Department of State and
Regional Development

First for Business

Risk management guide for small business

www.smallbiz.nsw.gov.au

GLOBAL RISK ALLIANCE

May 2005

DISCLAIMER

This package contains information, data, documents, pages and images prepared by Global Risk Alliance on the instruction of the New South Wales Department of State and Regional Development for and on behalf of the Crown in right of the State of New South Wales ('the Data').

Although the Data contained in this package has been formulated with all due care, the State of New South Wales does not warrant or represent that the Data is free from errors or omissions or that it is exhaustive.

The Data is made available on the understanding that the State of New South Wales and its employees and agents shall have no liability (including but not limited to liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the Data and whether caused by reason of any error, omission or misrepresentation in the Data or otherwise.

Furthermore, although the Data is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Data. The Data may change without notice and the State of New South Wales is not in any way liable for the accuracy of any information printed and stored by the user.

ISBN 0 7313 32490

Contents

Foreword

Every day, in both our personal and business lives, we confront and make decisions about risk.

The likelihood and consequences of an unwanted outcome from taking a risk vary with the circumstances and the type of risk.

The New South Wales Government values the entrepreneurial characteristics of business owners and their ongoing contribution to our economy and society. There are ways in which these businesses can assess and manage the risks to themselves, their businesses, their employees, their customers and their suppliers.

We have developed this *Risk management guide for small business* to assist the business operator to implement a risk management strategy for the business.

It guides the operator through the steps of understanding the environment in which the business operates, identifying, analysing and evaluating risks, and considering the options for treatment.

We trust that you benefit from using this guide.

David Campbell MP
Minister for Regional Development
Minister for Small Business

Purpose

This document is a practical guide for managing risk in small business. It reflects the risk management concepts being used in business practice in both the public and private sectors in Australia. It is based upon AS/NZS 4360, recognised internationally as industry best practice in risk management.

The guide includes risk management principles and philosophies, together with practical examples and tools, to assist with risk identification, analysis, management and planning.

The guide will help small business owners to:

- understand risk management and apply the theories and principles
- identify potential impacts, both of a negative and positive nature, on business objectives
- manage potential impacts to ensure the best outcome for the business
- identify where risk management fits with existing business functions
- understand the need for a proactive approach to risk management
- assist others within their business to understand the benefit of risk management and their roles
- implement the risk management process.

Why is risk management necessary?

Risk is a part of everyday life. There are many types of risk that will be encountered in business. Some will have a minimal impact and can be managed easily; others may threaten the longevity of a business. Understanding the principles and processes for effective risk management will help a business owner make the decisions necessary to ensure the best possible outcome for the business.

What is a small business?

Small businesses are businesses in the private sector, and across all industries, that employ fewer than 20 people. Nearly half of these businesses employ no more than one person.[1]

Small businesses are generally considered to have the following characteristics:

- they are independently owned and operated
- they are closely controlled by owners/managers
- decision-making is principally done by the owners/managers
- the owners/managers contribute most if not all of the operating capital.

[1] Agricultural businesses are normally excluded from small business statistics. Refer Australian Bureau of Statistics, *Small Business in Australia,* 2001 [Catalogue no. 1321.0].

How to use this guide

This guide is divided into six sections with supporting material.

1 Risk management principles and concepts

This section overviews the philosophies of risk management. It defines risk and explains how risk management can contribute to the management and performance of the business.

2 Categories of risk in small business

This section overviews the categories of risk a small business owner may face. It does not provide an exhaustive list of risk categories, but may guide the development of a risk management plan.

Sections 1 and 2 can be used by the business owner as a base for development of risk management practices.

3 The risk management process

Section 3 overviews the risk management process described by the Australian and New Zealand Standard for Risk Management (AS/NZS 4360) as it relates to small business.

Section 3 may interest both the business owner and other staff within the business, taking a step-by-step view of risk management.

4 Applying risk management

The application of risk management will differ from industry to industry and will depend on the size of the business. Many resources available currently are geared towards large organisations and may be too detailed and complex for application in a small business.

Section 4 will guide the business owner in applying risk management in the context of a small business.

5 Sustaining a risk management approach

Risk management is not simply a once-off exercise; it is an ongoing journey towards better business practice.

Section 5 provides tips and guidance on how risk management can be integrated into the overall management of a small business, to help achieve sustainability.

6 Risk management tools and activities

This guide is not just about theory. This section provides small businesses with a range of practical examples, tools and activities relevant to risk management and that can be applied in a risk management program.

Section 6 also suggests where to seek further assistance with risk management in small business.

Helpful resources

This guide provides a basic understanding of risk management in small business. Due to the diversity of the small business sector, it is difficult to ensure that the content of the guide answers all questions relating to the management of risk.

This section provides a list of contacts and websites for more information regarding risk management and assistance for small business.

Glossary

Effective risk management will create a positive risk culture in a business. One of the ways to achieve this is to ensure consistency in terminology relating to risk management.

This section is a glossary of terms to assist business owners to understand the information provided in this guide.

Bibliography

This section provides details of the references used to develop this document.

Picture icons

This guide contains picture icons to assist you.

The 'Tool Box' icon indicates a tool for implementing risk management practices or theories.

The 'Tips' icon indicates a useful tip to assist in applying a particular principle or process.

The 'Case Study' icon denotes an example used to illustrate a theory or concept.

Acknowledgements

This guide has been developed by Global Risk Alliance on behalf of the New South Wales Department of State and Regional Development.

Global Risk Alliance is an Australian-based company specialising in the provision of risk management services. Further information can be found at **www.globalriskalliance.com**

The Global Risk Alliance team included:

Authors

Kimberley Turner (CPRM), Chief Executive Officer of Global Risk Alliance and **Deanne Keetelaar** (CPRM), a risk management advisor for Global Risk Alliance.
Telephone: (02) 8336 3777 Email: admin@globalriskalliance.com www.globalriskalliance.com

Peer review

This document has been technically reviewed by the **Risk Management Institution of Australasia (RMIA)** Education and Professional Development Committee. RMIA is a representative organisation dedicated to advancing the discipline and practice of risk management. Its mission is to champion risk management as a legitimate business discipline in its own right and to foster and develop risk management professionalism. Further information can be found at **www.rmia.org.au**

1 Risk management principles and concepts

1 Risk management principles and concepts

1.1 Demonstrating good governance practice for small business

Governance in business refers to the way a business is directed and controlled, including structure, culture, goal-setting and decision-making.

Good governance focuses on areas such as:

- **good business conduct** – including management of areas such as customer relations, transparent finances, resources and staff management
- **quality outcomes** – ensuring that the products developed or the services provided by the business are of the highest quality and standard
- **compliance** – ensuring that the business complies with all required regulations, legislation and standards on an ongoing basis
- **risk management** – protecting the business from possible negative occurrences, as well as recognising opportunities and capitalising on these when they arise.

Effective governance can help improve performance, satisfy customer needs and meet compliance requirements. Risk management is an integral part of business governance.

This guide will help business owners to understand where and how risk management can assist the process of good governance.

1.2 Defining risk and risk management

Anything that has the potential to impact upon these objectives is considered a risk.

Risk is inherent in life. Everything we do involves risk.

A business owner chooses to take risks every day. Often business owners rely on experience and intuition to manage risk. However, the more complex the business, the more important it is to identify risks that may prevent a business from realising its potential, and to manage them in order to minimise adverse outcomes and maximise positive outcomes.

'Risk' can be defined as the chance of something happening that will impact upon objectives. [2]

To put this into perspective, the objectives of a small business might be: to provide the best quality service; to maximise revenue and decrease expenses; to have quality employees; to increase productivity and product quality; and to increase market share.

Risk may have positive or negative outcomes, resulting in either an opportunity or a loss for a business (opportunity-based risk will be further explored later in this section).

Risk management is the way in which adverse effects from risk are managed and potential opportunities are realised. Therefore, risk management involves:

- minimising those things that may negatively impact upon a business
- identifying and harnessing those things that will help to achieve the goals and objectives of a business.

[2] As defined in the Australian/New Zealand standard for risk management [AS/NZS 4360].

1.3 Types of risk

Every risk has its own distinct characteristic that requires particular management or analysis. Most people will recognise the 'obvious', or most apparent, risk that they are facing. For example, the owner of a take-away restaurant will immediately recognise the risk to the safety of their staff from using hot cooking oil and implements. However, the risk to the business from a new local competitor may not be as readily identified.

An emerging concept in risk management is that there are three types of risk:

- opportunity-based risk
- uncertainty-based risk
- hazard-based risk.

Figure 1.1 Three types of risk and their management

Opportunity-based risk

There are two main aspects of opportunity-based risks: risks associated with not taking an opportunity and those associated with taking an opportunity.

The latter is a conscious decision to accept identified risk associated with an opportunity and then to implement processes to minimise any negative impacts and maximise gains.

Opportunity-based risk may or may not be visible or physically apparent; it is often financial; it can have a positive or negative outcome; and it can have both short-term and longer-term outcomes.

Opportunity-based risks for small business include: moving a business to a new location; acquiring new property; expanding a business; and diversifying a product line.

Uncertainty-based risk

Uncertainty-based risk is the risk associated with unknown and unexpected events. This type of risk has attracted more recognition as a result of events such as Y2K, September 11 and recent natural disasters such as the Asian tsunami.

Uncertainty-based risks are: unknown or extremely difficult to quantify; catastrophic or disastrous in nature; associated with negative outcomes; and not possible to control or influence.

Uncertainty-based risks for small business include: physical damage or damage to buildings by fire or flood; financial loss; loss of a vital supplier; unexpected loss of insurance; and loss of market share.

Preparing for uncertainty

By their very nature, disaster and the unexpected are unpredictable. A business owner must plan accordingly and determine how to minimise business disruption.

Case study – opportunity-based risk

A clothing retail store is operating in a shopping strip of a suburb of a large city. The business relies on passing trade for sales and has had to do very little marketing over the four years of operation.

In recent times sales have been steadily decreasing. In review of the sales figures and the reasons for decreasing sales, the business owner recognises that the foot traffic on the shopping strip significantly reduced when a shopping centre was established only five kilometres away.

The business owner had resisted moving to the shopping centre in support of the survival of the shopping strip. However, the risk to the survival of the business is now obvious and the business owner must decide to relocate or to implement additional sales and marketing strategies.

Managing the risks

Opportunities associated with changing location include:

- increased foot traffic
- increased sales
- joint marketing with the shopping centre tenants and participation in special events to raise profile.

Risks associated with changing location include:

- increased competition
- loss of regular customers
- business damage to reputation in the local community
- significant increase in fit-out, leasing and marketing costs.

The business owner must decide whether the opportunity for the survival of the business outweighs the risks. If not, alternative strategies for boosting sales must be considered.

Case study – uncertainty-based risk

A local gardening business services a small rural town. The volume of business is enough to justify the employment of two staff on a part-time basis. It is a home business, that has been in operation for three years, and is the only one of its type in the town.

A new operator moves to the town and is operating under the branding of a popular franchise well known for the delivery of quality gardening services.

The business owner of the existing gardening business is now faced with a major competitor and is at risk of losing market share.

Managing the risks

The original business owner previously developed a risk management plan that had identified this contingency as an uncertainty-based risk.

The treatment strategy was to diversify services and to offer home maintenance services as well as gardening services. Previous market research supported this approach and the business owner will be able to continue to employ the existing staff and to consider employing one other.

There are various management methods to minimise the impact of uncertain events on a business.

Examples are:

- disaster and emergency planning
- planning to recover from a disaster
- business continuity planning to ensure a business can continue to operate after a major disruption.

Hazard-based risk

Hazard-based risk is the risk associated with a source of potential harm or a situation with the potential to cause harm. This is the most common one associated with business risk management, as addressed by occupational health and safety programs.

Hazard-based risks for small business include:

- **physical hazards** – including noise, temperature or other environmental factors
- **chemical hazards** – including storage and/or use of flammable, poisonous, toxic or carcinogenic chemicals
- **biological hazards** – including viruses, bacteria, fungi and other hazardous organisms
- **ergonomic hazards** – including poor workspace design, layout or activity and equipment usage
- **psychological hazards** –that may result in physical or psychological harm, including bullying, sexual discrimination, workload or mismatch of job specification to employee capability.

Case study – hazard-based risk

A small cleaning company specialises in providing contract cleaning services for medical providers. A recent OH&S audit conducted internally by this company identified the following hazards:

- manual handling tasks including heavy lifting and repetitive, forceful or awkward movements
- the work environment, including wet floors and cluttered workspaces
- unsafe work practices, including faulty electrical equipment
- prevalence of sharp materials resulting in exposure to dangerous blood-borne viruses
- the use of hazardous chemicals.

Managing the risks

To manage these hazard-based risks, the company trains staff to employ the hierarchy of controls for each new contract:

- **eliminate** – avoid wherever possible
- **substitute** – wherever possible use alternative methods or equipment
- **separate** – separate the hazard from workers wherever possible
- **redesign** – change the work layout, processes or equipment
- **administer** – change current work practices, train staff
- **protect** – consider all other control options first and then provide staff with protective equipment.

1.4 Drivers of risk management – why manage risk?

Risk management should be considered from the following three perspectives:

- why you ***want*** to implement risk management
- why you ***should*** implement risk management
- why you ***have*** to implement risk management.

Why you *want* to – benefits of risk management

Small businesses can expect to encounter many benefits from applying risk management principles in a structured and systematic way. These include:

- improved communication between staff and with external stakeholders
- improved understanding of the impacts that management practices have on a business

- improved relationships with stakeholders such as clients, employees, suppliers and contractors
- enhanced business planning and achievement of objectives and goals
- reduced litigation potential
- increased competitive advantage
- enhanced quality of product or service
- increased efficiency and productivity
- reduced budget blowouts
- reduced compliance costs.

Why you *should* – good business practices

There are many reasons why a business owner should apply risk management and these include:

- increased transparency in financial management
- enhanced staff confidence in a secure and safe work environment
- enhanced client confidence in the quality and integrity of a product or service
- protection of assets and the longer-term viability of the business.

