BSBOPS504

Manage business risk

Release 1

Learner Guide

Aspire Version 1.2

Aspire
Learning Resources

Aspire also has learning resources available in these areas:

- Foundation skills
- LLN and employability skills (non-competency)
- Community services
- Early Childhood Education and Care
- Allied health

Aspire is committed to developing quality resources that meet the needs of our customers. However, occasionally Aspire finds, or is notified of, errors. Please refer to our website at www.aspirelr.com.au to see if there are any updates that may be relevant to you.

Every effort has been made to ensure the information in this book is accurate; however, the author and publisher accept no responsibility for any loss, damage or injury arising from such information.

Except where an information source is acknowledged, the names and details of individuals and organisations used in examples are fictitious and have been devised for learning purposes only. Any similarity to actual people or organisations is unintentional.

All websites referred to in this unit were accessed and deemed appropriate at time of publication.

Aspire Training & Consulting apologises unreservedly for any copyright infringement that may have occurred and invites copyright owners to contact Aspire so any violation may be rectified.

BSBOPS504 Manage business risk, Release 1

Level 1, 464 St Kilda Road
MELBOURNE VIC 3004 AUSTRALIA
Phone: (03) 9820 1300

First published October 2020
Reprinted with amendments November 2023

Cover design: Anne-Marie Reeves Design
Printer: Doculink Australia Pty Ltd, 1d/28 Rogers Street, Port Melbourne VIC 3207

e-ISBN 978-1-76075-737-3 (PDF version)
ISBN 978-1-76075-736-6

Contact details

Participant
Name:
Start date:
Phone number:
Email:
Work location
Name:
Address:
Postal address:
Workplace supervisor name:
Phone number:
Fax:
Email:
Registered Training Organisation (RTO)
Name:
Address:
Postal address (if different):
Phone number:
Fax:
RTO contact name:
Mobile:
Email:

CONTENTS

Topic 4 | Select and implement treatments 81

Before you begin

This Learner Guide is based on the unit of competency *BSBOPS504 Manage business risk*, Release 1. Your trainer or training organisation must give you information about this unit of competency as part of your training program. You can access the unit of competency and assessment requirements at: www.training.gov.au.

How to work through this Learner Guide

This Learner Guide contains a number of features that will assist you in your learning. Your trainer will advise which parts of the Learner Guide you need to read, and which Practice Tasks and Learning Checkpoints you need to complete. The features of this Learner Guide are detailed in the following table.

Feature of the Learner Guide	How you can use each feature
Learning content	Read each topic in this Learner Guide. If you come across content that is confusing, make a note and discuss it with your trainer. Your trainer is in the best position to offer assistance. It is very important that you take on some of the responsibility for the learning you will undertake.
Examples	These highlight key learning points and provide realistic examples of workplace situations.
Practice Tasks	Practice Tasks give you the opportunity to put your skills and knowledge into action. Your trainer will tell you which practice tasks to complete.
Summaries	Key learning points are provided at the end of each topic.
Learning Checkpoints	There is a Learning Checkpoint at the end of each topic. Your trainer will tell you which Learning Checkpoints to complete. These checkpoints give you an opportunity to check your progress and apply the skills and knowledge you have learnt.

Foundation skills

As you complete learning using this guide, you will be developing the foundation skills relevant for this unit. Foundation skills are the language, literacy and numeracy (LLN) skills and the employability skills required for participation in modern workplaces and contemporary life.

The following table provides definitions for each foundation skill.

Foundation skill area	Foundation skill description
Reading	▪ Synthesises a variety of relatively complex texts ▪ Gathers, interprets and analyses textual information from a range of sources to identify relevant information
Writing	▪ Develops textual material and organises content in a manner that effectively documents risk management analysis and assessment priorities and processes
Oral communication	▪ Participates in interactions with stakeholders using questioning and listening to elicit opinions, and to confirm and clarify understanding
Numeracy	▪ Uses numerical tools to assess risk and uses numerical data to review plans
Navigate the world of work	▪ Refers to organisational processes, procedures and requirements when making decisions about risk management
Teamwork	▪ Selects appropriate conventions and protocols when communicating with stakeholders about risk management ▪ Consults and negotiates with stakeholders about risk management processes and outcomes
Planning and organising	▪ Sequences and schedules a range of routine and complex activities, monitors implementation, evaluates processes and manages relevant communication ▪ Systematically analyses information to decide on appropriate risk management treatments
Technology	▪ Uses digital technologies and systems to access information, document plans and communicate with others

What do you already know?

Use the following table to identify what you may already know. This may assist you to work out what to focus on in your learning.

Topic	Key outcome	Rate your confidence in each section
Topic 1: Establish the risk context	1A Evaluate organisational processes, procedures and requirements for risk management	❑ Confident ❑ Basic understanding ❑ Not confident
	1B Review existing arrangements	❑ Confident ❑ Basic understanding ❑ Not confident
	1C Document critical success factors, goals and objectives	❑ Confident ❑ Basic understanding ❑ Not confident
	1D Communicate risk process to stakeholders	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 2: Identify risks	2A Invite stakeholders to assist in identifying risks	❑ Confident ❑ Basic understanding ❑ Not confident
	2B Research the risks	❑ Confident ❑ Basic understanding ❑ Not confident
	2C Document the risks	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 3: Analyse risks	3A Assess the likelihood of risks occurring	❑ Confident ❑ Basic understanding ❑ Not confident
	3B Assess the impact or consequences of risks	❑ Confident ❑ Basic understanding ❑ Not confident
	3C Evaluate and prioritise risks for treatment	❑ Confident ❑ Basic understanding ❑ Not confident

Topic	Key outcome	Rate your confidence in each section
Topic 4: Select and implement treatments	4A Determine and select from options for treating risks	❑ Confident ❑ Basic understanding ❑ Not confident
	4B Develop a risk treatment action plan	❑ Confident ❑ Basic understanding ❑ Not confident
	4C Communicate and implement a risk treatment action plan	❑ Confident ❑ Basic understanding ❑ Not confident
	4D Monitor and evaluate the risk management process	❑ Confident ❑ Basic understanding ❑ Not confident

Topic 1 | Establish the risk context

1A Evaluate organisational processes, procedures and requirements for risk management

1B Review existing arrangements

1C Document critical success factors, goals and objectives

1D Communicate risk process to stakeholders

1A Evaluate organisational processes, procedures and requirements for risk management

Risk is the effect of uncertainty on a group or organisation, and its objectives, functions or outcomes.

Organisations conduct risk management to identify potential risks and to put in place measures to control the likelihood of these occurring. The aim is to protect the organisation's assets, and to protect and create value for its stakeholders – including owners, employees and customers. Before you begin any risk management tasks, you need to know how your organisation operates, how it views risk, what organisational processes or procedures it currently has in place for managing risk, and what processes may need to be developed.

Questions to ask when determining an organisation's potential risks might include:

- Is there a risk management plan? If so, what aspects does it cover?
- How does it align with the organisation's strategic plans?
- Is the manager's role in the plan clearly delineated?
- Do all staff know about the plan and understand what is required of them?

Understanding the organisation's operations

Managers must be familiar with the way their organisation is structured, its philosophy, how it operates and the potential risks it faces.

The size and nature of an organisation dictates its organisational hierarchy. For example, a large organisation may have a CEO, several managers for specific departments and a workforce to achieve its strategic objectives. A not-for-profit organisation may be overseen by a board.

An organisation may be a single entity, part of a franchise, part of an international network or it may have branches nationwide. All organisations should have a set of policies and procedures that govern the way they operate in accordance with relevant legislation and industry codes of practice, as well as a business plan that outlines their goals, objectives, strategies, responsibilities and resourcing in the short and long term. The planning should include a risk management process that identifies and prepares contingencies for dealing with risks likely to affect their operations.

Understanding the types of risk and how they are categorised

The types of risk to an organisation depend on its size and nature as well as its business operations.

The following table lists various types of risk an organisation may encounter that should be considered in risk management.

