trade-offs between potential benefits of implementing a response and actual cost of doing so.

2.7. Risk register

Formal recording and reporting of risk is an important phase of the risk management process. The risk register is the central starting point whereby risk reporting and risk treatment plans can be recorded and monitored, and reviewed regularly.

The register systematically documents and records identified risks, as illustrated below.

Example – Risk Register							
Strategic Objective	**Risk Event**	**Controls**	**Control Effectiveness**	**L**	**C**	**R**	**Risk Owner**
Improve safety	Client injury	Signage installed	Good	P	E	H	Jim Smith

L = Likelihood
C = Consequence
R = Level of Risk

From your centralised risk register, you are able to extract information for other reports like risk reports, risk treatment plans and risk profile for your stakeholders, as illustrated below.

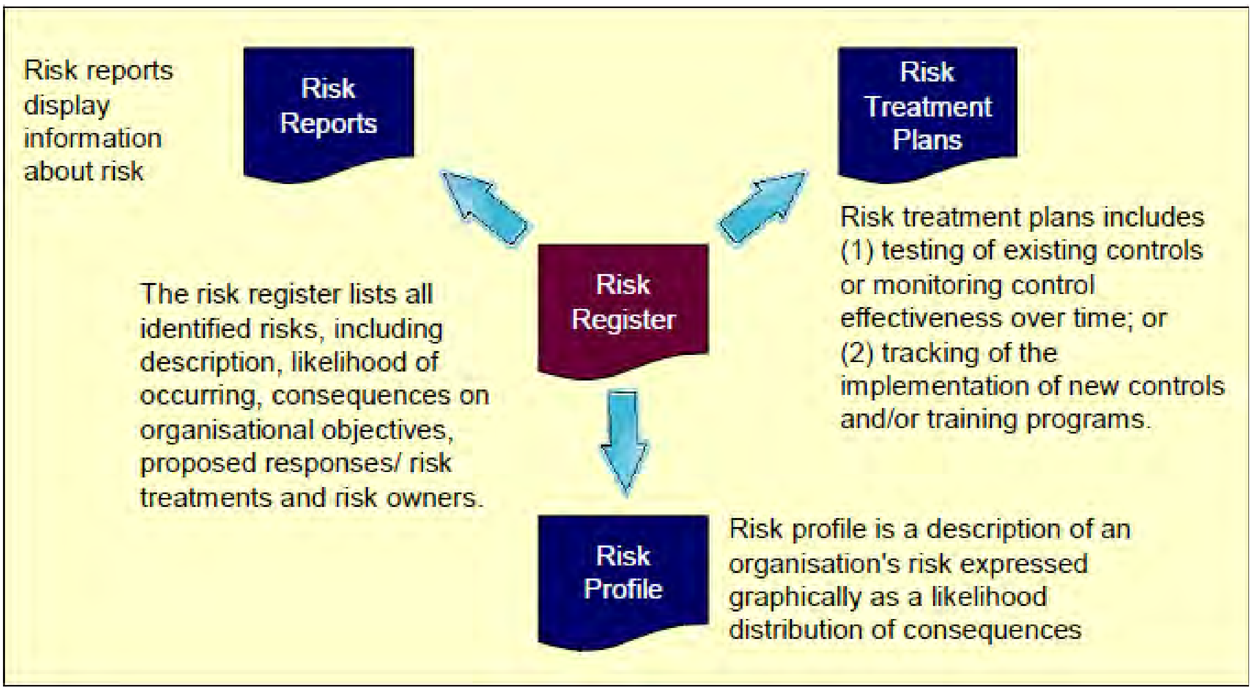

Risk reports display information about risk
Risk Reports
Risk Treatment Plans
Risk treatment plans includes (1) testing of existing controls or monitoring control effectiveness over time; or (2) tracking of the implementation of new controls and/or training programs.
The risk register lists all identified risks, including description, likelihood of occurring, consequences on organisational objectives, proposed responses/ risk treatments and risk owners.
Risk Register
Risk Profile
Risk profile is a description of an organisation's risk expressed graphically as a likelihood distribution of consequences

Figure 2: Types of risk reporting

2.8. Monitor and review

It should be appreciated that the management of risk may change over time. This may be due to:

- risk responses become ineffective
- control activities become less effective or are no longer used
- changes in the organisation's objectives

Risk monitoring is all about monitoring risk management procedures, particularly risk treatment plans, to assess whether they are effectively implemented and achieving their planned aims. Monitoring risk and the effectiveness of the risk management process should be a recognised activity tat is routinely performed.

Risk management review is a structured activity that is undertaken to determine the suitability, adequacy and effectiveness of the risk management policies and procedures to achieve established objectives. Regular review and re-evaluation of your organisation's risk is also essential to ensure that your risk register remains relevant, complete and current.

Risk reporting is the development of reports including strategic, operational, financial and compliance- related risk information, as a basis for directing and controlling the organisation as well as for external accounting and decision making. It should ensure effective communication and information flows both downwards and upwards throughout the organisation, as well as to stakeholders.

An example of a monitoring and review timetable is illustrated below.