Why you *have* to – legislative compliance

There are many legislative and regulatory requirements relating to risk management and these include:

- occupational health and safety legislation
- fair trading legislation
- contractual obligations
- insurance requirements
- financial reporting requirements.

1.5 Limitations of risk management

The limitations of risk management, as in any management process, should be clearly recognised by the business owner and management team.

These limitations include the following:

- *Risk management will not make decisions for the business*

  Risk management can assist a business owner to make decisions. However, these decisions will be limited by the depth of the research and analysis of risk, the individual (s) involved in the risk assessment, their relevant experience and exposure to risk management and, most importantly, who has not been involved

- *Risk management will not guarantee freedom from all risk*

  While it is impossible to be able to predict all negative consequences to a business, risk management can help a business owner to be prepared for an adverse consequence

- *Risk management will not guarantee that accidents won't happen*

  To err is human and where humans are involved there is always the possibility that a mistake may happen that will lead to an incident

- *Risk assessments will not be all-encompassing and are therefore not fail-safe*

  The risk assessment should attempt to identify all significant risk but it will be limited by the resources available, including information at hand, involvement of stakeholders, time and budget.

2 Categories of risk in small business

2 Categories of risk in small business

There are many examples of risk in small business. In order to identify these risks, it is helpful to consider risks in 'areas' or 'categories'. For example, a business may encounter areas of risk such as financial risks, safety risks, reputation risks, or operational risks.

This section aims to provide guidance on how to determine the categories of risk specific to a small business and how these can be used in the risk management process.

2.1 What is a category of risk?

As previously discussed, risk can be opportunity-, uncertainty- or hazard-based. However, there are also many 'areas' or categories of risk that relate to small business.

Risk categories are specific areas or topics to be considered one by one, providing a structured approach to risk identification. This will enable a greater focus within a particular category, stimulating thought, and increasing the opportunity of identifying a broader range of risks.

2.2 The use of categories of risk

Risk categories can assist a business in risk planning and communicating risk information. They provide a structure for identifying risk and are often initially identified through a 'brainstorming' exercise.

In addition, understanding these categories assists the business owner to select the most appropriate tools and techniques for risk identification and analysis. For example, if a particular risk category is technical in nature, the risk identification methodology used may involve significant research and collection of existing information about risk exposure. A risk category with a more strategic focus, such as commercial risk, may involve a structured brainstorming exercise or SWOT analysis (Section 3.4).

2.3 Common risk categories in small business

Some categories of risk in small business are shown in Table 2.1.

Table 2.1. Some categories of risk in small business

Risk Category			
• Financial • Equipment • Organisational • Security	• Legal & regulatory compliance • Reputation • Operational	• Service delivery • Commercial • Project • Safety	• Stakeholder management • Strategic • Technology

2.4 Definition of risk categories

The following provides further definition of the risk categories suggested in Section 2.3. Please note that this is not an exhaustive list. The risk categories will be particular to the specific business or activity the risk identification exercise is being conducted for.

Table 2.2. Definition of risk categories in small business

Financial	This category includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
Organisational	This relates to the internal requirements of a business, extending to the cultural, structural and people issues associated with the effective operation of the business.
Compliance / legal	This category includes compliance with legal requirements such as legislation, regulations, standards, codes of practice and contractual requirements. This category also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.
Operational	This covers the planning, operational activities, resources (including people) and support required within the operations of a business that result in the successful development and delivery of a product or service.
Commercial	This category includes the risks associated with market placement, business growth, diversification and commercial success. This relates to the commercial viability of a product or service, and extends through establishment to retention and then growth of a customer base.
Safety	This category includes the safety of everyone associated with the business. This extends from individual safety, to workplace safety, public safety and to the safety and appropriateness of products or services delivered by the business.
Strategic	This includes the planning, scoping and resourcing requirements for the establishment, sustaining and/or growth of the business.
Equipment	This extends to the equipment utilised for the operations and conduct of the business. It includes the general operations of the equipment, maintenance, appropriateness, depreciation, safety and upgrade.
Security	This includes the overall security of the business premises, assets and people, and extends to security of information, intellectual property, and technology.
Reputation	This entails the threat to the reputation of the business due to the conduct of the entity as a whole, the viability of product or service, or the conduct of employees or other individuals associated with the business.
Service delivery	This relates to the delivery of services, including the quality and appropriateness of service provided, or the manner in which a product is delivered, including customer interaction and after-sales service.
Project	This includes the management of equipment, finances, resources, technology, timeframes and people associated with the management projects. It extends to internal operational projects, projects relating to business development, and external projects such as those undertaken for clients.
Stakeholder management	This category relates to the management of stakeholders, and includes identifying, establishing and maintaining an appropriate relationship. This includes both internal and external stakeholders.
Technology	This includes the implementation, management, maintenance and upgrades associated with technology. This extends to recognising the need for and the cost benefit associated with technology as part of a business development strategy.

2.5 Integrating risk management in small business

Risk management in a small business should not be a stand-alone program. There are relationships between risk management and many of the management processes and techniques that may be employed to ensure the successful operation of a business. All of these will interrelate and should complement each other (Figure 2.1).

Figure 2.1 The wheel of integration

Business planning

Business planning is an important management technique in a business of any size and risk management can assist greatly in the business planning process. It can achieve this by assisting the business to effectively manage the weaknesses and threats to achieving the objectives of the business, as well as recognising where opportunities exist and capitalising on these to help the business grow and develop.

In addition, combining risk management planning with business planning will serve as a prompt to ensure that the risks and opportunities at a business level are identified and reviewed on an annual basis, in line with annual business planning.

Occupational health and safety (OH&S)

Every business has a 'duty of care' underpinned by state and federal legislation. This means that everything 'reasonably practicable' must be done to protect the health and safety of others at the workplace. This duty is placed on all employers, their employees and any others who have an influence on the hazards in a workplace (such as contractors and other external suppliers).

This integrates with the overall risk management strategy by ensuring that risks and hazards are identified/reported on an ongoing basis and measures are taken to reduce the exposure to this risk to as low as reasonably practicable.

Human resources management

Human resources management is closely linked with risk management. If a business is large enough to employ staff, there are many risk considerations that should be taken into account. For example:

- has the right person been employed for the job?
- is the person appropriately qualified, skilled and able to perform the task required of them?
- does the employee's performance align with the requirements of the business?
- is the client/customer satisfied with the level of service or product provided?

- has the right direction and guidance for employees been provided to ensure they understand the tasks allocated?
- are resources adequate or appropriate to meet the needs of the role, including training?
- is the business complying with anti-discrimination laws?
- is the remuneration provided compliant with award wages?

The risk management program will assist the business owner to identify risks associated with human resource management and to identify the treatment strategies to manage these appropriately, and monitor them on an ongoing basis.

Compliance

A business owner should be aware of and feel confident that areas requiring compliance have been identified and are not breached at any time. These include:

- legislation and regulations, such as OH&S, fair trading, anti-discrimination, environmental protection, industrial relations, taxation, and various trading and licence practices
- contracts, such as those with a client, sub-contractor, insurer or supplier
- insurance requirements
- financial reporting requirements.

A risk management program can assist a business owner to develop a clear understanding of the areas of compliance that must be managed and monitored, including the risks associated with potential breach and what can be done to avoid that breach.

Financial management

Any successful business relies on effective, transparent financial management. This includes maximising income, determining the pricing for a product or service, minimising and managing expenses (e.g. bills and correct wages paid on time) and ensuring creditors honour their accounts. Financial management is also about recognising and capitalising on opportunities.

Determining where both financial risks and opportunities exist can assist in ensuring that the financial management of the business is both efficient and effective.

Client–customer relationship management

Client-customer relationship management relates to the steps taken to ensure that the satisfaction of existing customers or clients is maximised to ensure their ongoing patronage. This will help to create a steady income from existing customers, as well as creating opportunities to attract new customers (e.g. from word of mouth).

A risk management program helps to identify existing relationships with clients or customers and to minimise their degradation. The complaints management system is an excellent source of retrospective risk, and if managed effectively, the quality of the service or product will increase.

Contract management

Most businesses rely on daily contracts with either individuals or other businesses. These may include suppliers, clients or sub-contractors. The contract may exist in a verbal or written form.

Contract management demands that the objectives and requirements for a partnership are clearly specified, and that particular obligations are met appropriately.

For example, if a business owner is outsourcing an important aspect of the business to a sub-contractor, the relevant requirements and expectations should be clearly stated. This will assist in avoiding breaches of the contract and improve the relationship.

If the business is sub-contracted to a larger organisation, it is important to be aware of the latter's risk management framework and requirements. For example, an annual external safety audit may be required. If the business owner does not have the resources available to comply with the risk management requirements of the larger organisation, this should be recognised as a risk in the first instance and managed appropriately.

All contracts contain risk but, if managed effectively, they can help to protect a business and its staff. Further advice should be sought if there is any uncertainty.

Quality assurance

A quality assurance program requires action to ensure the product or service fulfils customer expectations.

Quality assurance is integral to risk management: it is the process that continues from risk treatment through monitoring and reviewing to a cycle of continuous improvement.

3 The risk management process

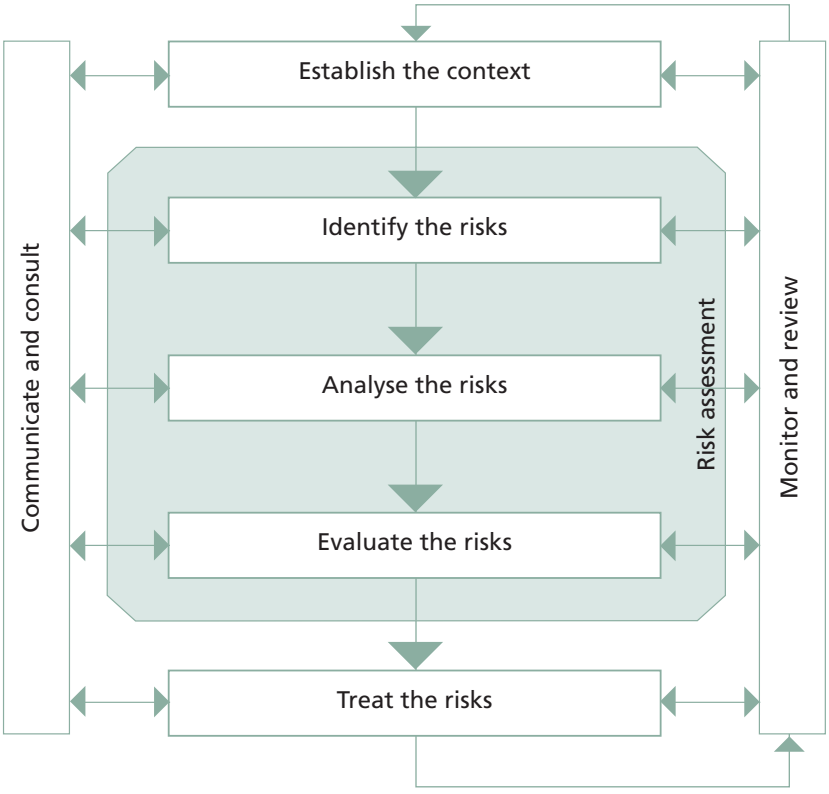
3 The risk management process

3.1 What is the risk management process?

The risk management process consists of a series of steps that, when undertaken in sequence, enable continual improvement in decision-making.

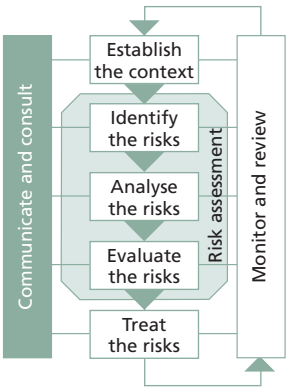
The elements of the risk management process are summarised in Figure 3.1.

Figure 3.1 The risk management process (AS/NZS 4360)



3.2 Step 1. Communicate and consult

Communication and consultation is ultimately one of the most important aspects of risk management and is integral to the entire risk management process.



This is shown in Figure 3.1 by the arrows against each step.

Communication and consultation aims to identify who should be involved in assessment of risk (including identification, analysis and evaluation) and it should engage those who will be involved in the treatment, monitoring and review of risk.

As such, communication and consultation will be reflected in each step of the process described in this guide.

As an initial step, there are two main aspects that should be identified in order to establish the requirements for the remainder of the process. These are communication and consultation aimed at:

- eliciting risk information
- managing stakeholder perceptions for management of risk.

Eliciting risk information

Communication and consultation may occur within the organisation or between the organisation and its stakeholders.

It is very rare that only one person will hold all the information needed to identify the risks to a business or even to an activity or project. It is therefore important to identify the range of stakeholders who will assist in making this information complete.

Case study – stakeholder management

A small family construction business consists of two brothers in a partnership structure. The business sub-contracts various tradespeople, such as plumbers, electricians and bricklayers, to complete their projects.

The business recently commenced work on a new development where land had been re-zoned. Unfortunately the business did not consult the sub-contractors when preparing the quote, expecting that it would be a straightforward job. When the project starts, the regular plumber identifies significant plumbing difficulties and indicates that the job will cost nearly twice the normal fee due to differing equipment and increased labour.

As such, the business finds it increasingly difficult to attract a sub-contractor who will provide the service within the price range quoted to the customer, and the business has to absorb the loss. This impacts greatly on their cash flow, as well as placing great strain on the partnership. The brothers consider dissolving the partnership as a result.