Commercial relationships	Risks of being associated with another organisation, directly or indirectly. Where an event affects an associated organisation, you need to consider whether the event is positive or negative, flow-on or collateral.
Economic circumstances	Risks associated with finance. Risk is inherent in international markets (currency, trade, etc.) and in domestic areas such as debt exposure, supplier/customer business failure or collapse. Property-centred risks include buildings, assets and product development.
Human behaviour	Human risks include company performance due to morale, as well as issues in the organisation's international business or work culture; for example, during company mergers or takeovers, staff cutbacks or recruitment. Human behaviour risk is also often recognised as part of work health and safety.
Individual activities	Theft, embezzlement and fraud can take place on a small or large scale. Individual activities contain these types of risk.
Legislation	Legislative changes affecting organisational operations are often foreseeable, but risk arises from the changes themselves and the change process; for example, reorganisation; relocation; and differing federal, state and local requirements for licensing, public risk and liability.
Management activities	These include the effects of changes implemented by management, or adverse effects of other risk mitigation or control measures such as change of leadership or a restructure or merger.
Natural events	Natural events include risks posed by natural disasters (cyclone, flood and drought) and longer-term risks associated with natural phenomena such as climate change.
Political circumstances	Changes in government at national, state or local level and the underlying politics may affect an organisation's way of doing business, services offered or products manufactured.
Technological issues	In organisations that have a high degree of reliance on technology, risk surrounds technology failures, redundancy, emerging technology and the associated costs of maintaining a technological edge over competitors.

Once you have understood your organisation's potential risks, you should familiarise yourself with the process it uses to manage them – regardless of whether you are managing risks across the whole organisation, a specific business unit or a particular area.

This table presents some criteria an organisation might use to categorise risks.

Property-centred risks	Property-centred risks include risks associated with: ▪ theft ▪ poor asset management ▪ the building.
Personnel-centred risks	Personnel-centred risks include risks associated with: ▪ personal safety ▪ travel accidents ▪ loss of personnel ▪ costs of recruitment ▪ public liability.
Market-centred risks	Market-centred risks include risks associated with: ▪ product liability ▪ falling product demand ▪ changing economic conditions ▪ competition ▪ lack of diversity of products and services.
Operation-centred risks	Operation-centred risks include risks associated with: ▪ suppliers ▪ information technology ▪ financial management.
Legislation-centred risks	Legislation-centred risks include risks associated with: ▪ work health and safety ▪ taxation ▪ equal opportunity.
Governance-centred risks	Governance-centred risks include risks associated with: ▪ poor risk management ▪ failure to take opportunities ▪ failure to provide policies and procedures ▪ failure to provide strategic direction.

Understanding an enterprise risk management approach

Enterprise risk management (ERM) is a holistic framework for managing risk as a corporate management strategy.

You may come across the term 'enterprise risk management' (ERM), particularly if you work for, or with, a large business and especially in the finance sector (brokerage houses, banks, etc.). The framework was developed in the United States in 2003 and is now widely employed as a common approach to risk management for many organisations and enterprises. ERM looks at risk management across four risk types and risk management processes, and aligns risk management goals with corporate or enterprise outcomes.

While there are different approaches to risk management at an organisational or enterprise level, they all follow the same four-part process which is:

- identifying the risks
- analysing the risk
- evaluating the risks
- treating the risks

Then monitoring and reviewing the risk management process as a continual cycle.

Following the Standard for risk management

In Australia, organisations generally follow the international risk management Standard, 'AS/NZS ISO 31000:2018 Risk management – Guidelines'.

The Standard provides practical advice on how organisations can develop, implement and improve the way they manage risk. It is designed to help organisations identify and treat risks effectively, improve risk controls, comply with relevant legal and regulatory requirements, and improve overall operational effectiveness and efficiency. Organisations can use the Standard as a benchmark against which to compare their own risk management practices.

Your organisation should have a copy of this Standard and you should keep up to date with any changes to the Standard or supplementary material produced.

Useful complementary publications that support the Standard include:

- 'IWA 31:2020 Risk management – Guidelines on using ISO 31000 in management systems'
- 'ISO/IEC 31010:2019 Risk management – Risk assessment techniques'
- 'ISO 31073:2022 Risk management – Vocabulary', which provides a collection of terms and definitions relating to risk management.

A process for managing risks

You need to be familiar with the steps for managing risks as stated in the AS/NZS ISO 31000:2018 Standard so you can see where and how they can be integrated into your organisation's existing practices and ensure all of the organisation's procedures are consistent with the Standard.

This table presents the steps and rationale for the process covered by the Standard.

Step 1: Communicate and consult	Consult with internal and external stakeholders at every step of the risk management process. In this way, you can be sure everyone understands why a procedure has been put in place and takes the identification and management of risks seriously.
Step 2: Establish the context	Establish the current conditions in which the organisation operates in an internal, external and risk management context. Define the criteria used to evaluate risk and establish a risk analysis framework.
Step 3: Identify the risks	Identify and document the factors that affect the organisation's goals, both positively and negatively. Determine how and why these factors exist.
Step 4: Analyse the risks	Analyse existing controls. Assess the likelihood of the occurrence of risks and their consequences within these controls. Combine consequence and likelihood to produce an estimated level of risk.
Step 5: Evaluate the risks	Compare estimated levels of risk with the established context developed in Step 2. Rank and prioritise risks within the contextual framework.
Step 6: Address the risks	Develop and implement strategies and management plans to prioritise and treat/control risks, in particular addressing high-priority risks. Lower priority risks may be accepted and monitored.
Step 7: Monitor and review the system	Monitor the risk management system at all stages to ascertain its effectiveness and track any changes that affect it. Revise the system to accommodate necessary changes identified during the monitoring.

Example

Understanding risk management processes

The risk management process as described in the AS/NZS ISO 31000:2018 Standard is as follows.

Communication and consultation			
Establish context	**Identify risks**	**Analyse and evaluate risks**	**Treat risks**
▪ Strategic plan ▪ Corporate plan ▪ Projects ▪ Policies ▪ Programs ▪ Business unit ▪ Disaster/ emergency	▪ Financial ▪ Legal ▪ Operational ▪ Market ▪ Construction ▪ Reputational	▪ Likelihood ▪ Consequence ▪ Adequacy of control measures ▪ Risk tolerance ▪ Action	▪ Strategic realignment ▪ Administrative actions ▪ Budget review ▪ Safety review ▪ Continuity planning ▪ Emergency planning ▪ Insurances

Determining the scope of risk management processes

Determining the scope is an important step in risk management as it enables you to see where risk management should be implemented. Accurately defining the scope at the outset allows you to apply your risk management resources in a targeted manner, avoid duplication and waste, and involve appropriate personnel where required. For example, if you get the scope wrong, your costs and resources will be wrong.

Determining the scope means identifying how widely – or narrowly – you wish to apply your risk management processes and measures. Do you need to develop a process for a project of a specific business division, unit or area; for a specific function, such as financial management or work health and safety; or for the organisation as a whole?

Often, the scope of the risk management process is deliberately limited by budget restraints, personnel resources or managerial directives. Even if your scope is predefined, you are still required to determine whether there is any overlap or ambiguity in the defined scope.

The scope of a risk management strategy may include:

- which business or organisational areas the risk management process is covering
- whether there are specific areas that require attention
- who the stakeholders are (who is affected by the process)
- who is involved in the implementation of the process
- time frames (for example, ongoing or cyclical processes)
- how far into the future you project your strategy.

Techniques for determining scope

Accurate determination of scope is essential to ensure organisational outcomes are achieved. Knowing why you are conducting risk management will help you understand what your risk management process has to achieve for you to be able to determine the scope.

Although this is not an exhaustive list, here are some questions you should ask when determining the scope of a risk management process:

- How is the organisation structured?
- What is the likelihood of risks occurring on a day-to-day basis?
- What is the purpose of the risk management process and what outcomes do we want?
- Is our scope defined in existing organisational documents or procedures?
- What are the limitations for completion of the process, in terms of time and resources?
- What business projects, units or areas will be examined?
- Are there any specific areas in these units that must be targeted?
- What time horizon will be used for identifying emerging risk (e.g. 12 months)?
- What potential risk types need to be addressed?

Example

Defining scope accurately

'Recently, I helped a high-risk, high-visibility project to succeed when all the observers were predicting failure because the project had hostile stakeholders, disengaged, part-time developers, a vendor trying to do things via long distance, an unrealistic scope, an arbitrary deadline, and a new project manager with no experience in software project management. The organisation had a well-defined business process which was being funded well to meet the deadline.