Sample – Risk and risk management process monitoring and review timetable		
Monitoring / Review Activity	**Frequency**	**Forum (Responsibility)**
Risk register review	Annually	Management team meeting (CEO)
Reporting on risk registers	Annually	Operational planning (Managers)
Review of risk treatment plan	Monthly	Team meeting, reporting (Managers)
Reporting on risk treatment plans	Quarterly	Board or Management (Managers)

As a general rule, volatile risk environments require closer monitoring and more frequent review and re-evaluation of risk and the risk management process itself.

2.9. Assurance program and audits

Risk audit is the systematic, independent and document process for obtaining audit evidence and evaluating it objectively to determine the extent to which risk management policies and procedures are fulfilled.

As part of the assurance program, it is essential that risk treatment plans and subsequent monitoring of progress are assigned to the appropriate person. The frequency of the monitoring should be dictated by the level of risk and cost-benefit for doing so.

Sample – Assurance program	
Assurance Activity	**Frequency**
Client satisfaction survey	3 yearly
Policy review	3 yearly
Equipment maintenance checks	Annual
Client feedback, complaints and complements audit	Annual
Incident, near miss audits	Annual
Performance appraisal audit	Annual
Professional development / training audit	Annual
Occupational, health and safety audit	6 monthly / Annual
Human resource or personnel file audit	Annual

3. Specific industry examples

	Child Care Centre	Kindergarten	Disability Services Organisation	Neighbourhood House	Cemetery Trust
Objective	To ensure the financial viability of the organisation.	To ensure the safety of children	To ensure the safety of staff whilst conducting home visits.	To ensure the privacy of clients whilst attending grief counselling and/or other support service sessions held at neighbourhood house meetings	To ensure that the business is managed prudently, meeting financial and asset management accountabilities
Identified Risk	Fraudulent activity by an employee leading to embezzlement of funds.	Child consumes peanut products leading to an allergic reaction.	Assault by a patient or member of the patient's household whilst attending home visit leading to staff injury.	Information is discussed outside sessions leading to Infringements of client privacy.	Insufficient revenues leading to failure to maintain cemetery in perpetuity.
Risk Category	Financial	Occupational, health and safety	Occupational, health and safety	Legal	Financial
Likelihood (1-5)	2	3	3	3	4
Consequence (1-5)	5	5	4	3	5
Existing Controls	• Child care payments are required to be transacted electronically • No cash is kept on premises.	• Kindergarten tuck shop had been instructed not to sell any food that contains peanut products. • Parents are required to advise the staff whether their children suffer from a peanut based allergy.	• Staff members have been trained and have protocols of how to recognise a potentially violent situation. • Staff member to carry a mobile phone	None.	• Asset management Plan that supports the ongoing improvement of existing plant equipment and facilities • Prudent investment of surplus funds for future growth and innovation
Control Effectiveness (1.0 – 2.5)	0.75	1.0	0.5	1.0	0.75
Level of Risk	7	15	6	9	15
Treatment Option	Reduce	Reduce	Reduce	Reduce	Reduce
Treatment Plan (Response)	• Security access to online banking arrangements to be limited to two personnel only • Passwords to be updated on a monthly basis	• Parents notified at start of term that lunches/ snacks/ birthday cakes brought to kindergarten must not contain peanut products • Staff trained to treat anaphylaxis	• Ensure that all staff contact patient prior to each visit to determine their emotional state • Ensure that any referrals given by GP's identify whether the patient suffers from any mental illness • Ensure that two staff members visit at risk patients	• Privacy training to be scheduled for appropriate personnel	• Develop budgets that will ensure long-term viability and sustainability • Establish systems to more accurately measure costs and to identify opportunities for reducing waste
Risk Owner	Manager	Manager	Operations Manager	Administrator	Finance Manager
Action	Immediate	Ongoing	Immediate	Next quarter	Immediate

4. About the VMIA

4.1. Who are we

The Victorian Managed Insurance Authority (VMIA) provides risk and insurance services to protect Victoria's assets and minimise losses from adverse events. The VMIA offer support and advice in strategic and operational risk management and insurance products tailored to meet the specific needs of individual clients. Our clients sit primarily within the general government and public health care sectors and include departments, statutory authorities, agencies, infrastructure, rail operations, hospitals, health centres, community service organisations, medical research bodies, tertiary institutions, cemetery trusts, national parks, galleries, museums and event bodies.

4.2. What we offer

Our service platform is built around helping clients better manage their risks while ensuring that they have appropriate insurance cover. We provide this through integrated, cross-functional client teams and a client education program including seminars and forums available across the State.

Risk services include site risk surveys, risk reviews, clinical risk advice, incident analysis, insurance and reinsurance, loss prevention engineering, education and training. Insurance cover typically depends on client needs. Some of the main forms of insurance cover we offer are medical indemnity, professional indemnity, public and products liability, directors and officer's liability, personal accident, industrial special risks and contract works.

4.3. Risk management services

The VMIA develops and tailors risk management and insurance services to clients needs. If you would like to know more about our risk services, contact your Risk Management Advisor or visit our website at www.vmia.vic.gov.au

4.4. Your client relationship team

Deborah Stenning
Client Relationship Manager
Phone : 03 9270 6917
Email: d.stenning@vmia.vic.gov.au

Jennifer Phemister
Insurance Advisor
Phone : 03 9270 6922
Email: j.phemister@vmia.vic.gov.au

Patrick Ow
Risk Management Advisor
Phone : 03 9270 6968
Email p.ow@vmia.vic.gov.au