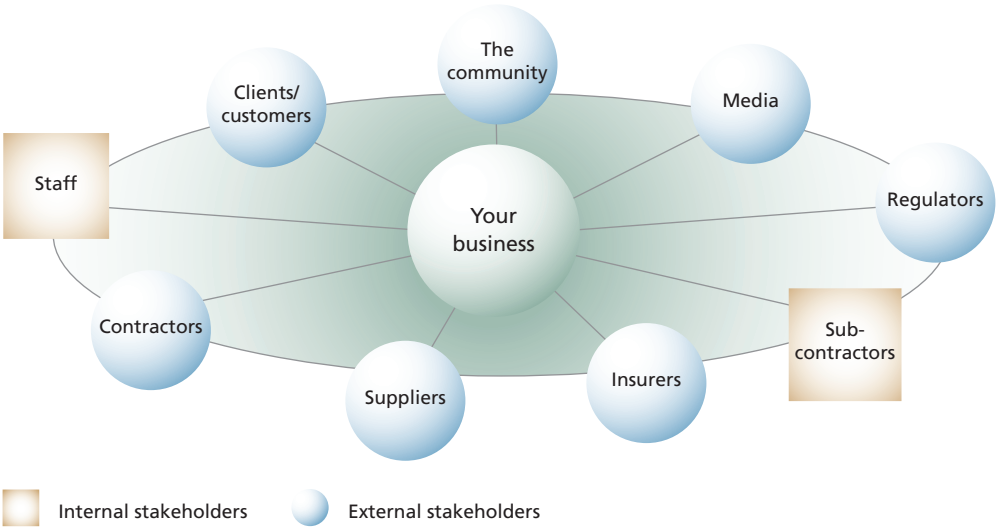
To ensure effective communication, a business owner may decide to develop and implement a communication strategy and/or plan as early as possible in the process. This should identify internal and external stakeholders and communicate their roles and responsibilities, as well as address issues relating to risk management.

Consultation is a two-way process that typically involves talking to a range of relevant groups and exchanging information and views. It can provide access to information that would not be available otherwise.

Managing stakeholder perceptions for management of risk

There will be numerous stakeholders within a small business and these will vary depending upon the type and size of the business (Figure 3.2).

Figure 3.2 Stakeholders in small business



Stakeholder management can often be one of the most difficult tasks in business management. It is important that stakeholders are clearly identified and communicated with throughout the risk management process.

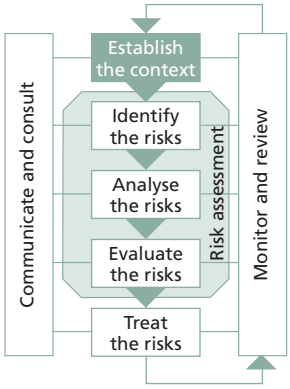
They can have a significant role in the decision-making process, so their perceptions of risks, as well as their perceptions of benefits, should be identified, understood, recorded and addressed.

Stakeholder communication should incorporate regular progress reports on the development and implementation of the risk management plan and in particular provide relevant information on the proposed treatment strategies, their benefits and planned effectiveness.

Tips for effective communication and consultation

- Determine at the outset whether a communication strategy and/or plan is required
- Determine the best method or media for communication and consultation
- The significance or complexity of the issue or activity in question can be used as a guide as to how much communication and consultation is required: the more complex and significant to the organisation, the more detailed and comprehensive the requirement.

3.3 Step 2. Establish the context



When considering risk management within a small business, it is important to first establish some boundaries within which the risk management process will apply. For example, the business owner may be only interested in identifying financial risks; as such the information collected will pertain only to that area of risk.

AS/NZS 4360 provides a five-step process to assist with establishing the context within which risk will be identified.

1. Establish the internal context

As previously discussed, risk is the chance of something happening that will impact on objectives. As such, the objectives and goals of a business, project or activity must first be identified to ensure that all significant risks are understood. This ensures that risk decisions always support the broader goals and objectives of the business. This approach encourages long-term and strategic thinking.

Case study – establishing the internal context

An electrician employs one full-time staff member and an apprentice, who is nearly halfway through completing his apprenticeship. The business has recently lost a major contract to a competitor, which has significantly affected the cash flow. In response, the electrician regretfully retrenches the apprentice, but does so in order to maintain the employment of the other staff member, who has a family to support.

In six months time the business wins a three-year contract with a local primary school. The business owner had identified this opportunity in his business plan and had been preparing for this contract for some time.

The contract provides more work than the business is able to cope with utilising existing staff. Unfortunately the previous apprentice has found work with another company and, therefore, the business must employ a new apprentice. This results in increased stress on the existing staff, who are then required to train and supervise a junior staff member.

The business owner may have been better off looking for other options to increase cash flow or reduce expenses, recognising the investment already made in training the first apprentice, and to maintain the knowledge and confidence of the first apprentice.

In establishing the internal context, the business owner may also ask themselves the following questions:

- Is there an internal culture that needs to be considered? For example, are staff resistant to change? Is there a professional culture that might create unnecessary risks for the business?
- What staff groups are present?
- What capabilities does the business have in terms of people, systems, processes, equipment and other resources?

2. Establish the external context

This step defines the overall environment in which a business operates and includes an understanding of the clients' or customers' perceptions of the business. An analysis of these factors will identify the strengths, weaknesses, opportunities and threats to the business in the external environment. A business owner may ask the following questions when determining the external context:

- What regulations and legislation must the business comply with?
- Are there any other requirements the business needs to comply with?

- What is the market within which the business operates? Who are the competitors?
- Are there any social, cultural or political issues that need to be considered?

Establishing the external context should also involve examining relationships the business has with external stakeholders for risk and opportunity.

Tips for establishing internal and external contexts

- Determine the significance of the activity in achieving the organisation's goals and objectives
- Define the operating environment
- Identify internal and external stakeholders and determine their involvement in the risk management process.

3. Establish the risk management context

Before beginning a risk identification exercise, it is important to define the limits, objectives and scope of the activity or issue under examination. For example, in conducting a risk analysis for a new project, such as the introduction of a new piece of equipment or a new product line, it is important to clearly identify the parameters for this activity to ensure that all significant risks are identified.

Establishing the parameters and boundaries of the activity or issue also involves the determination of:

- timeframe (e.g. how long will it take to integrate a new piece of equipment?)
- resources required
- roles and responsibilities
- additional expertise required
- internal and external relationships (e.g. other projects, external stakeholders)
- record-keeping requirements
- depth of analysis required.

The amount of analysis required for this step will depend on the type of risk, the information that needs to be communicated and the best way of doing this. To determine the amount of analysis required consider the:

- complexity of the activity or issue
- potential consequence of an adverse outcome
- importance of capturing lessons learned so that corporate knowledge of risk associated with the activity can be developed
- importance of the activity and the achievement of the objectives
- information that needs to be communicated to stakeholders
- types of risks and hazards associated with the activity.

Tips for establishing the risk management context

- Define the objectives of the activity, task or function
- Identify any legislation, regulations, policies, standards and operating procedures that need to be complied with
- Decide on the depth of analysis required and allocate resources accordingly
- Decide what the output of the process will be, e.g. a risk assessment, job safety analysis or a board presentation. The output will determine the most appropriate structure and type of documentation.

Case study – establishing the risk management context

A metal fabrication business employing 15 staff and operating from a factory in western NSW is relocating from its current premises into a larger factory because of business growth. Prior to the move the business owner decides to complete a risk assessment of the task.

The risk management context included:

- the primary objective: to successfully move the business to the new premises with minimal disruption to current levels of productivity
- a timeframe for completion of one month
- a budget of $10,000 for external support for relocation
- availability of three additional staff to assist in the move.

Discussion

From a risk management perspective, this information provides the business owner with enough information to assess the risks that may impact on the primary objective, to identify the possible events or circumstances that may cause significant disruption to current levels of productivity.

4. Develop risk criteria

Risk criteria allow a business to clearly define unacceptable levels of risk. Conversely, risk criteria may include the acceptable level of risk for a specific activity or event. In this step the risk criteria may be broadly defined and then further refined later in the risk management process.

It is against these criteria that the business owner will evaluate an identified risk to determine if it requires treatment or control. Where a risk exists that may cause any of the objectives not to be met, it is deemed unacceptable and a treatment strategy must be identified.

The table below (Table 3.1) provides a number of examples of risk criteria for a project.

Table 3.1. Examples of risk criteria for a project in small business

Risk criterion	Objective
Safety	Safety must be upheld at all times. No injuries or fatalities will be accepted
Financial impact	Project costs should remain within allocated budget
Media exposure	The project must ensure that the reputation of the business is protected from negative media exposure
Timing	The project must be completed within the contractual timeframe
Staff management	The project must utilise existing staff skills. Where a particular skill set is not available, sub-contracting may be considered
Environment	The project must operate within requirements of environmental legislation and be consistent with the business's environmental commitment

Tips for developing risk criteria

- Decide or define the acceptable level of risk for each activity
- Determine what is unacceptable
- Clearly identify who is responsible for accepting risk and at what level.

5. Define the structure for risk analysis

Isolate the categories of risk that you want to manage. This will provide greater depth and accuracy in identifying significant risks.

The chosen structure for risk analysis will depend upon the type of activity or issue, its complexity and the context of the risks. Examples of risk categories for a particular risk analysis are provided in the following case study.

Case study – defining the structure for risk analysis

A boat builder located on the NSW central coast develops unique designs and innovations. His business has been steady for nearly 20 years, sustaining a staff of three tradesmen and one factory hand/driver. He leases all his major equipment.

He is nearing retirement age and for the past three years his son-in-law has been working in the business, preparing to take it over. The son-in-law has a sales background and is keen to expand the business, identifying a market for the business in other locations around the country.

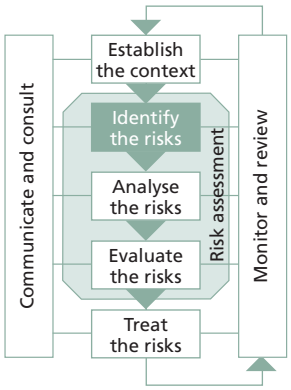
The boat builder agrees to consider allowing his son-in-law to travel to specific locations in each state with an example of their craftsmanship, to attempt to enter the market outside of the local area. In planning for this trip, the son-in-law decides to complete a risk analysis to give his father-in-law confidence that the trip is well planned. The key risk categories of the project identified include:

- transport (e.g. mechanical problems)
- finances and general resources (e.g. exceeding budgetary requirements)
- logistics of individual locations (e.g. access, storage, weather)
- commercial risks (e.g. possible competitors)
- administration risks (e.g. follow-up of enquiries)
- general operations (e.g. timings for the trip).

Discussion

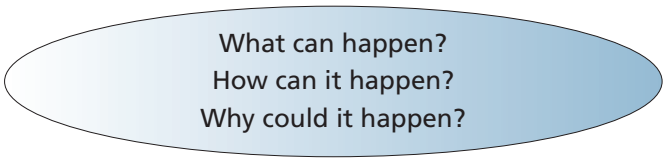
This approach allows the business to clearly identify the risks involved in the venture and informs the decision of the business owner to accept or not accept various identified risks. This will help the boat builder to decide whether this will be a viable venture for the business, or whether the risks outweigh the benefits.

3.4 Step 3. Identify the risks



Risk cannot be managed unless it is first identified. Once the context of the business has been defined, the next step is to utilise the information to identify as many risks as possible.

The aim of risk identification is to identify possible risks that may affect, either negatively or positively, the objectives of the business and the activity under analysis. Answering the following questions identifies the risk:



There are two main ways to identify risk:

- retrospectively
- prospectively.

Identifying retrospective risks

Retrospective risks are those that have previously occurred, such as incidents or accidents.

Retrospective risk identification is often the most common way to identify risk, and the easiest. It's easier to believe something if it has happened before. It is also easier to quantify its impact and to see the damage it has caused.

There are many sources of information about retrospective risk. These include:

- hazard or incident logs or registers
- audit reports
- customer complaints
- accreditation documents and reports
- past staff or client surveys
- newspapers or professional media, such as journals or websites.

Identifying prospective risks

Prospective risks are often harder to identify. These are things that have not yet happened, but might happen some time in the future.

Identification should include all risks, whether or not they are currently being managed. The rationale here is to record all significant risks and monitor or review the effectiveness of their control.

Methods for identifying prospective risks include:

- brainstorming with staff or external stakeholders
- researching the economic, political, legislative and operating environment
- conducting interviews with relevant people and/or organisations
- undertaking surveys of staff or clients to identify anticipated issues or problems
- flow charting a process
- reviewing system design or preparing system analysis techniques.

Risk categories will help break down the process for prospective risk identification. It is important to remember that risk identification will be limited by the experiences and perspectives of the person(s) conducting the risk analysis. Problem areas and risks can be identified with the help of reliable sources.

SWOT analysis

An effective method for prospective risk identification is to undertake a strengths,

weaknesses, opportunities and threats (SWOT) analysis. A SWOT analysis is a tool commonly used in planning and is an excellent method for identifying areas of negative and positive risk at a business level.

A sample SWOT analysis for a plumbing business is shown in Figure 3.3.

Figure 3.3 SWOT analysis example for a plumbing business

Positive risk	**Strengths** • Exceptionally skilled tradespeople • Excellent relationships with existing customers • High-quality work and reliable service.	**Weaknesses** • Second-hand tools of trade, may be unreliable • Ageing workforce • Limited familiarity with new technology.
	Opportunities • Retirement of only other plumber in town • New industry development currently tendering to outsource trade services.	**Threats** • Purchase of retiring plumber's business by somebody from out of town • Startup of another business in town • Difficulties in recruiting new staff due to skill shortages • Loss of an existing employee, leaving the business unable to cope with workload.
		Negative risk

Refer to Section 6.1 for a summary definition of risk identification methodologies.

Tips for effective risk identification

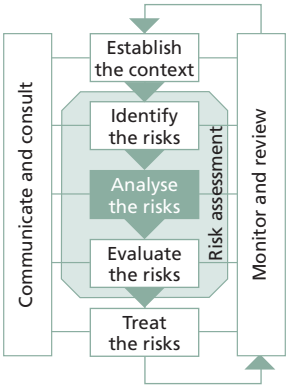
- Select a risk identification methodology appropriate to the type of risk and the nature of the activity
- Involve the right people in risk identification activities
- Take a life cycle approach to risk identification and determine how risks change and evolve throughout this cycle.