'With support from the organisation, I was able to improve the situation so that management were aware of the risks involved if the project wasn't implemented more efficiently. But most importantly we re-defined scope to match the exact legal definitions of the terms stated in the directive from management and nothing more. This cut 70 per cent of the features from the first release of the scope where superfluous and undefined areas were included.'

(Adapted from, and reproduced with the permission of, Digital Publications LLC, www.digitalpbs.com)

Practice Task 1

Question 1

Locate a copy of the AS/NZS ISO 31000:2018 Standard. If your organisation does not have a copy, your trainer will help you obtain one. Read the steps involved in risk management.

Outline the purpose and key elements of the Standard.

Question 2

Draw a line to match each type of business risk to its description.

» Legislation	» Company performance is affected due to morale or poor work culture. Often recognised as part of work health and safety.
» Natural events	» Risks associated with finance associated with international markets and domestic areas such as supplier/customer business failure or collapse.
» Commercial relationships	» Examples include reorganisation, relocation and differing federal, state and local requirements for licensing, public risk and liability.
» Human behaviour	» Risks posed by natural disasters and longer-term risks associated with natural phenomena such as climate change.
» Economic circumstances	» Risks of being associated with another organisation, directly or indirectly.

Question 3

Provide three examples of stakeholders that are responsible for risk management?

Question 4

Number each step from 1 to 7 in the order you would follow in the risk management process as outlined in the AS/NZS ISO 31000:2018 Standard.

- ◯ Address the risks
- ◯ Analyse the risks
- ◯ Establish the context
- ◯ Evaluate the risks
- ◯ Establish the context
- ◯ Monitor and review the system
- ◯ Communicate and consult

Question 5

Why is it important to define the scope for risk management purposes?

Question 6

What steps do you need to follow to define scope?

1B Review existing arrangements

Monitoring and reviewing are ongoing parts of the risk management process.

The context in which a business or organisation operates is fluid and dynamic, with old risks disappearing and new risks emerging. For example, the organisation may have grown since risk treatments were introduced, new technology may have rendered old controls obsolete, or the market may have changed. Key areas in the organisation that must be assessed for strengths and weaknesses include the organisation's culture, structure, capabilities (personnel, systems and resources) and strategic directions, goals and objectives. Before you conduct a risk assessment, you need to review the existing arrangements for managing risks to determine how effective or ineffective they are.

Questions you should ask when reviewing existing arrangements include:

- How do your existing internal mechanisms address the current environment?
- How is policy influencing the processes and procedures?
- What are the strengths and weaknesses of these mechanisms?

Determining strengths

Look at the strengths of your organisation's current policies, processes or procedures and acknowledge where they have worked effectively to manage risk. These strengths can be carried forward into any newly resulting policy, or amended, if appropriate, to current circumstances.

These are some examples of policy strengths:

- An effective alarm system has ensured a low risk of theft.
- Having firm contracts with suppliers has ensured timelines and costs are always met.
- Regular servicing of technology has ensured fewer breakdowns and less downtime.
- Effective market research has resulted in targeted products and increased profits.
- Forming partnerships has helped share the risk of a project.

Determining weaknesses

Look at previous documents and performance reports to identify any weaknesses in your current control measures. Identify whether any mechanisms based on an older policy, process or procedure are sufficient to deal with a contemporary event. For example, insurance cover may have been appropriate at the time when a strategy was developed but may now be inadequate. You may find that human error has resulted in a weakness, or otherwise sound policies or guidelines have been applied incorrectly or inadequately.

Once you have identified the weaknesses, you need to learn from them and adjust your current arrangements, such as redefining policies or introducing contingencies to ensure unforeseen circumstances are addressed. Make sure you understand what you are looking for when identifying a weakness in existing arrangements.

Here are some questions to ask when identifying weaknesses.

Was the weakness due to a failure to identify an unforeseeable event?
For example, some personnel were sick, and this caused a project to pass its deadline and incur additional costs.
Was the weakness due to a failure to predict technological breakthroughs?
For example, deciding not to introduce online purchasing cost the company customers and money.
Was the weakness due to a failure to communicate?
For example, procedures for informing stakeholders were not specific enough, resulting in key steps not being followed.
Was the risk strategy too broad?
For example, were there no measurable goals?
Was a decision inappropriate?
For example, deciding to save money by using a new distribution company was a knee-jerk reaction that in fact cost the company time and money as the new company did not meet its obligations.

Example

Identifying weaknesses in current risk management processes

Wheymore's Pastries, a supplier of pastries and bakery goods to a large national cafe chain, has an ageing risk management strategy in place.

- There has been minimal illness attributed to food contamination, so it is recommended to have no more than $10,000 liability cover for this risk.
- On review, the risk manager found that, in extreme cases, litigation over food poisoning had seen damages of up to $1.2 million awarded. This was classified as a severe risk to the company and it was noted that this weakness would have to be addressed as a priority in the current review cycle.

Reviewing the context of risk management activities

The context, or environment, in which you conduct your risk management activities should be reviewed regularly.

By reviewing the environment, you can achieve a greater understanding of how external factors can influence your risk assessment process and the potential threats or opportunities presented by these – now and into the future.

The environment includes the following contexts:

- political
- legal
- economic
- social
- technological
- policy.

Political and legal contexts

Political decisions made at the federal, state and local government levels can greatly affect your organisation's operations. In particular, a change of government may result in a different focus or economic direction. This can affect the way your organisation conducts its business, the products it provides and the rules and regulations it has to comply with.

The political context also includes the legal context. You need to be familiar with a range of legislation, codes of practice and national standards that relate to your organisation's risks. So make sure you know where to access the documentation and read relevant material that identifies upcoming political or legislative changes.

Legislation, codes of practice and national standards can relate to:

- duty of care: *Work Health and Safety Act 2011* (Cth)
- environmental law: *Environment Protection and Biodiversity Conservation Act 1999* (Cth)
- freedom of information: *Freedom of Information Act 1982* (Cth)
- industrial relations law: *Fair Work Act 2009* (Cth)
- privacy and confidentiality: *Privacy Act 1988* (Cth)
- access and equity legislation: *Disability Discrimination Act 1992* (Cth); *Age Discrimination Act 2004* (Cth); *Racial Discrimination Act 1975* (Cth); *Workplace Gender Equality Act 2012* (Cth)
- company and contract law, and competition and consumer protection: *Competition and Consumer Act 2010* (Cth)
- the AS/NZS ISO 31000:2019 Standard.

There are several key factors to consider if you want to understand the political and legal context of risk:

- It is important to be aware of any upcoming or proposed parliamentary Acts, legislation, decisions on legal challenges, regulatory amendments or other political changes and to find out whether they will affect your risk management scope.
- Risk assessments should identify the potential for accidents, and strategies should be in place to comply with all work health and safety laws.
- Check that the organisation complies with equal employment opportunity legislation to avoid any possibility of being sued for recruitment discrimination or wrongful dismissal.
- Ensure that the risk management policy and plan comply with anti-discrimination legislation to minimise the risk of litigation relating to age, gender or race discrimination.
- Organisations are required by law to make reasonable adjustments in the workplace for people with a disability. Risk assessments should consider possible risks for people with a disability; for example, whether all people have easy access to the building and facilities; and what safety measures are in place in relation to floor surfaces, railings, walkways and lighting.
- Competition and consumer protection laws govern an organisation's operations, so adequate protection should be built into the organisation's risk management strategy.

Economic context

Understanding the impact of changing economic conditions on business or organisational functions requires a review of not only the national economic conditions, but also the macro (global) and micro (local) economies. Reviewing the economic context allows you to gain a better understanding of possible future movements in the economy and therefore possible impacts on, or risks to, your organisation's operations. Examples of the key factors to be considered include:

- economic growth or downturn
- industry trends and cycles
- currency exchange rates (impact on export industries)
- disposable income or consumer confidence
- unemployment or underemployment rate.

You can research and access information on the economic context by reading documentation such as industry reports (e.g. IBISWorld), business reports and data from the Australian Bureau of Statistics.

Questions to ask about the possibility of economic risk include:

- Is there an opening for your organisation now that a competitor has gone?
- Is demand for your product falling?
- Will the organisation need to cut back on staff?

Social context

The social context in which your organisation operates represents demographic characteristics, changing social and cultural norms and values, and community awareness and attitudes. Examples of social trends include:

- the population growth rate, age distribution, income distribution and other factors that may impact the organisation's activities or how the services are delivered. Such factors can affect its brand, reputation, commercial relationships and retail sales
- changing social attitudes to consumption, health consciousness and lifestyle attitudes. This impacts how your organisation is viewed in the wider community
- the cultural context, including cultural barriers that may be perceived as risk
- the impact of social media; for example, the rise of social networking as an advertising medium and the need for financial accountability.

To evaluate the social context, research information on the Australian Bureau of Statistics website on demographics, use the Google Trends tool and read more widely to learn about social issues.

Technological context

It doesn't matter if you are in a high- or low-tech industry, changes in technology – from the smallest micro-processor or nanotechnology advancement to heavy plant equipment – can produce a risk to operations, particularly where these advances are also embraced by competitors. Does the technology produce real benefits? How much training and lead time is needed before benefits are seen?

Technology also has a flip-side, where a positive risk outcome may appear if a competitor rushes to embrace unproven technology that then fails to deliver promised potential. By reviewing the technological context, you gain an understanding of what technologies are on the horizon and the risks that may emerge from either introducing or not introducing them. Read research into current technological advances and monitor industry publications for information relevant to your organisation.

Policy context

Policy can refer to both government policy (often known as 'public policy risk') and internal policies. Policies must be reviewed to understand how risk management can be applied to existing internal guidelines. A review can also provide the impetus to push for policy change where risks cannot be adequately managed otherwise.

Here are some examples of policy contexts.

Government policy
A particular party's stance on the environmental impact of a certain industry where the policy may present risks by impeding political support.
Internal policies
Policy issues that prevent adequate responses to emergent risks where internal policy was written before a law was introduced.

Example

Understanding the context

The following example shows how one organisation reviewed the political, legal, social, technological and policy contexts.

'When our Queensland-based doors and windows business expanded into New South Wales in early 2011, we looked at the context we were moving into. Not only did we have to examine what our competition would be – the obvious first step – but also such things as the different building codes, licensing, permits and legislative requirements and so on. Much of this occurred after we had set up shop, which was hardly ideal.

'In 2014, following some sustained growth, we looked to move into Victoria and Western Australia. These turned out to be quite diverse markets in terms of legal, economic and social context. This time, however, we conducted a risk evaluation that highlighted the need for us to address these contextual differences prior to making a move. Victoria had quite different material and construction standards, while in Western Australia the codes varied dramatically based on regions, allowing for cyclone standards in the north. A major benefit of this contextual analysis was that we identified the parochialism demonstrated by WA consumers for our competitor's established brand.'

Practice Task 2

Refer to the previous example in the Learner Guide to answer Question 1.

Question 1

For each of the following areas below, provide at least two examples that may present as risks to the business.

a) Political context

b) Economic context

c) Social context

d) Technological context

e) Policy context

Question 2

Select three of the following areas and provide an example of corresponding legislation. Briefly outline its relevance to the development of a risk management strategy.

- duty of care
- company law
- contract law
- environmental law
- freedom of information
- industrial relations law
- privacy and confidentiality
- legislation relevant to the organisation's operations
- legislation relevant to the organisation as a business entity

1C Document critical success factors, goals and objectives

When preparing your risk management context, it is important to identify and document the outcomes of any research you.

By documenting your critical success factors, goals and objectives you can be confident that you understand and are able to develop and manage comprehensive strategies that target the particular risks facing your organisation.

Identifying critical success factors

It is important to know how you will measure the success of your risk management strategies.

A successful strategy cannot be measured by simply looking at how well the organisation is running or by establishing that no risks have eventuated, because these circumstances could be due to contributing factors such as there not being any risk, or even pure luck. To measure your strategy's success, you also need to include other measurable factors. Ask experienced practitioners, your trainer or your manager whether there are any other factors they think are important for risk management success.

Here are some areas that most people agree are essential for success.

Scope	The scope of the risk management should be correctly identified; if it has not been, you might waste your time developing an inappropriate or ineffective strategy.
Stakeholders	All stakeholders should be consulted and should agree on the scope of the strategy; if there are issues that have not been resolved, they may surface later and give rise to additional time or costs.
Resources	Risk management should be sufficiently resourced; if it is not, a strategy may be ineffective or counter-productive.
Goals	Goals and outcomes should be clearly defined, realistic, achievable and measurable.

Setting goals, objectives and outcomes

Before you develop a risk management strategy, identify the desired outcomes.

Setting goals provides you with benchmarks you can use when you evaluate the success or otherwise of your risk management process.

Although the terms 'goals' and 'objectives' are often used interchangeably, there is a slight difference. Goals are usually broad and long term, and objectives are more specific targets.

Many people apply the SMART principles to help them ensure their objectives are specific, measurable, attainable, realistic and timely. It is unlikely, for example, that you will be able to eliminate all risk. It would be better to say you will reduce risk to an acceptable level; or provide sufficient offset of risk through risk sharing or reduction methods for it to become acceptable; or that the risks have been documented and measures put in place should a contingency arise.

Here are the SMART principles:

Specific	Target and clearly define a specific area that you want to improve.
Measurable	Suggest an indicator of progress; quantify if possible. Determine how you will know the objective has been achieved.
Attainable	Agree what the objectives should be and keep them achievable within the time frame.
Realistic	Identify what results can realistically be achieved given the available resources, knowledge and time.
Time framed	Specify when the result can be achieved; make sure there is enough time to achieve the objective, but not too much time.

Using the SMART principles to set objectives

Use the SMART principles to set objectives for each goal or specific item in your scope. For example, if the scope of your risk management includes technology, your objective might be 'to reduce technology breakdowns by 70 per cent within three months'. By applying the SMART principles, you might find three months is too short a time to realistically improve technology performance, so you might adjust this objective to six months. Similarly, if your organisation uses suppliers, a goal might be 'to ensure suppliers meet organisational requirements'. This is a broad and less-defined goal, so you may need to articulate what the requirements are, such as contracts, timely delivery and high-quality service.

Documenting goals, objectives and outcomes

After identifying your desired outcomes, document your goals, objectives and outcomes so that you have a road map to keep you on task.

Documenting your goals, objectives and outcomes allows you to revisit and modify the content as your risk environment changes. A documented set of goals should be advertised to stakeholders for comment and feedback. It should also be advertised to the wider workforce, to allow the process to be transparent and encourage participation.

Example

Setting objectives

A gym has lost several personal trainers recently due to injuries. Given that much of the gym's income is generated by the personal trainers, management wishes to implement a risk management strategy for training staff to reduce lost time and increase the business's productivity. The scope includes all trainers at the gym. The desired outcome of this risk management strategy is 'to reduce the rate of trainer absence (due to injury) to 10 per cent of the total trainers on staff by the end of a three-month time frame'.

The business goals will be achieved by:

- implementing a roster for trainers
- expanding the pool of trainers
- ensuring all staff are trained for each piece of equipment and technique, as well as in work health and safety, and stress and conflict resolution.

Practice Task 3

Refer to the previous example in the Learner Guide to answer Question 1.

Question 1

Identify the SMART objectives as they are applied in the example and include any information you believe may have been left out or overlooked. Reword the objectives to reflect each of the SMART elements.

Question 2

List three factors that are critical to the success of a risk management process.

1D Communicate risk process to stakeholders

Risk management cannot operate without the full support of all stakeholders and participants in the process.

It is especially important for senior management to commit to the process of identifying and communicating with stakeholders to show leadership. Management support is crucial in seeking approval for the risk management plan, gaining authorisation for allocating human and physical resources and implementing the plan effectively. Communication is the key to gaining and having continued support, especially in motivating staff to comply with the procedures and processes. You can communicate the benefits of risk management to all participants, stakeholders and staff members via various media such as presentations, meetings, newsletters, email and websites to encourage a risk-aware workplace culture. It may also be useful to invite guest speakers, such as insurance brokers or commercial financiers, to give presentations on external benefits to the company of conducting risk management activities.

It is important to remember that as risks emerge, evolve, mutate or disappear, you will need to change your processes accordingly. Consequently, you need to maintain support from directors and management to modify processes to achieve risk management goals and ensure the ongoing success of the process.