Case study – risk identification

A childcare centre in an inner city location is operating from a rented site. An accreditation requirement for the centre is to develop a strategic risk management plan. The business owner sets the following elements for which the risk analysis will be conducted and the methods to be used for risk identification.

Key element	Risk identification method
Financial management	External financial audit
Staff management	Staff interviews Competency testing
Compliance	Compliance mapping to map regulations, legislation and accreditation standards
Health and safety	OH&S audit
Reputation	Client satisfaction survey
Environmental impact	Structured interview with stakeholders
Facility management	Site inspection for assets and equipment Structured focus groups with stakeholders
Operations – general running of the business	SWOT analysis with staff

3.5 Step 4. Analyse the risks



During the risk identification step, a business owner may have identified many risks and it is often not possible to try to address all those identified.

The risk analysis step will assist in determining which risks have a greater consequence or impact than others.

This will assist in providing a better understanding of the possible impact of a risk, or the likelihood of it occurring, in order to make a decision about committing resources to control the risk.

What is risk analysis?

Risk analysis involves combining the possible consequences, or impact, of an event, with the likelihood of that event occurring. The result is a 'level of risk'. That is:

Risk = consequence x likelihood

This is discussed further later in this section.

So how is the level of risk determined?

Elements of risk analysis

The elements of risk analysis are as follows:

1. Identify existing strategies and controls that act to minimise negative risk and enhance opportunities.
2. Determine the consequences of a negative impact or an opportunity (these may be positive or negative).
3. Determine the likelihood of a negative consequence or an opportunity.
4. Estimate the level of risk by combining consequence and likelihood.
5. Consider and identify any uncertainties in the estimates.

1. Identify existing strategies and controls that act to minimise negative risk and enhance opportunities

To provide a clear understanding of the possible impact of a risk, existing control measures should first be identified and then the risk analysed to determine the amount of 'residual risk'.

For example, the risk of theft from a business is reduced by the employment of a security camera. However, this has not eliminated the risk – a residual risk remains.

2. Determine the consequences of a negative impact or an opportunity (these may be positive or negative)

Consequences are the possible outcomes or impacts of an event. They can be positive or negative, and can be expressed in quantitative or qualitative terms and are considered in relation to the achievement of objectives.

It is necessary to estimate the impact of a risk or opportunity on the identified objectives.

For example, the consequence of failing to maintain a major piece of machinery may be major injury requiring hospitalisation, or possible death, of an employee.

Refer to Section 6.2 for examples of consequence descriptors.

3. Determine the likelihood of a negative consequence or an opportunity

Likelihood relates to how likely an event is to occur and its frequency.

An example is the likelihood that a non-maintained piece of machinery will malfunction and result in major injury requiring hospitalisation, or possible death, of an employee.

* Likelihood = probability x exposure

Likelihood relates to the probability of a risk occurring combined with the exposure to the risk. This means that although the probability of a risk resulting in a negative outcome may be deemed rare, a higher frequency of exposure to that risk can increase the overall likelihood of a negative outcome.

For example, based upon experience, the probability that an experienced courier company will encounter an increased accident rate is low when delivering within regional areas. However, this probability increases considerably when exposed to heavier traffic, e.g. if the business decides to relocate to a larger city.

Refer to Section 6.2 for examples of likelihood descriptors.

4. Estimate the level of risk by combining consequence and likelihood

As previously introduced, to determine the level of risk, risk analysis involves combining the consequence of a risk with the likelihood of the risk occurring:

Risk = consequence x likelihood*

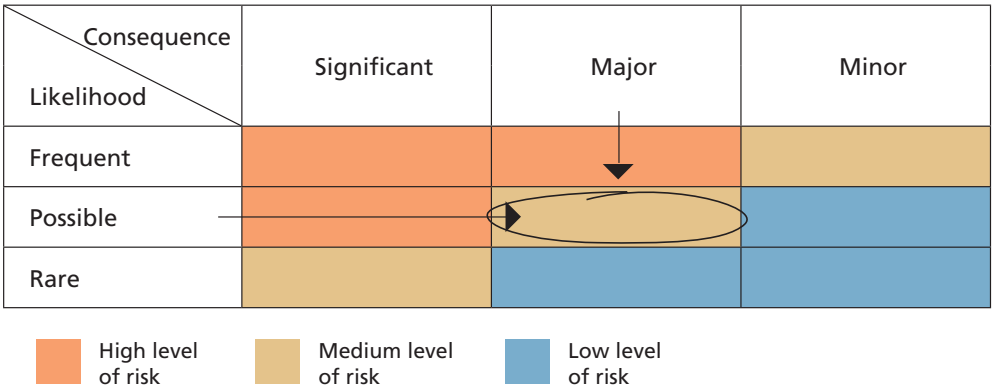
This is known as the '**risk analysis equation**'.

Techniques for determining the value of consequence and likelihood include descriptors, word pictures, or mathematically determined values. These are further described later in this section.

Most commonly, the overall level of risk is determined by combining the identified consequence level with the likelihood level in a matrix (Figure 3.4).

Refer to Section 6.2 for an example of a risk analysis tool.

Figure 3.4 Risk analysis matrix for determining level of risk



Note: This has been included as an example only and should not be used for analysis of risk in your business. Refer to Section 6.2 for an example of a risk analysis tool plus descriptors of consequence and likelihood.

5. Consider and identify any uncertainties in the estimates

In all estimates of likelihood and consequence, uncertainties will exist. This is a common limitation of the risk management process. It is important therefore to consider and identify any uncertainty. It may not be necessary to act on that uncertainty, but be aware and monitor any increases in the risk level.

Analysis techniques

The purpose of risk analysis is to provide information to business owners to make decisions regarding priorities, treatment options, or balancing costs and benefits. Just as decisions differ, the information needed to make these decisions will also differ.

Not all businesses or even areas within a business will use the same risk analysis method. For example, a doctor's clinic will have very different types of risk from a software developer. As such, the risk analysis tools need to reflect these risk types to ensure that the risk levels estimated are appropriate to the context of the business.

Types of analysis

Three categories or types of analysis can be used to determine level of risk:

- qualitative
- semi-quantitative
- quantitative.

The most common type of risk analysis is the qualitative method. The type of analysis chosen will be based upon the area of risk being analysed. More information regarding the semi-quantitative and quantitative techniques can be found within the Australian and New Zealand Standard *Risk Management Guidelines* (HB 436:2004).

Qualitative risk analysis

This form of risk analysis relies on subjective judgement of consequence and likelihood (i.e. what might happen in a worst case scenario). It produces a word picture of the size of the risk and is a viable option where there is no data available.

Qualitative risk analysis is simple and easy to understand. Disadvantages include the fact that it is subjective and is based on intuition, which can lead to the forming of bias and can degrade the validity of the results.

Methods for qualitative risk analysis include:

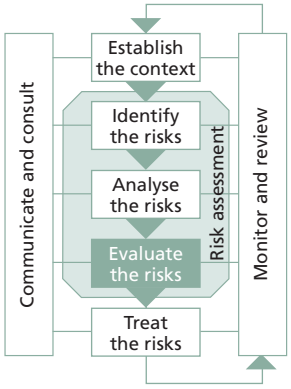
- brainstorming
- evaluation using multi-disciplinary groups
- specialist and expert judgement
- structured interviews and/or questionnaires
- word picture descriptors and risk categories.

Refer to Section 6.2 for an example of a common risk analysis tool.

Tips for effective risk analysis

- Risk analysis is usually done in the context of existing controls – take the time to identify them
- The risk analysis methodology selected should, where possible, be comparable to the significance and complexity of the risk being analysed, i.e. the higher the potential consequence the more rigorous the methodology
- Risk analysis tools are designed to help rank or prioritise risks. To do this they must be designed for the specific context and the risk dimension under analysis.

3.6 Step 5. Evaluate the risks



As discussed in Section 3.3, it is important to be able to determine how serious the risks are that the business is facing. The business owner must determine the level of risk that a business is willing to accept.

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria, and deciding whether these risks require treatment.

The result of a risk evaluation is a prioritised list of risks that require further action.

This step is about deciding whether risks are acceptable or need treatment.

Risk acceptance

Low or tolerable risks may be accepted. 'Acceptable' means the business chooses to 'accept' that the risk exists, either because the risk is at a low level and the cost of treating the risk will outweigh the benefit, or there is no reasonable treatment that can be implemented. This is also known as ALARP (as low as reasonably practicable).

A risk may be accepted for the following reasons:

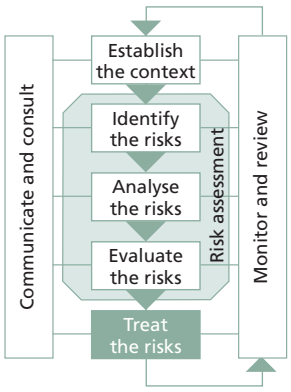
- The cost of treatment far exceeds the benefit, so that acceptance is the only option (applies particularly to lower ranked risks)
- The level of the risk is so low that specific treatment is not appropriate with available resources
- The opportunities presented outweigh the threats to such a degree that the risk is justified
- The risk is such that there is no treatment available, for example the risk that the business may suffer storm damage.

Case study – risk acceptance

A newsagent identifies a risk of theft from her store. Existing controls include mirrors and the counter being close to the front of the shop. In analysing this risk she identifies that an additional way of reducing the residual risk is to install a security camera and/or security alarms, which will alert staff if an item has been stolen. The cost of these treatment strategies is over $5000. The owner expects that the annual value of the items that might be stolen would be less than $1000. So she decides to accept this risk.

Discussion

Although the newsagent has decided to accept this risk, she should continue to regularly monitor the loss from the store. The majority of items sold are relatively inexpensive; however, should the store decide to stock larger items, or if the security of staff is compromised, or if the amount of loss increases above an acceptable level, or the cost of the treatment significantly reduces, the newsagent should reconsider the additional options for increasing security at the store.



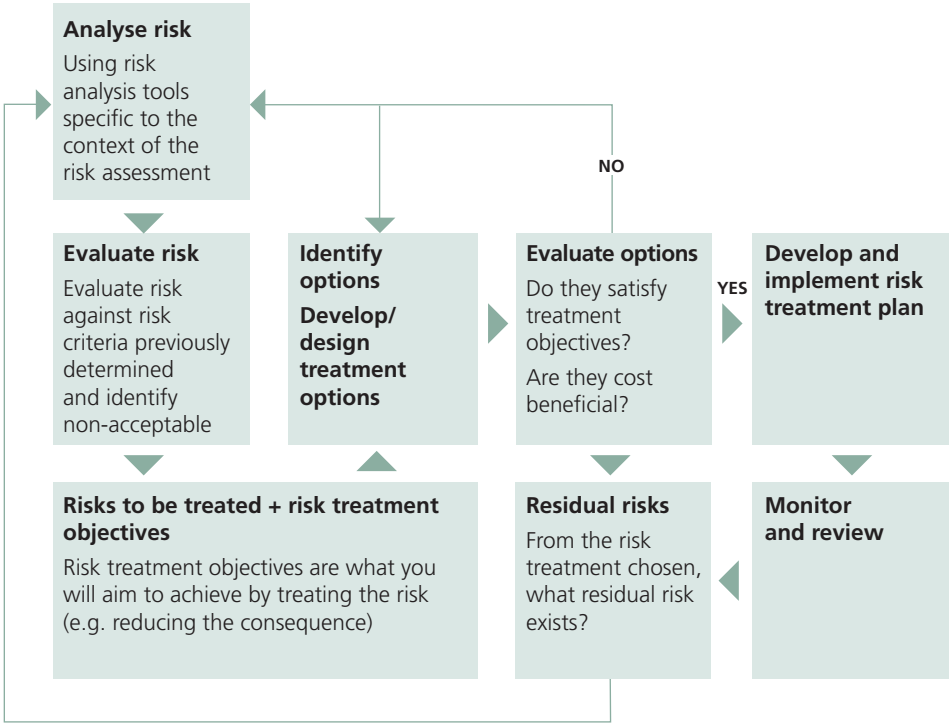
3.7 Step 6. Treat the risks

Risk treatment is about considering options for treating risks that were not considered acceptable or tolerable at Step 5.

Risk treatment involves identifying options for treating or controlling risk, in order to either reduce or eliminate negative consequences, or to reduce the likelihood of an adverse occurrence. Risk treatment should also aim to enhance positive outcomes.

It is often either not possible or cost-effective to implement all treatment strategies. A business owner should aim to choose, prioritise and implement the most appropriate combination of risk treatments. Figure 3.5 overviews the risk treatment process, including what needs to be considered in choosing a risk treatment.

Figure 3.5 Treating risks (modified from AS/NZS 4360)



Treating the root cause

Before a risk can be effectively treated, it is necessary to understand the 'root cause' of a risk, or how risks arise.

Case study – treating the root cause

The business owner of a mechanical repair shop employing five staff is concerned that his business is constantly running behind time. He has recently received multiple complaints from clients. His head mechanic cannot provide an adequate reason for this fall in productivity. He mentions that a new employee who has only been working for the firm for five weeks may be the reason. This new employee orders the supplies.

The head mechanic speaks to this new staff member on a number of occasions about his performance and tells him to improve it. The delays continue and the new employee is asked to leave.

Despite this action the delays in productivity continue. After some weeks, the business owner decides to close the shop for half a day and discuss the problem with his team. During discussion, it is revealed that there was a problem with the responsiveness of a new supplier. Although most staff had noticed this, each had considered the issue to be a 'once-off' and had not shared the information with the rest of the team.

Discussion

In this situation the root cause of the issue had not been identified in the first instance and so the risk issue was not effectively managed. Had the business owner or his senior staff member spent the time better understanding the issue at hand, the real cause of the problem may have been identified much earlier. The result would have been to retain the employee and not expose the business to risk of a claim for unfair dismissal, to manage the supply company in a more professional manner and to minimise impact on client satisfaction and therefore business reputation.

Options for risk treatment

AS/NZS 4360 identifies the following options that may assist in the minimisation of negative risk or an increase in the impact of positive risk.