Identifying stakeholders

When initiating a risk management process, you need to identify who has a stake in the process and any outcomes that may flow from their involvement.

Stakeholders are all those directly involved in the risk management process; that is, personnel in your organisation and externally, such as such as clients and customers, contractors, regulators, insurers/underwriters and investors. Look at each area affected by your risk management application and determine the stakeholders. For example, if your scope includes examining logistical risks such as inventories, costs, transport and facilities, you need to include managers, budget controllers, accountants, insurers and safety advisors from the logistics area.

Here is a list of people you may need to identify and work with as you manage your organisation's risk management strategy.

Internal stakeholders
▪ Owners ▪ Employees ▪ Managers
External stakeholders
▪ Suppliers ▪ Society ▪ Government ▪ Creditors ▪ Customers

Consulting with stakeholders

It is essential to consult with people who can provide information about risks, as well as those likely to be affected by the processes or potential impacts or outcomes of identified risks.

Stakeholders may have different and occasionally conflicting concerns and issues they need to voice or want you to address. You have to maintain a high level of interpersonal communication skills to encourage stakeholder cooperation. You should also establish what information about the process stakeholders want to be informed of, and when. If you workshop a reporting schedule with your stakeholders at this point, you can pre-program reporting times as part of the process. By understanding your stakeholders, you can predict or pre-empt any issues that may arise. Most importantly, they will want to know how the process involves them.

Other issues that may arise are those involving:

- costs
- timing
- resources
- other personnel involved
- aspects of the process itself.

Prioritising

Finally, when all stakeholders have been identified, you need to prioritise participants according to their stake in the process. Not everyone needs to be informed or consulted about every part of the risk process. Don't be tempted to rank the participants by number, as this can be difficult and even unhelpful where the stakeholding is equal. Assign them into one of three areas: high, medium and low priority.

Example

Involving a wide range of stakeholders

The following information, adapted from the NSW Office of Environment and Heritage, shows the wide range of stakeholders that can be involved in a project.

Stakeholders include:

- owners and operators in local industries and businesses
- local councils
- local chambers of manufacture
- local catchment management committees
- industry associations
- local chambers of commerce
- local media.

Stakeholders are:

- concerned about 'painting industries in a bad light'
- concerned about discouraging further business and industry from setting up in the area
- of the view that 'business development' and 'environment' have little common ground.

Communicating the benefits of risk management

In your communications, you should help stakeholders understand the wider implications of risk management.

If you are doing a presentation, you should discuss how a risk management strategy enables an organisation to protect its assets, allocate resources wisely, reduce the chance of making strategic mistakes and help minimise financial losses. You might also discuss how having a sound risk management process helps an organisation take advantage of opportunities and plan more effectively, as well as minimise the threat of possible negligence claims. You might mention how the process shows good governance and sound business practices and provides a solid basis for doing business, taking on partnerships and forming alliances.

Tips for creating a presentation include:

- expressing benefits in terms your audience can understand. Don't use technical words or jargon your audience may be unfamiliar with
- framing the process in terms of corporate objectives
- relating the process to previous events, current conditions or planned future courses of action
- relating the process to the organisation's competition: What is the competition doing? Will this give us a competitive advantage?

Communicating the risk management process and inviting participation

The best way to achieve support and ultimate success for any risk management process is to maintain open and transparent lines of communication with your stakeholders.

You need to relate information to the various groups that have a direct stake in the risk management process. Remember, you want to get generic information about the risk management process out to as many of those involved as possible, while targeting special-interest stakeholders. Make sure you have included the following people and know how and why they are involved.

All staff in the organisation
Type of information you need to provide: ▪ How the process will affect them personally ▪ Benefits to themselves and the company ▪ Their role in the development process ▪ Meeting times ▪ Their role in following the control measures ▪ Type of information they can provide: ▪ Potential risks ▪ Solutions they have applied to risks

Senior management, directors
Type of information you need to provide: ▪ The impact on operations and time required ▪ Steps to be followed in the risk management process ▪ What input they are required to provide ▪ What the process will achieve and draft outcomes ▪ Risk management areas to be addressed ▪ Timelines for ongoing review ▪ How they can support the process ▪ Type of information they can provide: ▪ Organisation's business plans and strategic directions ▪ Annual report showing current situation (sales, competition, success or weakness of current risk management strategies) ▪ Advice and suggestions from previous experience
Specific teams or business units
Type of information you need to provide: ▪ Details about the risk management process ▪ What they need to do ▪ How this will affect their existing business objectives ▪ Whether they will have to change their processes ▪ The likely impact on their human resources ▪ Other stakeholders ▪ Meeting schedules ▪ Type of information they can provide: ▪ Potential risks ▪ Solutions they have applied to risks
Technical experts
Type of information you need to provide: ▪ Details about the risk management process ▪ When and where they will be required ▪ What they need to do ▪ How their business/job role may be affected ▪ Meeting schedules ▪ Type of information they can provide: ▪ Possible technological risks ▪ Strategies for contingencies

External stakeholders
Type of information you need to provide: ▪ Details about the risk management process ▪ The cost of the process to the company ▪ How their business with the organisation may be affected ▪ Benefits to their organisation ▪ Whether their business practices need to be changed ▪ Stakeholders ▪ Meeting schedules ▪ Type of information they can provide: ▪ Potential risks ▪ Solutions they have applied to risks ▪ Previous arrangements that were successful

Using appropriate communication strategies

Communicating the process does not require endless meetings with all concerned or constant one-on-one time with every stakeholder. Communicating the process can be done via print or a presentation, or electronically. The method/s you use to communicate your information depends on variables such as the size of your stakeholder body, the number of participants in the process, the scope and the time frame for the activities.

Communication options can include:

- training and risk workshops
- briefings
- report back presentations
- communication booklets
- websites
- newsletters
- intranet/emails
- articles and periodicals
- corporate plans and strategies.

Example

Involving all stakeholders

At a small Victorian boatbuilding and fibreglass factory, the managers recently began putting in place a risk management strategy for the safety of their workers, facilities and the environment. Their approach was to sell the environmental aspects to the public and the safety aspects to their staff and contractors.

As part of the process, they invited the general public to participate by providing environmental concerns and feedback, while union and health and safety representatives, WorkSafe (Vic.) representatives and several worker representatives were asked to sit in on the initial planning meetings and offered places on the risk management committee. The results of the meeting, along with the names of the new committee, were published in the local community newspaper and the company's staff newsletter.

Practice Task 4

Question 1

Identify the internal stakeholders in risk management for a project in your organisation.

Question 2

Identify the external stakeholders. Be specific and target them to your organisation, industry sector or local constituency and state bodies. For example, don't use 'government', but specify (e.g. 'Wollongong Council Planning Department', 'Wollongong Development Corporation', 'WorkCover NSW').

Question 3

Prioritise these stakeholders' involvement as high, medium or low priority.

Question 4

Against each stakeholder, list an issue they are likely to have.

Question 5

Imagine you are the risk manager (with a small team) for your organisation or one you are familiar with. Draft an email to the board or senior management of your organisation requesting support for the risk management process. Include information about the goals, scope and benefits of the process and list the areas in which you intend to conduct risk identification.

Question 6

What communication methods would you use to inform internal stakeholders about the overall progress of the risk management process?

Question 7

What communication methods would you use to obtain formal support from management and external stakeholders?

Summary

- Any risk management process begins with reviewing the organisation's existing processes, procedures and requirements for risk management.
- Once the baseline procedure has been established, scope should be determined to ensure resources can be allocated efficiently.
- The risk context is established by looking at the current political, economic, social, legal, technological and policy environments.
- Risk criteria are defined and goals and success factors are set using SMART goals where possible.
- Stakeholders – that is, everyone, both internally and externally, who has a vested interest in an organisation's risk management – are identified and their issues noted.
- Support for the risk management process is gained through positive engagement, open communication and consultation with stakeholders.

Learning Checkpoint 1
Establish the risk context

Part A

Access and review your organisation's workplace policies and procedures (or those of an organisation that you are familiar with). Policies and procedures must include those relating to:

- risk management processes or plans
- WHS legislation
- equal employment opportunity laws
- anti-discrimination laws
- competition and consumer protection
- privacy laws.

Answer the following questions to evaluate each policy and procedure.

1. What is the significance of reviewing and analysing the existing risk management processes, procedures and requirements before updating a risk management plan?

2. Explain why it is essential to clearly identify the scope of risk management.

3. What specific types of documentation and sources of information should be reviewed during the 'establishing the risk context' stage of the risk management process?

4. Reword the following statement to become a goal (or two) for a risk management process: 'We are conducting risk management at this time to ensure our shareholders and investors maintain confidence that the board is comfortable with its current risk exposure'.

5. Provide two reasons why it is important to gain support for risk management activities in an organisation?

Part B

Read the case study, then answer the questions that follow.

Case study

In early 2013, Lily Hi, a clothing retail company from New South Wales, launched into the Queensland and Victorian markets simultaneously. Before the launch, the company conducted a minimal risk management process: it determined a very limited scope that included only the financial aspects of competition. Only management was involved. Their stated goal was to 'be successful'.

The company struggled against competition and local government issues in Victoria, which led to the store closing and Lily Hi withdrawing from the market in that state.

The case highlights a lack of understanding of the risk context faced in Victoria, but there may have also been over-exuberance on behalf of management, who may not have estimated the risks of moving into two markets simultaneously.

1. Identify two types of business risks that Lily Hi should have investigated.

2. Outline the mistakes the management team made

3. List at least three strategies the management of Lily Hi could put in place to ensure this doesn't happen again.

4. How would knowing about AS/NZS ISO 31000:2018 Risk management – Principles and guidelines have helped management at Lily Hi?

5. Document the following information as you prepare to develop a risk management plan for your organisation, unit or area:
   - An overview of the operations of the organisation
   - A brief overview of the strengths and weaknesses of current arrangements
   - The scope of your risk management processes
   - The internal and external stakeholders, their priority ranking and their issues
   - The political, economic, social, legal, technological and policy context for your risk management strategy
   - The goals and objectives for the areas in your scope
   - The critical success factors for the areas in your scope
   - How you will communicate with all parties.

Topic 2 | Identify risks

2A Invite stakeholders to assist in identifying risks

2B Research the risks

2C Document the risks

2A Invite stakeholders to assist in identifying risks

When identifying risks, it is essential that everyone involved in the organisation who is affected by risk management decisions is consulted and has the opportunity to provide input.

These stakeholders can contribute their expertise and experience to help you prepare a list of potential risks over a range of areas. By doing this, they feel valued and gain a degree of ownership of the risk management process.

In addition to inviting internal personnel (such as managers and staff) to participate, you may need to target specific stakeholders, advisors, technical experts or other specialist personnel. When a course of action may affect the public, you might need to consult residents, councillors and other local stakeholders. The type of specialist who can assist you with risk identification depends on the types of risk you expect to encounter. By using everyone's knowledge and skills, you can generate a list of risks you may not have considered.

Parties for consultation

Here are some of the stakeholders, consultants and specialists you may need to consult and invite to participate in identifying risks in your organisation or business area. Each can offer specific information and assistance.

Finance	▪ Accountant (internal): audited books, profit/loss details, financial impact of previous events, costings for risk servicing, financial impacts of negative (or positive) risk events ▪ Directors/members of the board (internal): strategic planning, upcoming events, mergers, acquisitions, disposals ▪ Auditors (external): financial risks associated with other entities ▪ Financiers (external): risks associated with borrowings, refinancing, currency movement (exchange rates, interest rates) ▪ Shareholders (external): their perceptions of future events, whether they would participate in share buybacks, splits, new issues, etc.

Sales and marketing	▪ Marketing managers (internal): market research on current conditions, budgets, advertising campaigns ▪ Marketing research company (external): broader market research budgets/ advertising campaigns than may be possible using internal assets ▪ Members of the public (external): attitude towards the company (reputation), level of trust in the company's product or service ▪ Shareholders (external): initial feelings about future advertising campaigns, effectiveness of current marketing
Security	▪ Department heads (internal): concerns regarding personnel, general feeling towards the company by employees (HR risks) ▪ Security firm (external): physical and electronic security risks and vulnerabilities, industrial espionage
Equipment	▪ Equipment operators: intimate knowledge of safety risks associated with operating specific plant, equipment or machinery
Safety	▪ WHS representatives (internal): conversant with company WHS policy, and probably national/state legislation ▪ WHS advisors (external): conversant with state and federal WHS policy, codes, legislation and regulations ▪ Trade unions/labour representatives (external): represent members' conditions at work ▪ Specialists: provide in-depth knowledge of specified hazards: chemicals, pharmaceuticals, asbestos, corrosives, etc.
Personnel	▪ HR managers (internal): identifying personnel issues, morale, training deficiencies, gripes or complaints ▪ Security firm (external): advice on identifying potential for theft, fraud, malicious damage
Legal	▪ Directors/members of the board (internal): due diligence matters, corporate governance issues, disclosure requirements, legal requirements of directors ▪ Legal advisors (external): corporate law advice regarding business entity dealings, advice on product liabilities, general advice on legal position in litigation, copyright, etc. ▪ Specialist lawyers (external): specialist legal issues or matters, litigation, copyright and patent infringement, etc.
Political	▪ Political analyst (external): party doctrine advice, political affiliations, possible direction of policy by governments, political sensitivities

A strategy for consultation

Once you know who you are going to invite to help you identify workplace risks, you can prepare a strategy for how to make this happen.

Here are some consultation procedures to follow when preparing a risk strategy.

Thumb	Contact participants by formal letter, mail or telephone.
Finger 1	Explain the scope of the risk management.
Finger 2	Describe the expertise they can offer.
Finger 3	Arrange a forum for their contribution, such as a one-on-one meeting, interview discussion, focus group or public consultation meeting.
Finger 4	Ask participants to bring along or send you relevant documents that justify their points of view.

Example

Inviting specialists to identify risks

In conducting a risk assessment for a large hardware firm, area manager James identifies several areas in the scope that are beyond his field of expertise. This includes the requirement to assess the risk of unbudgeted repairs to ageing storage and logistics facilities, particularly where it is suspected that asbestos is present. James also identifies that there is insufficient expertise in dealing with asbestos and the impact of treating such a risk in his organisation, so James invites specialist asbestos removal personnel to assist with the assessment.

Practice Task 5

Question 1

Identify at least three stakeholders that could be invited to assist to determine the risks.

Question 2

Outline the method/s that could be used with stakeholders to identify risks.

2B Research the risks

After determining the scope of your risk assessment, you may have some idea of the associated potential risks.

If you are working with an existing risk management plan, it is likely that some risks have already been eliminated and new ones have emerged. If the plan covers the whole organisation, there may be risks associated with other divisions, departments or work units external to your direct area of responsibility that you may not be aware of. For these reasons, you need to do some research to ensure you identify all the major risks within the scope. While part of this research includes involving the stakeholders, consultants and other people you have already identified as being able to provide expertise and input, these people have localised knowledge of what risks they face in their own context, but not necessarily at a group or enterprise level. Therefore, you cannot rely on this method alone. There are several ways to research potential risks, including collecting statistical information, identifying lessons learnt from previous projects and conducting market research.

Research methods

Here is a list of relevant research methods you can use. Once you have determined the way you will conduct your research, you need to put this into action. As you work through your research, document the risks you and others identify. This initial list will later be refined and organised, then analysed in depth.

Statistics	▪ Collect information about existing and potential risks for all the areas of your scope relevant to your context of operations, such as financial, property, market, legislation and personnel. ▪ Consult sales statistics, competitor data, work health and safety information, and financial statistics. ▪ Access agencies such as the Australian Bureau of Statistics or market research organisations for statistics on market share, population, sales trends and economic forecasts.
Business areas	▪ Managers and staff in other business areas in the organisation may be able to tell you about similar, coincidental or concurrent risks they are facing. ▪ This information can be obtained through formal, structured sessions or one-on-one meetings.