Avoid the risk

One method of dealing with risk is to avoid the risk by not proceeding with the activity likely to generate the risk. Risk avoidance should only occur when control measures do not exist or do not reduce the risk to an acceptable level. Uncontrolled or inappropriate risk avoidance may lead to organisational risk avoidance, resulting in missed opportunities and an increase in the significance of other risks.

Case study – avoiding the risk

A food retailer identifies that a particular item on the lunch menu contains an ingredient with a short shelf life. The retailer is concerned that the item may become unfit for consumption prior to sale. To avoid the risk of a food poisoning incident the item is removed from the menu.

Change the likelihood of the occurrence

This option enhances the likelihood of beneficial outcomes and reduces the possibility of loss.

Case study – changing the likelihood

A deli operator reduces the likelihood of a meat slicer blade injuring staff by ensuring that everyone has received early training on the use of the machine and that there are clear signs displayed demonstrating the correct techniques for its use and maintenance.

Change the consequences

This will increase the size of gains and reduce the size of losses. This may include business continuity plans, and emergency and contingency plans.

Case study – changing the consequences

A small pharmacy relies on a computer system to process and record prescriptions. The pharmacist backs up the computer system weekly and the back-up tapes are stored in a safe on-site. A risk analysis identifies that there is still a significant residual risk associated with this practice. The pharmacist then backs-up daily and stores the tapes off-site. Paper records are also now generated on a monthly basis and archived.

Share the risk

Part or most of a risk may be transferred to another party so that they share responsibility. Mechanisms for risk transfer include contracts, insurance, partnerships and business alliances. It is important to note that risks can never be completely transferred, because there is always the possibility of failures that may impact on the business. Transfer of risk may reduce the risk to the original business without changing the overall level of risk.

Case study – sharing the risk

A personal trainer currently has the professional indemnity insurance required to be a registered fitness professional in NSW. However, he has recently completed a course in child and adolescent fitness. His insurer indicates that the current insurance policy would not cover injury to individuals under the age of 14.

The personal trainer's insurance broker identifies an indemnity provider who will support the new requirement and provide the trainer with professional indemnity for provision of child fitness programs. The trainer has now shared or transferred his risk to the new insurance company.

Retain the risk

After risks have been reduced or transferred, residual risk may be retained if it is at an acceptable level.

Identifying appropriate treatments

Once a treatment option has been identified, it is then necessary to determine the residual risk; that is, *has the risk been eliminated?* Residual risk must be evaluated for acceptability before treatment options are implemented (refer to the risk analysis matrix in Figure 3.4).

Conducting a cost–benefit analysis

Business owners need to know whether the cost of any particular method of correcting or treating a potential risk is justified. Considerations include:

- number of treatments required
- benefit to be gained from treatment
- other treatment options available, and why the chosen one has been recommended
- effectiveness of the treatment

- timeframe
- total cost of treatment option
- total reduction in residual risk
- legislative requirements.

Business owners are required by law to provide a safe workplace. If existing work environments need to be upgraded to fully meet codes of practice and standards, a risk management approach should be adopted to demonstrate due diligence.

A staged action or risk treatment plan can be used to document the risks and to outline a remedy. Appropriate consultation with stakeholders should also occur.

Risk treatment plan

A risk treatment plan indicates the chosen strategy for treatment of an identified risk. It provides valuable information about the risk identified, the level of risk, the planned strategy, the timeframe for implementing the strategy, resources required and individuals responsible for ensuring the strategy is implemented.

The final documentation should include a budget, appropriate objectives and milestones on the way to achieving those objectives.

Case study – risk treatment plan

An event manager operating her own business in a regional area is contracted by a local council to assist in the management of a children's fair to be held in conjunction with the annual agricultural show.

The event manager organises a site assessment of the facility planned for the fair. A number of hazards and other general issues are identified, including the site's proximity to a busy road, absence of convenience facilities, a faulty drinking fountain and a damaged fence bordering a residential property next to the facility. The event manager, in conjunction with the council, develops a treatment plan that demonstrates how and when the identified risks will be addressed, the resources required and who will be responsible for ensuring the strategy is implemented. The treatment plan also identifies the need for a subsequent site assessment to ensure that the identified risks have been successfully controlled to a level deemed appropriate by the organising committee.

Discussion

The risk treatment plan provides confidence to the council that there is a planned approach to addressing the identified risks. The document can also be used as a level of control and source of information when making decisions about signing off on resource allocation or approvals.

Tips for implementing risk treatments

- The key to managing risk is in implementing effective treatment options
- When implementing the risk treatment plan, ensure that adequate resources are available, and define a timeframe, responsibilities and a method for monitoring progress against the plan
- Physically check that the treatment implemented reduces the residual risk level
- In order of priority, undertake remedial measures to reduce the risk.

Refer to Section 6.3 for an example of a risk treatment plan.

Risk recovery

Although uncertainty-based risks are difficult, if not impossible, to predict, there are ways in which businesses can prepare for a significant adverse outcome. This is known as risk recovery.

Businesses should consider adopting a structured approach to planning for recovery. This planning may take many forms, including the following:

- *Crisis or emergency management planning*

  The business anticipates what might occur in a crisis or emergency, such as a fire or another physical threat, and then plans to manage this in the short term. This will include listing emergency contact details and training staff in evacuation and emergency response procedures.

- *Business continuity planning*

  The business moves beyond the initial response of a crisis or emergency and plans for recovery of business processes with minimal disruption. This might, for example, include ensuring that there is sufficient documentation of processes if a key staff member is unavailable to return to work and another staff member is required to fulfil that role, identifying options for alternative premises if the existing premises are damaged, or documenting alternate suppliers for key supply material if a key supplier does not fulfil their contract.

- *Contingency planning*

  Contingency planning can be a combination of the above.

  A contingency planning tool can help to identify what should be done to minimise the impact of a negative consequence on key business processes arising from an uncertainty-based risk. This would include the initial response (crisis management) and the delayed response (business continuity).

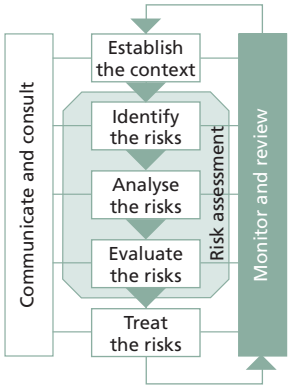
Case study – contingency planning

The senior accountant in a small accountancy firm travelling interstate has her laptop stolen from a restaurant where she is conducting a dinner meeting with clients. The laptop contains nearly four weeks of data that had not been backed up. This is a significant loss of a large amount of personal information regarding clients and business opportunities. In addition to this loss, the accountant is now without use of a laptop and still has much client work to conduct.

Discussion

As a result of this loss the accountancy firm decides to conduct a contingency planning exercise, where the key business processes for the business are mapped and a contingency plan is developed in the event that any of these processes fail. For example, the firm recognises that the use of laptops by accounting staff is critical, as is the information the laptops contain. The contingency plan lists the warranty and insurance details of the asset, provides instructions on how to report the loss of the laptop and how to expedite replacement. It also provides instruction on how to access the software programs necessary for a new laptop to become functional as well as backed-up data. In addition to the contingency plan, the firm recognises the lack of process and protocol in place for protection of data while staff are mobile and addresses this accordingly.

3.8 Step 7. Monitor and review



Monitor and review is an essential and integral step in the risk management process. A business owner must monitor risks and review the effectiveness of the treatment plan, strategies and management system that have been set up to effectively manage risk.

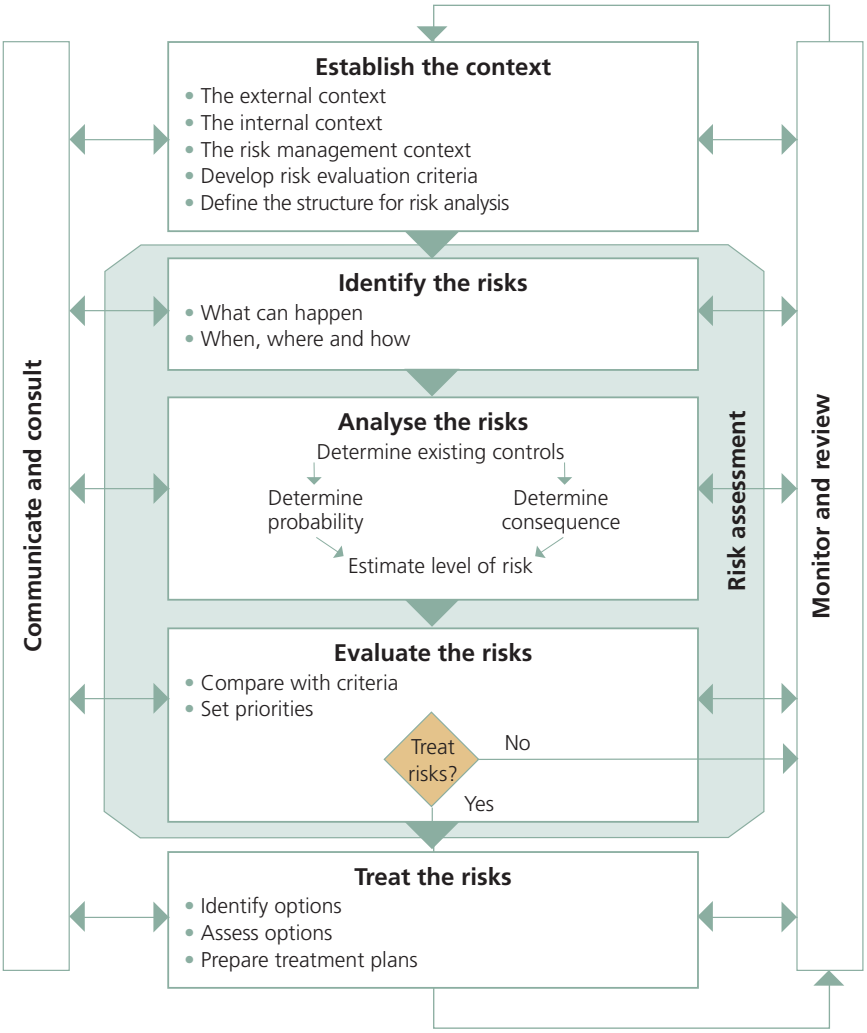
Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Very few risks will remain static, therefore the risk management process needs to be regularly repeated, so that new risks are captured in the process and effectively managed.

A risk management plan at a business level should be reviewed at least on an annual basis. An effective way to ensure that this occurs is to combine risk planning or risk review with annual business planning.

3.9 Summary of risk management steps

Figure 3.6 illustrates the components of each step of the risk management process and illustrates the cyclical nature of the process.

Figure 3.6 Details of the risk management process (source: AS/NZS 4360:2004)



4 Applying risk management

4 Applying risk management

4.1 Who should use risk management?

Risk management is the responsibility of anyone operating a small business. Accountability for management of risk cannot be outsourced or delegated.

Ultimately, the business owner will remain accountable for the risk decisions made within the business. This is why there should be a clear definition of the level of risk the business is willing to accept and who is able to make that decision. The business owner should oversee the management of risks deemed significant to the organisation.

4.2 Where should risk management be applied?

Risk management should be integral to the ongoing management of a business and applied at all levels of a business.

There are two basic levels in the management of a small business:

- **strategy and planning** – including identifying business requirements and the direction the business is taking
- **operational (product/service development and delivery)** – including ensuring efficiency and effectiveness in producing and delivering a product or service and meeting clients' expectations and requirements.

Risk management should be applied at both management levels.

Table 4.1 demonstrates the various uses of risk management within several areas related to the two management levels.

Table 4.1 Applications of risk management in small business

Management level	Area	Application of risk management
Strategy and planning	Business continuity planning	Business interruption procedures and strategies
	Emergency planning	Contingency planning Disaster planning and recovery Fire and life safety management
	Business planning	Business plan Strategic plan
	Human resources management	Training Culture Knowledge management Occupational health and safety
	Financial management	Budgeting Cashflow management Asset management Capital expenditure
	Outsourcing	Intellectual property protection Contract management
Operations	Product/service development	Insurance Equipment management Environmental management Resource allocation Housekeeping Emergency response Security Quality assurance Documentation Reporting Occupational health and safety Supply management Maintenance
	Product/service delivery	Project management Customer relationship management Post-sale service Guarantee management Occupational health and safety Hazard assessment/management Contract management Complaints management

4.3 How much risk management is enough?

One of the common complaints about risk management is the requirement for documentation – waging a 'paper war'.

The amount and formality of risk management and documents required will depend on the complexity of the activity for which risk analysis is being conducted, who requires the information, and the associated documentation required.

The line of risk management complexity is known as 'formalisation'; that is, how formal the risk management approach needs to be. The three levels of formalisation are:

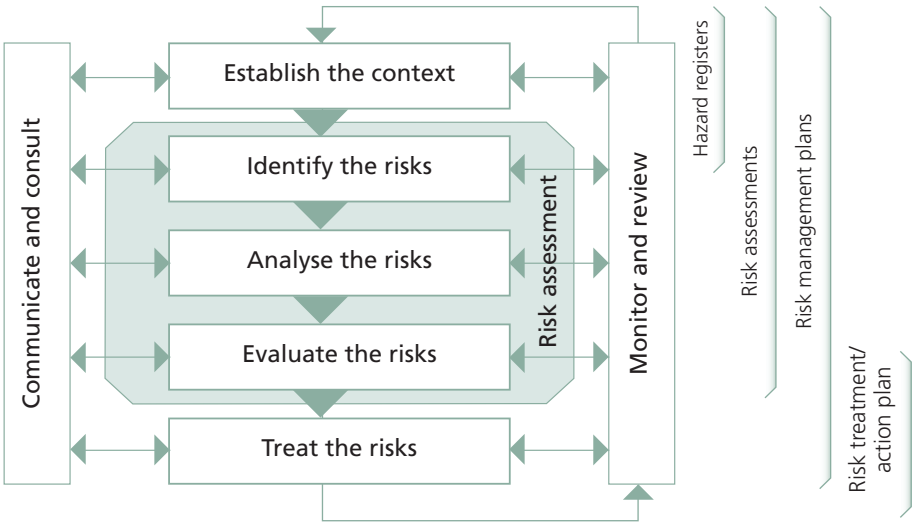
- **intuitive** – an 'on-the-run' mental or oral risk management process, which uses the risk management process without any paper records. Simply, it is the type of risk management that can be applied through intuition in time-critical or dynamic environments
- **planned** – involving the formal application of the risk management process as depicted within this guide. It uses experience, judgement and all available information (including stakeholder input) to determine and assess the risks, and then to consider appropriate controls
- **calculated** – a more thorough risk assessment or risk management plan. It may involve more research and data collection, and more comprehensive consultation with stakeholders and expert advisers. This approach is used when there is a major project or activity that involves significant input from other stakeholders as well as significant resources or equipment. The business continuity plan and emergency/crisis plan are examples of this level of formalisation.