Previous activities	▪ Formal reports and anecdotal evidence can tell you what risks were faced, what unexpected risks arose and how they were managed in similar projects or activities that have previously been undertaken. What lessons were learnt? ▪ For example, if a project went over budget (the risk) it may have failed to include incidentals (the cause of the risk). Being aware of this might ensure you don't make the same mistake.
Market research	▪ You might ask your sales and marketing division to conduct market research into potential risks associated with your organisation's business operations, such as demand for product, competitor activity and new technology. ▪ Alternatively, you may need to commission research from an external marketing company to provide a new or fresh insight into consumer sentiment, cultural context and market directions.
Previous experience	▪ It's useful to harness the experience that others have gained through their current work, previous jobs or life experience. They might be able to mentor you or show you how to predict the cause of a risk and minimise its impact. ▪ For example, pooling experiences from inside your organisation may mean you gain a better understanding of how to use certain equipment, of the environment or context in which the company operates, or of the stability of suppliers and clients. You might identify risks you have never considered before.
Public consultation	▪ Where a course of action may affect the public in any way, it is worth consulting residents, local officials and the wider populace to determine what types of risk there might be; for example, public liability for outdoor events; or environmental risks to endangered local species in the case of a building development project.
Literature reviews	▪ Operational guides, user manuals and operator instructions contain advice on risks or hazards associated with equipment. ▪ A SWOT analysis may have identified risks. ▪ For example, an opportunity to introduce an online business department might identify risks such as a lack of sales due to poor marketing, a financial blow-out due to poor budgeting or increased sales due to correctly identifying the target market. ▪ An audit may have highlighted areas of concern; for example, repetitive work, storage of chemicals, security.

Generating a draft list of potential risks

Prepare a draft list of the risks stakeholders and your research have identified that apply to your scope.

Your draft list will be refined as you carry out further research and analysis until you have a final list that you can take to stakeholders for confirmation. It's a good idea to categorise the potential risks under the areas the organisation uses in its risk management plan, such as financial, technological and operational. As you identify the risks, it's also useful to find out the nature of the risk. What factors are contributing to the cause of the risk? Are they internal or external?

Example

Identifying stock market risks

It is important to consider stock market risks before entering any share purchase.

When investing in or making money from initial public offerings (IPOs) on the stock exchange, proper education and careful research are vital. Research must examine the risks of investing in these offerings, such as business, financial and market risks.

Many investors and large investment firms have been burnt during market downturns by not adequately hedging, or insuring, their large exposures to single stocks. Risks were accepted without an adequate understanding of either the historical or current risk context, due to lack of research into the risks.

Practice Task 6

Question 1

Draw a line to match each research method to its description.

» Literature reviews	» Using sales figures, competitor data, work health and safety information, and financial budgets and end of year results.
» Public consultation	» Referring to the Australian Bureau of Statistics or market research organisations for information.
» Statistics	» Consulting with staff in other areas in the organisation to find out about similar, coincidental or concurrent risks they are facing.
» Business areas	» Investigating potential risks associated with your organisation's business operations, such as demand for product, competitor activity and new technology.

Question 2

A business is about to become a market-capitalised, independent listed company. List the potential risks that research may uncover.

2C Document the risks

The draft list of risks you have identified should be as comprehensive and specific as possible.

Ensure you've captured all the risks applicable to your scope and not just those in a few areas of expertise. How many of the risks you identified are either irrelevant or insignificant when contextualised?

At this point you should meet with your stakeholders and invited participants to document a thorough list of risks in line with the scope. To achieve this most effectively, you need to apply a range of tools and techniques. However, it is important to remember that regardless of the tools or techniques chosen, the result is only as good as its inputs; that is, if you make use of specialists from the fields or areas of your scope, you will have a far more complete and extensive list of risks than you may otherwise generate.

Brainstorming

Brainstorming is a technique commonly used to identify a range of ideas from many different perspectives.

Remember to take note of all responses from participants. Then filter the results to eliminate duplicates and refine each suggestion further for clarity. To gain the most from brainstorming, be well prepared with a structured plan to conduct the session. For example, you might go through the categories identified in the business plan and ask what the participants think are the possible risks for each one.

Here are examples of suggestions made for two risk areas:

- Market-centred risks may include falling product demand, competition, lack of diversity of products, changing economic conditions, and sales and marketing management.
- Technology risks may include equipment breakdown, viruses, lack of training, poor management and using an outdated system.

Using fishbone diagrams

A fishbone or Ishikawa diagram (named after its inventor) is often used in project management for cause and effect identification.

To apply this to risk identification, you start by writing the category on the 'backbone' of the fish, then spin off into the smaller 'bones' as you identify risks and refine your ideas. The risks become clearer and more focused.

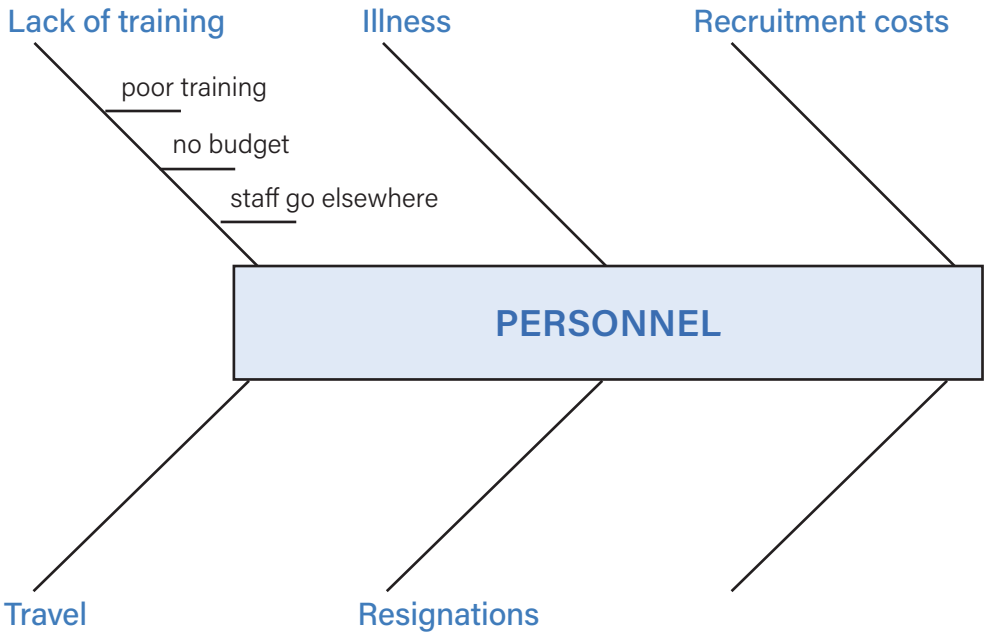
Here are the steps for preparing a fishbone diagram in collaboration with participants.

1. Prepare the basic framework of the fishbone diagram on a whiteboard or a large piece of paper.
2. Define the category that needs to be addressed and write it in clear and simple terms in the fish's spine; for example, 'Personnel'.
3. Identify and define the risks associated with personnel on the major 'bones' and write these at the tips. These headings could be developed through a brainstorming session focusing on the category in the fish's spine.
4. Tease out the causes or contributing factors (risks) by further brainstorming and by adding these ideas and suggestions to the smaller bones on the diagram.
5. Interpret the fishbone diagram once it's finished to develop a checklist of risks.

Example

Fishbone diagram

Here is an example of a fishbone diagram. It shows how personnel risks might include lack of training, illness, recruitment costs, travel and resignations.



Using flow charts

This method allows you to progress ideas through logical steps. This is not so much a development tool as a process-streaming tool in that a flow chart can be used to spawn ideas by analysing each step of a project or process for potential risks. By looking at each step and documenting it on the flow chart, you may be able to identify the risks inherent in each step.

For example, steps in property management would involve:

- screening the potential tenants
- signing them to a lease
- making regular property inspections.

Using a scenario analysis

Working from a given scenario can be an effective way to identify risks from ideas that may not come to mind in a normal brainstorm-type session.

Scenario building lets stakeholders review each stage of the process, identifying all possible outcomes from each course of action in the scenario and also the most likely occurrences (higher risk of actuating). From the list of likely outcomes, a prioritised list can be developed to help managers with future contingency planning.

Here are the steps for preparing a scenario analysis in collaboration with participants.

1. Prepare the basic scenario on a whiteboard or a large piece of paper; for example, releasing a new product onto the market.
2. From the basic storyline, identify participants and plot a course of action.
3. Identify and define the major actions and a 'safe' route, where no risks are encountered. For example, releasing a new product onto the market may include actions such as a product launch, advertising blitz, free sample promotions, and so on.
4. Tease out the potential deviations from the planned 'safe' route (unforeseen incidents or contingencies) by further brainstorming, and add these ideas and suggestions along the pathway.
5. Interpret the scenario once it has finished to develop a checklist.