4.4 Recording the risk management process

Many different types of documentation can be used in the risk management process. It is easy to become confused about which documents to use and when. This section offers a simple way to record the risk management process in small business.

There are several types of risk documentation. In line with the level of risk management formalisation (Section 4.3), each step of the risk management process may require a different level of documentation (Figure 4.1).

Figure 4.1 Documents used in the risk management process



Registers and hazard logs

These provide details about risks, incidents or hazards identified within the workplace, activity or situation. These are useful when there is limited subject matter expertise available when conducting risk assessments (Section 3.4). This is a method for retrospectively identifying risk.

Risk treatment and/or action plans

These plans document the management controls or treatments to be adopted for each risk and should list the following information:

- individuals responsible for implementing the plan
- resources to be used
- budget allocation
- timetable for implementation
- details of the mechanism and frequency of review for compliance with, and effectiveness of, the treatment plan.

Risk management plans

Risk management plans (RMPs) are used to formally document the entire risk management process for a particular activity. An RMP can be used for any activity, regardless of the complexity or context. The RMP is like any other management plan in that it documents a decision, allocation of resources, timeframes and responsibilities.

The most common way to identify the difference between a risk assessment and an RMP is to identify how many and which steps of the risk management process have been recorded.

Refer to Section 6.3 for an example of risk documentation.

4.5 Risk management and business size

This guide provides direction and guidance to owners of small business in general; however, small businesses have varying requirements depending on their size.

In this section, small businesses are categorised as follows:

- non-employing businesses and micro businesses (1–4 employees)
- other small businesses (5–19 employees).

Risk management for non-employing businesses and micro businesses

Non-employing businesses are those in which one person or two or more partners work, but there are no employees. People who work in these businesses are referred to as 'own account workers'. Micro businesses are those employing fewer than five staff.

Approximately 85% of small businesses in NSW are categorised as micro businesses[3]. More than half of these are non-employing businesses.

The risk categories for a non-employing business will differ from that of a business employing staff. For example, the human resources element will be minimal for a non-employing business; however there will be greater focus on areas such as partnership relations (where applicable) and sustainability.

For example, owner-operators of a small business are reliant upon their own health and wellbeing to ensure the sustainability of the business. Should they become sick or injured, the operations of the business will cease to function unless a contingency plan exists.

[3] Australian Bureau of Statistics, *Small Business in Australia*, 2001 [Catalogue no. 1321.0]

Non-employing businesses and micro businesses are also common categories for 'home-based' businesses. Of all businesses in NSW, approximately 20% carry out most of their work at home[4].

Home-based work creates additional risks to a business, including:

- **ergonomics** – Is the home appropriately designed for the work being conducted?
- **regulations** – Does the business comply with local government regulations?
- **environment** – Is the environment appropriate for the type of business?
- **productivity** – Do distractions impact on the productivity of the business? An outlay for leased premises may be recognised as an opportunity to grow the business and gain increased credibility from potential clients.

Risk management for other small businesses

A business with 5-19 employees is more complex and therefore risk management formality becomes more important.

For example, the human resources for a business of this size will have a much higher priority than for non-employing and micro businesses. The increased number of staff indicates a need for formalised systems and structures to provide guidance, direction and supervision, to ensure that they are assisting the business to achieve its objectives.

The formality of the risk management program should reflect this complexity.

[4] Australian Bureau of Statistics, '*Characteristics Of Small Business*', 2004, Cat. 8127.0

5 Sustaining a risk management approach

5 Sustaining a risk management approach

5.1 Risk management framework

Regardless of the size of a business, a risk management framework will help to visualise how risk management can be applied.

Risk management plans and risk management frameworks

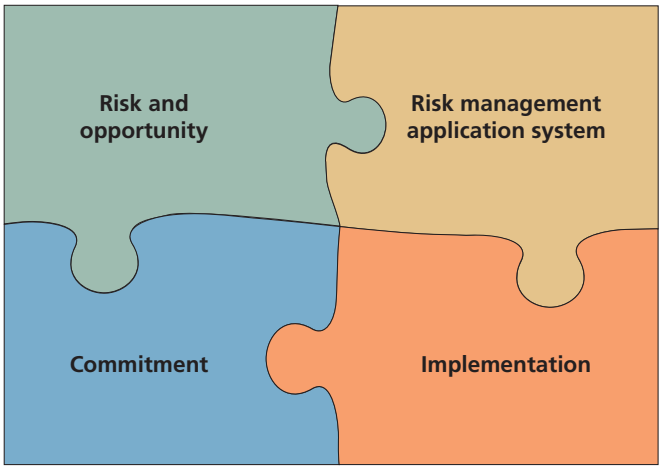
A risk management plan (RMP) is a document used to record the risks that have been identified through the risk management process, the level of risk assessed and the strategy for treating that risk. An RMP should also document the strategies in place to communicate the risk information to stakeholders and the method for monitoring and reviewing risk information.

A risk management framework (RMF) is the set of elements in the business management system concerned with managing risk. It describes the systems, processes, attitudes and commitment needed to successfully integrate risk management with existing business management processes, to ensure that the risk management program can assist a business to achieve its corporate objectives.

There are many different examples of RMFs that have been adopted worldwide. Larger organisations may choose to adopt a recognised RMF, such as the COSO Enterprise Risk Management – Integrated Framework, developed by the Committee of Sponsoring Organisations of the Treadway Commission. (See Section 7 for more information about COSO.) Many organisations have also adopted the Global Risk Alliances Risk Management Implementation Model as a framework to assist in the successful implementation of a risk management program and the achievement of a positive risk culture. This model is discussed in more detail later in this section.

For small business, an RMF may consist of the elements shown in Figure 5.1.

Figure 5.1 Elements of a risk management framework for a small business



Risk and opportunity

This is the first part of the framework. It contends that every business will encounter risk and opportunity. In identifying risk and opportunity, there are two levels that a business should consider:

- *Business level*

  At a business level, it is important to identify the significant risks and opportunities that will affect the objectives and goals of the business.

  Every small business should conduct an annual risk profiling exercise to identify risk at a business level.

  Risk profiling uses the risk management process to identify retrospective and prospective risks to the business at a 'strategic' level, as well as potential opportunities. This assists the business to implement strategies to ensure the objectives of the business are realised.

Refer to Section 6.4 for an example of a risk profile.

- *Operational level*

  In addition to identifying risk at a business level, it is also necessary to identify risk and opportunity at a project, activity or speciality level. For example, with the introduction of major change, such as implementation of a new piece of equipment, a new contract, a change in supplier or the diversification of products, it is important to take a risk management approach to ensure the objectives of the project or activity are successfully achieved.

Risk management application system

The risk management application system incorporates the various elements required for successful implementation of a risk management framework. These include:

- the risk management process (Section 2)
- where risk management should be applied
- common language for risk management
- risk analysis tools
- risk reporting
- risk management techniques
- scale of risk escalation and acceptance.

The application system aims to ensure that the resources required to implement a risk management program exist, are consistent and are clearly understood.

Commitment

A statement of commitment will provide a clear understanding of the business's approach to risk management. The risk management policy should be underpinned by:

- intention and expectation for risk management
- defined business objectives and rationale for managing risk
- links to other management processes, such as business planning
- categories of risk that have been identified as specific to the business
- levels or types of risk to be accepted
- responsibilities and accountabilities for identifying and managing risk (especially important for businesses with multiple staff)

- guidance on risk management documentation
- requirements for monitoring and reviewing performance against the policy.

An example of a commitment statement may be:

> *The business will provide a safe and healthy environment for all its staff and customers through the appropriate management of all recognised risks. All staff members are expected to support the risk management framework and are responsible for identifying, reporting and participating in the management of all risks in our operations.*

To make this statement effective, it should be appropriately resourced to ensure that the commitment (e.g. to a safe working environment) will be upheld.

The commitment to risk management should be the foundation on which culture change is achieved and a positive risk culture is established.

Implementation

It is not enough to conduct a risk profiling exercise or to develop a risk management plan. Risk management is an ongoing process.

Business owners should consider what is needed to adopt risk management into the fabric of their business so that effective risk management becomes part of good business practice. This should include:

- ensuring appropriate commitment to risk management
- setting clear objectives and guidelines for risk management
- allocating adequate resources
- training staff appropriately
- implementing systems for monitoring and reviewing risks.

An excellent way to ensure that risk management becomes an ongoing process is to integrate risk management planning for the business with the business planning cycle. The existing RMP should be reviewed annually, to ensure that the risks identified are being managed appropriately and to identify any new risks.

6 Risk management tools and activities

6 Risk management tools and activities

6.1 Risk identification methodologies

There are numerous methods of identifying risks. A business owner needs to choose the most appropriate method based upon the context of the risk identification exercise, the level of risk management planning and the type of risk being examined. A number of examples of risk identification methodologies are provided here.

Risk categories

Setting risk categories was introduced in Section 2. This involves identifying what categories of risk will be associated with a particular activity or the business as a whole. These might include:

- financial
- reputation
- safety
- environment
- equipment.

Once categories of risk have been established for a business, the risks within each category can then be identified using methods such as those detailed below.

Structured brainstorming

Brainstorming allows a range of personal knowledge and experience to be brought together to identify risks. This is a way of encouraging lateral thinking as people introduce new ideas and thoughts based on their interaction with other people.

The brainstorming exercise is normally centred on a particular topic, for example the risks associated with closing an office for renovations, or entering into a new contract.

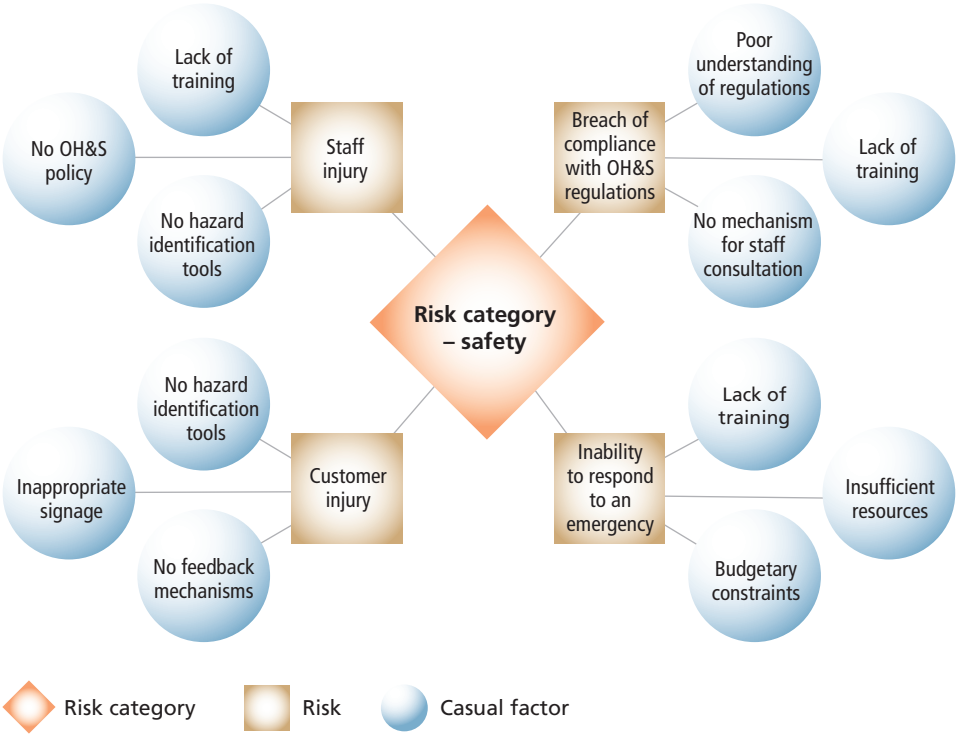
During brainstorming, the person running the session should keep the participants focused. The group should keep to the topic and remain objective.

A structured brainstorming map might be similar to the model in Figure 6.1. Associated issues, each of which will have individual risks, surround the central issue. A template for this exercise is located in Annex A.

This involves working within a 'risk category' to identify associated risks. The next step is to determine the factors that may lead to that risk, i.e. the causal factors. For example, a causal factor may be a lack of training, poor communication strategies, or budgetary constraints.

Figure 6.1 Structured brainstorming exercise for the category of safety for a food retailer

(Note: This is for demonstration purposes only and is incomplete.)



SWOT analysis

A SWOT analysis was introduced in Section 3.4. This method identifies strengths, weaknesses, opportunities and threats to an activity or a business. The strengths and opportunities can be viewed as positive risks and the threats and weaknesses as negative risks.

A SWOT analysis is a form of structured brainstorming. A template for a SWOT analysis is located in Annex B.

Figure 6.2 A worked example of a SWOT analysis for a plumbing business.

Positive risk		Negative risk
Strengths • Our tradespeople are exceptionally skilled • We have excellent relationships with our existing customers • Our work is considered high quality and our service reliable.	**Weaknesses** • Our tools of trade are second hand and may be unreliable • Ageing workforce • Limited familiarity with new technology.	
Opportunities • The only other plumber in town wants to retire • A new industry development is currently tendering to outsource trade services.	**Threats** • Somebody from out of town might buy retiring plumber's business • Another business may start up in town • Difficulties in recruiting new staff due to skill shortages • Loss of an existing employee leaving the business unable to cope with workload.	

Task analysis

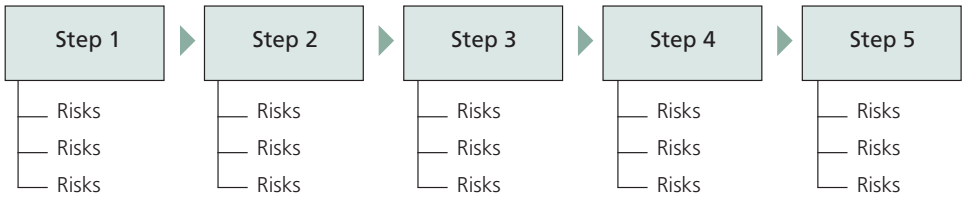
Task analysis is useful for activities involving a series of steps or tasks. An example is the introduction of a new major piece of equipment.

Task analysis is a relatively simple tool to use, see Figure 6.3. For a particular task, think about each major step in the process and what might go wrong, or indeed what the opportunities might be.

Draw the steps of the task on a whiteboard or piece of butcher's paper. If working with a team, ask each team member to consider the risks associated with each step and to write them on a sticky note. Work on one step at a time.

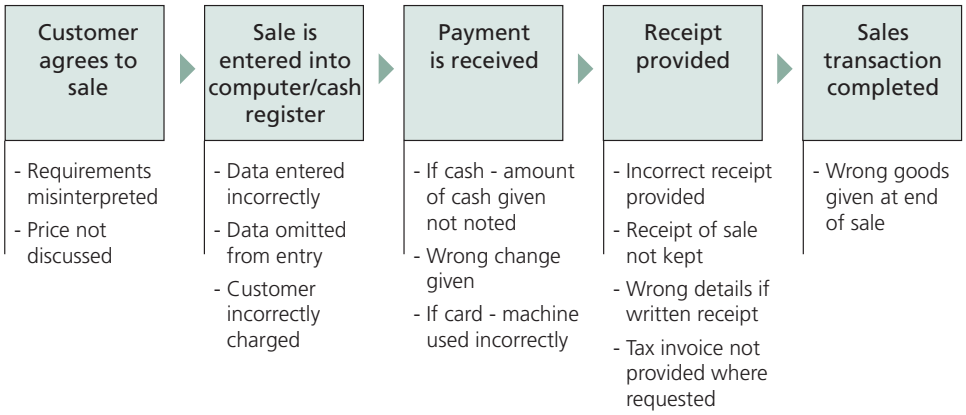
Discuss the risks identified for each step before moving onto the next step.

Figure 6.3 Model for task analysis



A template for a task analysis can be found in Annex C.

Figure 6.4 Task analysis for completing a sales transaction



6.2 Risk analysis tools

Table 6.1 is an example of a qualitative risk analysis tool. This tool should be used with caution. The word pictures for consequence and likelihood should be carefully reviewed and modified to suit the context of your business. This tool was introduced in Section 3 (3.5 Step 4. Analyse the risks).

This tool is used as follows:

1. Once a risk has been identified within a particular risk category (for example, safety)
2. Using the consequence descriptors (left hand side of the table), to determine the possible impact of the risk
3. Using the likelihood scale (across the top, right hand side of the table), to determine the likelihood of the possible impact
4. To estimate the level of risk by combining the consequence and likelihood within the matrix.

Table 6.1 Qualitative risk analysis

	LEGEND	Extreme	High	Medium	Low					
	Consequence					Likelihood				
	Commercial	Finance	Security	Safety	Legal and regulatory compliance	Almost certain	Likely	Possible	Unlikely	Rare
						Almost certain to occur at some time.	Known to have been present or occurred/ likely to occur.	Not likely to occur in normal situations.	Unlikely to occur.	Has not occurred in the past and requires unusual circumstances to occur.
Significant	Significant loss of market share resulting in 10–30% loss of current clients and no increase in new clients over a three-month period.	Loss > 30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Significant reputation damage.	Death or multiple injuries requiring hospitalisation.	Investigation by authority and significant penalty awarded. Very serious litigation, including class actions. Closure of business.	**Extreme**	**Extreme**	**Extreme**	**High**	**High**
Major	Major loss of market share resulting in <10% loss of current clients. No new clients for 1–3 months.	Loss of 20–30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Some reputation damage.	Major injury requiring hospitalisation.	Major breach with potential major penalty and/or investigation and prosecution by authority. Major litigation. Future of the business threatened.	**Extreme**	**Extreme**	**High**	**High**	**Medium**
Moderate	Loss of market share. Current clients are retained but no new clients for 1–3 months.	Loss of 10–20% of total income or budget.	Staff threat resulting in some injury but no hospitalisation required. Minor reputation damage.	Minor injury – first aid required.	Serious breach with investigation by or report to authority. Moderate penalty possible.	**High**	**High**	**Medium**	**Medium**	**Low**
Minor	Minor loss of market share. Current clients are retained but new clients have visibly decreased (50% of normal uptake).	Loss < 10% of income or total budget.	Staff threatened, but no injury. No reputation damage.	No injury.	Low-level legal issue. Penalty or prosecution unlikely.	**High**	**Medium**	**Medium**	**Low**	**Low**

6.3 Risk management documentation – risk management plan

An RMP enables a business owner to document the stages of the risk process within one document. An RMP template can be found in Annex D.

The RMP template provides a simple approach to developing an RMP. It can be used to document the results of a risk assessment and risk treatment strategies, either for the business as a whole or for a particular activity for which a risk management exercise is being conducted.

The template comprises four parts.

Part 1. Contextual information

- Provide a brief description of the activity for which the risk management planning exercise is being conducted. Be clear and concise, indicating the exact aim of the activity
- Provide a reason for the activity/task – why is the risk management planning exercise being conducted?
- List the objectives of the activity. The risk identification exercise should relate directly to the impact on these objectives
- Highlight the significance and/or the importance of the activity. Consider this within the context of the business's overall objectives
- Provide a list of references needed to conduct the exercise. Include legislation, regulations, internal procedures and policies, and accreditation requirements
- Identify any assumptions that need to be made to conduct the exercise. Assumptions may relate to any unanswered questions that may exist. The final RMP should be viewed in light of these assumptions. Where assumptions are either proven or not proven, the RMP should be modified accordingly
- List any limitations to the exercise. This may include time constraints, availability of stakeholders or financial limitations.

Part 2. Risk register

For each risk category, use the template to document the risks identified, the current treatment strategy (if relevant), the risk rating elements, the priority levels of each risk and the further treatment options available.

The columns in the template should be used as follows:

- **Serial no.** – Use a numbering system to differentiate the risks identified within each category
- **Risk description** – Write a risk statement that defines the risk, including what can happen and how it can happen
- **Impact** – Describe the possible impact on objectives as a result of the risks
- **Consequence rating** – Use a risk analysis tool to estimate the possible consequence or impact upon objectives, taking into consideration existing treatment strategies
- **Likelihood rating** – Use a risk analysis tool to estimate the likelihood that a risk may impact upon objectives, taking into consideration existing treatment strategies
- **Level of risk** – Use a risk analysis matrix or similar tool to combine the results of consequence and likelihood to achieve the level of risk or risk rating
- **Risk priority** – Compare the level of risk with the pre-determined risk criteria and rank the risks in order of priority
- **Treatment options** – Identify the various treatment options available for managing the identified risk. (These options should be in addition to current treatment strategies and should aim to reduce the residual risk).

Part 3. Risk treatment plan

The Risk Treatment Plan (RTP) can be incorporated into Part 2, or kept as a stand-alone document. The RTP is a high-level project plan designed to keep track of the treatment strategies required and associated actions.

1. Document the treatment strategies selected from Part 2 for use to mitigate the risk. Ensure the numbering system provides direct reference back to the risk register.
2. Document any resources required for implementing the treatment.
3. Document any resource implications that may exist, such as funding implications or staff requirements.
4. Identify the person responsible for ensuring the action is addressed.
5. Provide a timeframe to ensure the action is completed in a timely manner. This should reflect the priority of the risk.
6. Indicate the strategy required for reviewing the treatment. Identify how the treatment strategy will be monitored/reviewed to ensure residual risk does not change (e.g. monthly review of client complaints).

Part 4. Summary

The final part of the RMP is the summary page, which provides details of the author of the RMP, the methodology used to identify risk, and specific tools used. This section is also used to document the review and to capture any changes required.

Checklist for preparing to develop an RMP

The following checklist can provide guidance through the risk management planning process.

Preparation for development of an RMP	Complete ✔
• Obtain relevant references / policies / legislation / contracts / other resources	
• Collect background data (including past RMPs where existing) and review data	
• Identify the purpose of the RMP	
• Identify the audience of the RMP	
• Identify stakeholders that need to have input into the RMP	
• Obtain guidance on the type of analysis (qualitative, semi- quantitative, quantitative)	
• Determine the method for risk identification	
• Determine timeframe required to produce the RMP	

Example of a risk management plan

Note: This is an example only and should not be replicated. Use the risk management plan template to prepare a plan for your small business.

Fresh Flowers for You is a small business operating in a suburban shopping strip, employing three full-time staff. Due to a decrease in foot traffic over recent months, the business owner has decided to expand the business and create online purchasing. This is a result of many customer enquiries and suggestions. However, the business owner is concerned about customers feeling secure about using the system, any legal implications and the business's exposure to IT security risks. A risk management planning exercise is conducted to prepare for the launch of the system.

Risk management plan – part 1 (contextual information)	
Brief description of activity	Introduction of an online ordering and purchase system into Fresh Flowers for You. It is expected that the online ordering in the first 12 months will account for 10–20% of overall income
Reason for activity or task	New initiative, looking to expand and grow the business
Objectives	1. To introduce secure ordering and purchasing online 2. To minimise exposure to fraud and other security risks 3. To maximise customer confidence in the use of the system
Significance/ importance of activity	Medium to high – currently are unable to keep up with client demands
References required (e.g. regulations, policies)	1. Commonwealth and State legislation, including: • copyright • privacy • trade practices and consumer protection • spam • cybercrime. 2. IT security guidelines
Assumptions	The information contained within the references is true and correct at time accessed
Limitations	1. Budget 2. Expertise available

Risk management plan – part 2 (risk register)			
	Risk dimension: security	Risk dimension: financial	Risk dimension: legal/compliance
Serial no.	1	2	3
Risk description	Cybercrime, including virus damage, identity theft, spyware, general fraud	Costs associated with online transactions outweigh benefits associated with initiative	Breach of regulations within e-business legislation
Impact	Direct financial loss, reputation damage, equipment damage, system unavailability	Direct financial loss due to increased fees Customer loss due to increased costs	Possible fine and/or legal prosecution
Consequence	Significant	Moderate	Moderate
Likelihood	Likely	Likely	Possible
Level of risk	Extreme	High	Moderate
Risk priority	1	2	3
Treatment options	1. Update anti-virus software and check firewall viability 2. Review requirements to ensure secure online banking 3. Develop and test security policies 4. Develop disaster recovery plan	Develop business case to identify impact of increased fees	1. Review all legislation 2. Consult solicitor to seek advice 3. Develop and test compliance policies and procedures

Risk management plan – part 3 (risk treatment plan)			
Serial no.	1	2	3
Treatment strategy	1. Update anti-virus software and check firewall viability 2. Review requirements to ensure secure online banking 3. Develop and test security policies 4. Develop disaster recovery plan	Develop business case to identify impact of increased fees	1. Review all legislation 2. Consult solicitor to seek advice 3. Develop and test compliance policies and procedures
Resources required	Security guidelines 5 days allocated to complete	3 days allocated to complete	5 days allocated to complete
Priority rating	1	2	3
Person responsible	Business owner	Business owner	Business owner
Deadline	<date>	<date>	<date>
Strategy for review	Test security policies Engage an IT security specialist to review systems	Survey customers Review impact against weekly income every week for three months	Consult solicitor to review policies and procedures Implement a review of legislation every three months
RMP compiled by:	Business owner		
Risk methodology:	Structured brainstorming with staff; discussion with software developer; consultation with previous users		
Risk analysis tool:	Risk matrix developed for the context		
Signature:			

6.4 Risk profile

Developing a risk profile will help a small business owner to determine their major areas of risk, and what needs to be done to make sure these are effectively managed. The risk profile can also assist to identify and realise the opportunities for a business.

An annual business risk profile (Table 6.2) can be produced for a business to provide a holistic view of the major risks influencing the business. This should be at an executive or high level. The risk profile will not provide detail about each risk area or what is in place to manage the risk; this will be documented within the business's risk register or RMP. However, it will provide information for business planning and/or as a communication tool for the business's accountant or insurer.

Table 6.2 Annual business risk profile

Brief description of business		
Vision and mission of business		
Context		
External context	Internal context	Risk management context
Determine: • key external influences on your business, e.g. political, social, legal • key internal influences, e.g. organisational objectives • risk management context, e.g. risk management requirements, objectives, timeframes.		
Stakeholders		
Internal stakeholders	External stakeholders	
Risk categories	**Risk criteria**	
1. Identify the categories of risk for your business	1. For each risk category, document what is an acceptable risk level for the activity and what is unacceptable	
2.	2.	
3.	3.	
4.	4.	
5.	5.	
Key objectives	**Major risks / opportunities**	**Level of risk**
1.		
2.		
3.		

Helpful resources

	Topic	Organisation	Contact details	
			Website	Phone
Risk management	Australian risk management standard	SAI Global (Standards Australia)	www.standards.com.au	1300 360 314
	Implementation	Risk Management Institution of Australasia	www.rmia.org.au	(03) 9899 7100
	Occupational health and safety	Business Assistance Unit, WorkCover NSW	www.workcover.nsw.gov.au	13 10 50
Other business assistance	Starting a business	Business Advisory Services, NSW Dept of State and Regional Development	www.smallbiz.nsw.gov.au	1300 650 058
		Business Entry Point	www.business.gov.au	
	Registering a business name	NSW Office of Fair Trading, Dept of Commerce	www.fairtrading.nsw.gov.au	13 32 20
	Business licences			
	Retail leasing issues	Retail Tenancy Unit, NSW Dept of State and Regional Development	www.retailtenancy.nsw.gov.au	(02) 9223 0466 1800 063 333 (toll free)
	Taxation	Federal - Australian Taxation Office	www.ato.gov.au	13 28 66
		State – NSW Office of State Revenue	www.osr.nsw.gov.au	(02) 9689 6200
	Employing staff	Federal – Dept of Employment and Workplace Relations	www.workplace.gov.au	1300 363 264
		State – NSW Office of Industrial Relations, Dept of Commerce	www.industrialrelations.nsw.gov.au	13 16 28
	Training	NSW Dept of Education and Training	www.skilling.nsw.gov.au	13 28 11
	Business development	NSW Dept of State and Regional Development	www.smallbiz.nsw.gov.au	1300 134 359
	Exporting	Austrade	www.austrade.gov.au	13 28 78
		NSW Dept of State and Regional Development	www.smallbiz.nsw.gov.au	1300 134 359

Glossary

The following terms and definitions are used in this guide:

Accreditation - The certification by a statutory or approved authority of the facilities, capabilities, objectivity, competence and integrity of a business or an individual to provide a specified service and/or required operation

Best practice – A comprehensive, integrated and cooperative approach to the continuous improvement of all facets of an organisation's operations. It is a method by which leading-edge companies manage their businesses to achieve world-class standards of performance

Consequence (AS/NZS 4360) – An outcome or impact of an event
(Note: There can be more than one consequence from one event

- Consequences can range from positive to negative
- Consequences can be expressed qualitatively or quantitatively
- Consequences are considered in relation to the achievement of objectives)

Contingency planning – The part of risk management that aims to ensure that swift and appropriate action is taken when an undesirable outcome, particularly an emergency situation, arises. It has two broad aspects:

- development of crisis management plans aimed at maximising safety for people and minimising damage and disruption during a crisis
- development of business resumption plans or continuity plans aimed at ensuring business functions are recovered as quickly as possible after a crisis

Cost–benefit analysis – A method of evaluating projects or investments by comparing the present value or annual value of expected benefits to costs

Environmental management – The use of procedures that minimise adverse environmental impact during work practices

Event (AS/NZS 4360) – The occurrence of a particular set of circumstances
(Note: The event can be certain or uncertain; the event can be a single occurrence or a series of occurrences)

Hazard (AS/NZS 4360) – A source of potential harm

Likelihood (AS/NZS 4360) – How likely an event is to occur, or the frequency with which an event may occur (Note: Likelihood can be expressed qualitatively or quantitatively)

Loss (AS/NZS 4360) – Any negative consequence or adverse effect, financial or otherwise

Maintenance – All actions necessary to retain an item or asset in optimal condition

Occupational health and safety (OH&S) – The management issues that affect the health and safety of individuals in a workplace environment, such as ergonomics, indoor air quality, weather conditions or fire egress

Probability (AS/NZS 4360) – A measure of the chance of occurrence expressed as a number between 0 and 1. The extent to which an event is likely to occur

Residual risk (AS/NZS 4360) – The risk remaining after implementation of risk treatment

Risk (AS/NZS 4360) – The chance of something happening that will have an impact on objectives

Risk analysis (AS/NZS 4360) – A systematic process to understand the nature of risk and to deduce the level of risk

Risk assessment (AS/NZS 4360) – The overall process of risk identification, risk analysis and risk evaluation

Risk avoidance (AS/NZS 4360) – A decision not to become involved in, or to withdraw from, a risk situation

Risk criteria (AS/NZS 4360) – Terms of reference by which the significance of risk is assessed

Risk evaluation (AS/NZS 4360) – The process of comparing the level of risk against risk criteria

Risk identification (AS/NZS 4360) – The process of determining what, where, when, why and how something might happen

Risk management (AS/NZS 4360) – The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects

Risk management process (AS/NZS 4360) – The systematic application of management policies, procedures and practices to the tasks of communication, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk reduction (AS/NZS 4360) – Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk

Risk sharing (AS/NZS 4360) – Sharing with another party the burden of loss or benefit of gain from a particular risk

Risk treatment (AS/NZS 4360) – The process of selection and implementation of measures to modify risk

Stakeholders (AS/NZS 4360) – Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision, activity or risk

Bibliography

Aerosafe Risk Management Pty Ltd, 2002, *Risk Management: Guidelines for Managing Safety Risk within the Australian Defence Organisation*, Defence Publishing Services, Department of Defence, Canberra, HB 001 – 2002

CPA Australia, 2002, *Enterprise Risk Management: Better Practice Guide for the Public Sector*, Public Sector Centre of Excellence, Melbourne, ISBN 187687442 2

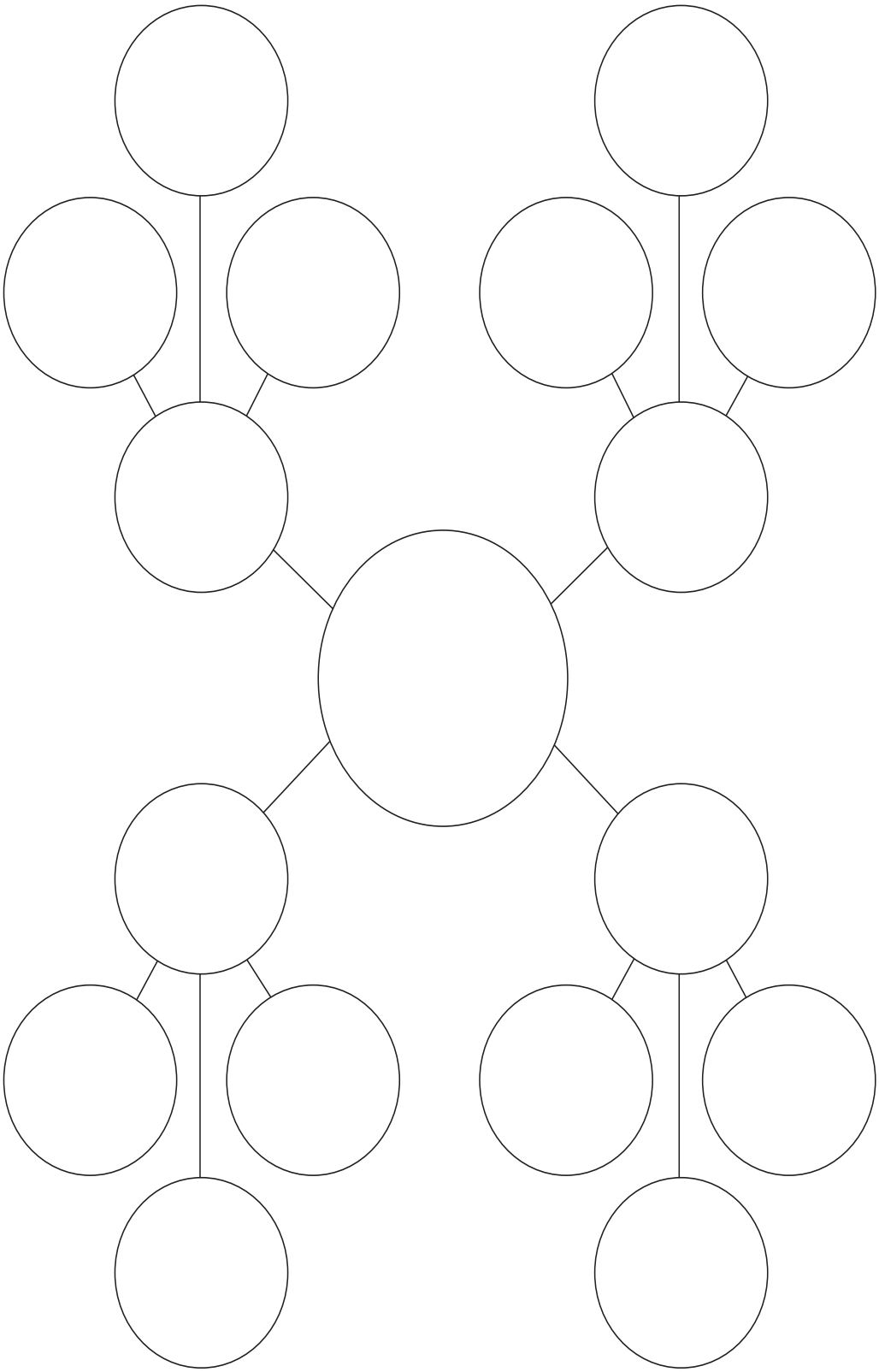
National Occupational Health and Safety Commission, **www.nohsc.gov.au** (accessed January 2004)

Standards Australia, 2004, *Standard for Risk Management AS/NZS 4360:2004*, New South Wales, ISBN 0-7337-5904-1

Standards Australia, 2004, *Risk Management Guidelines HB 436:2004* (Companion to AS/NZS 4360:2004), New South Wales, ISBN 0 7337 5960 2

Annex A

Structured brainstorming exercise template



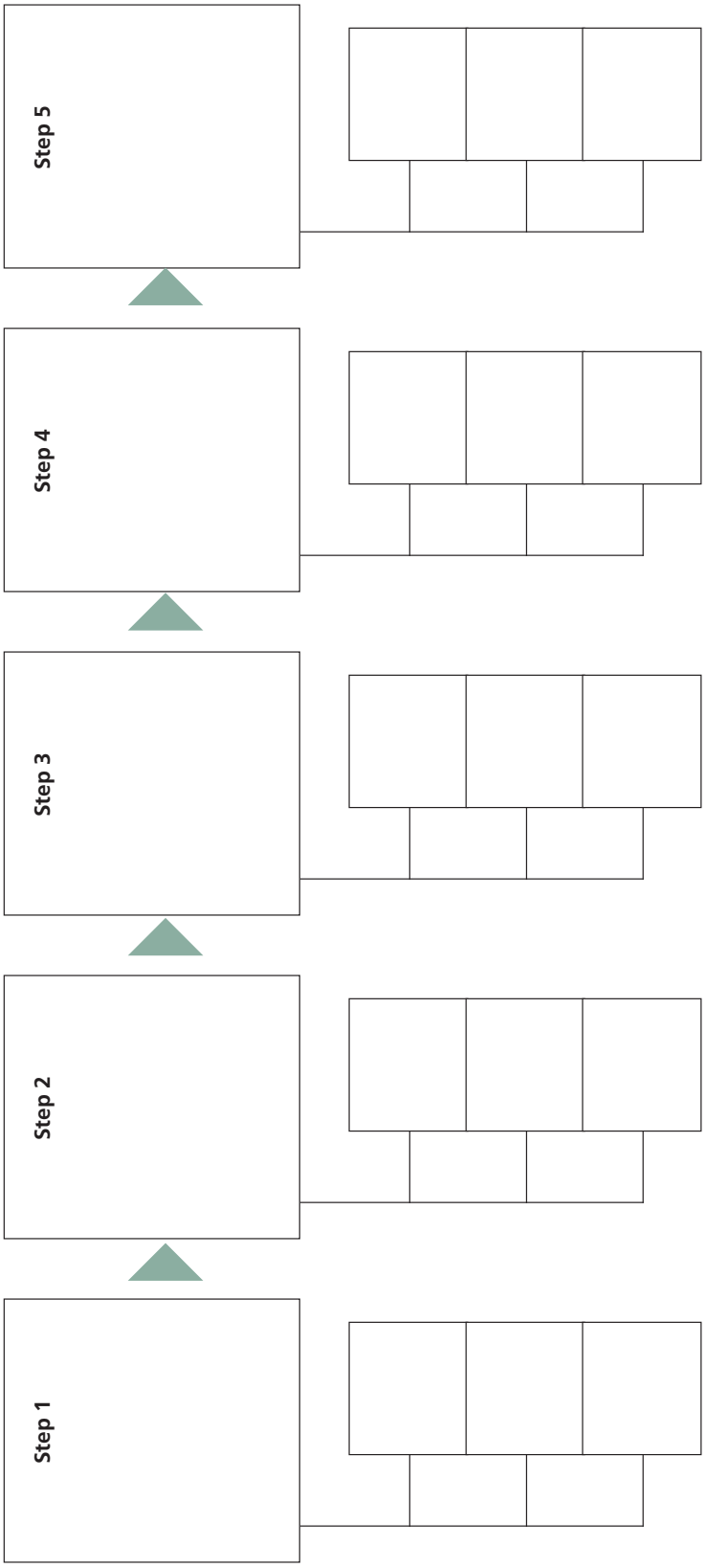
Annex B

SWOT analysis template

Strengths	**Weaknesses**
Opportunities	**Threats**

Annex C

Task analysis template



Annex D

Risk management plan template

Risk management plan – part 1 (contextual information)	
Brief description of activity:	
Reason for activity or task	
Objectives of RMP	
Significance/importance of activity	
References required (e.g. regulations, policies)	
Assumptions	
Limitations	

Risk management plan – part 2 (risk register)							
Risk dimension: (Document dimension of risk here, e.g. financial, safety)							
Serial no.	Risk description	Impact	Consequence	Likelihood	Level of risk	Risk priority	Treatment options
1							
2							
3							
4							

Risk management plan – part 3 (risk treatment plan)						
Serial no.	Treatment strategy	Resources required	Priority rating	Person responsible	Deadline	Strategy for review
1						
2						
3						
4						

RMP compiled by:	
Risk methodology:	
Risk analysis tool:	
Signature:	

NSW Department of State and Regional Department
Small Business Development Division

PO Box N818 Grosvenor Place
Sydney NSW 1220

Tel: 02 9338 6600
Fax: 02 9338 6705
Email: first@business.nsw.gov.au
www.smallbiz.nsw.gov.au