Documenting a final list of risks

Checklists are a useful way to manage data. Simply list the risks as you identify them through your research, brainstorming, flow charts and analysis. Remember to categorise them as you go under specific categories according to the organisation's risk management process and procedures, such as finance, technology and business operations. Check with stakeholders and other participants to ensure they agree the risks identified are relevant and may occur. At this point the main objective is to list the risks to prepare for a more detailed analysis.

Topic 4 will discuss how to maintain risk management documentation in more detail.

Example

Identifying risks

These two examples show the benefits of using research and consultation to identify risks.

Using a scenario analysis
In a risk management team meeting for a small packaging products company in Perth, more than 40 risks are identified by the research team investigating up-scaling operations. However, a subsequent brainstorming session follows with an applied scenario analysis (playing out all possible outcomes in terms of technology, efficiency gains, market/competition) that indicates that more than half of the risks are unacceptable or insignificant, and a further eight are irrelevant to the context. This allows the team to concentrate fully on the remaining 11 risks, reducing the overall risk to an acceptable level for management to proceed with the project.
Consulting
The board of Soulcede Packaging and Plastics initiates a risk management plan for safety at their manufacturing facility in western Sydney. The process of risk identification is passed to a three-person team comprising a safety officer, a union steward and the facility manager. The first point on Soulcede's agenda is to invite specialists in to assist in recognising and understanding the risks in the plant's processes. The specialists include a chemicals advisor, a technical advisor from the company that made the plant's machinery, a representative from the fire department and an external work health and safety auditor. With the help of these extra personnel, the Soulcede team shares research information about the various safety risks and hazards at the plant. These are quickly filtered, and generic risks and hazards are identified to fit the scope as provided by the board and refined earlier.

Practice Task 7

Question 1

Choose three techniques for identifying risks and briefly outline the benefits of each method.

Summary

- When identifying the risks to your organisation, it is wise to engage with stakeholder specialists – both internal and external – in the areas or fields of your scope. They provide you with the greatest opportunity to capture all relevant risks.
- Once you have identified your risks, research them thoroughly using a range of sources such as existing data and statistics, market research, literature reviews, lessons from experience and public consultation.
- Use a variety of appropriate tools and techniques to further identify risks and ensure you have covered each area thoroughly. These may include brainstorming, fishbone diagrams, checklists, flow charts and scenario analyses.

Learning Checkpoint 2
Identify risks

Part A

1. Explain the benefits of having a range of stakeholders to be involved in identifying risks.

2. In the table below, list five research methods that may be used in determining operating risks relevant to a small car-tyre retailer, and describe what general type of information may be retrieved or gained from each of these methods. An example has been done for you.

Research method	Operating risks
Survey	▪ Collect responses from owners about previous difficulties to understand potential business risks. ▪ Seek customer feedback about both positive and negative experiences to understand process requirements. ▪ Collect responses from accountants about financial risks.

Research method	Operating risks

3. Give three advantages of using a scenario analysis to identify risks?

Part B

Read the case study, then answer the questions that follow.

Case study

Greenville Emergency Management fire service personnel have conducted a risk assessment for fire risks at a suburban distribution centre that is adjacent to chemical plants and virgin bushland on two sides. The process is handed to new staff as an exercise to help their learning and understanding of the risk assessor's roles. The staff have to research current arrangements such as warning systems, staffing levels, the chemicals involved, expertise available to fight a fire, and how much time there may be before a fire approaches.

The scope of the assessment is to determine health and safety risks to workers in the distribution centre should a bushfire come through the area. They are asked to use some analysis techniques to generate a list of risks.

1. What personnel should be invited to participate in the risk identification and research process?

2. What research methods could be applied?

3. What appropriate tools and techniques could be used to ensure all possible risks have been identified?

Part C: Report

In the organisation you work for, or one you have access to, access a range of appropriate personnel, research methods and analysis techniques to identify risks in the organisation or a business area.

Present your analysis under the following headings, or use a table:

- Stakeholders: the people you will speak to and what they can offer
- Consultation methods used
- Methods used to research the risks
- Tools and techniques used to generate a final list of risks
- A final list of at least five risks, generated in consultation with relevant parties.

Item	Action
Stakeholders	
Consultation methods	
Research methods	
Tools and techniques	

Topic 3 | Analyse risks

3A Assess the likelihood of risks occurring

3B Assess the impact or consequences of risks

3C Evaluate and prioritise risks for treatment

3A Assess the likelihood of risks occurring

It is important to determine the likelihood of an organisation, business unit, individual, project or activity being exposed to any risks you identify.

Frequency of exposure to a risk and the likelihood of it occurring are usually expressed as a range: from whether you're certain an area will be exposed to the risk (very likely), to whether you think it's possible (likely), to whether it would be a rare occurrence (unlikely). Some organisations use terms such as expected, probable, possible, improbable and rare.

Likelihood is usually expressed in terms of:

- probability (the chance that when a risk exists, a consequence will follow)
- frequency of exposure to the risk (how often and for how long the source of the risk exists)
- a combination of both.

Assigning an accurate ranking

When assigning a ranking, the first thing to do is check what systems are already in place and what terminology is used to analyse, manage and control risks.

The systems in place should form the basis of your risk analysis. Make sure you have relevant and accurate information available for your analysis.

To be able to assign an accurate ranking, you need to:

- look at past records, reports and the organisation's risk management plan to find out how often the risk has eventuated and whether the organisation is prepared for it
- question relevant people who have had similar experiences to see what ranking they would give the risk
- analyse market research that may predict future circumstances
- conduct research using the internet, journals and trade magazines, government policies and competitors' experiences to understand the nature of the risk and the likelihood of the organisation's exposure to it.

Types of risk analysis

There are three types of risk analysis: qualitative, semi-qualitative and quantitative.

Which type/s of risk analysis you use – qualitative, semi-qualitative and/or quantitative – depends on the data available.

In practice, qualitative analysis is generally used to obtain an indication of risk levels. It is only when more specific and precise indicators are required that quantitative analysis is applied to risk analysis.

Qualitative analysis

Qualitative means using descriptive words or word pictures in scales to analyse the likelihood of an event occurring and its consequences or outcomes. These are used to analyse risks in different contexts or situations by varying, adapting and adjusting them. Most business risk management scenarios use qualitative analysis, consisting of a descriptor along with an alphabetical grade identifying the level of likelihood. You may find your organisation uses similar but different words; for example, 'expected' instead of 'extremely likely'; 'probable' for 'likely'; and 'improbable' for 'unlikely'. Ratings may be numerical or alphabetical.

This table gives examples of some qualitative analysis ratings and descriptors used when assessing the likelihood of risks occurring.

A: Extremely likely (expected)
This rating and descriptor equates to: ▪ The incident will most probably occur under almost all circumstances. ▪ The risk has more than a 75 per cent chance of occurring. ▪ The risk will occur within the next six months. **Example:** A rival organisation within your industry also bids for lucrative supply contracts with the government.
B: Likely (probable)
This rating and descriptor equates to: ▪ The incident will probably occur under most circumstances. ▪ The risk has a 50 to 74 per cent chance of occurring. ▪ The risk will occur within 18 months. **Example:** Loss of staff.

C: Possible
This rating and descriptor equates to: ▪ The incident may occur under certain circumstances. ▪ The risk has a 25 to 49 per cent chance of occurring. ▪ The risk will occur within 36 months. **Example:** New commercial off-the-shelf software integrated into your organisation does not fully meet specifications or requirements and requires modification.
D: Unlikely (unexpected)
This rating and descriptor equates to: ▪ The incident will probably not occur. ▪ The risk has less than a 25 per cent chance of occurring. ▪ The risk may occur within 48 months. **Example:** A competitor employs risky predatory pricing tactics to drive your organisation out of the marketplace.
E: Rare
This rating and descriptor equates to: ▪ The incident is highly unlikely to occur or will only occur under the most exceptional circumstances. ▪ The risk is not likely to occur within the next five years. **Example:** A staff member dies on the job while complying with general safety procedures.

Semi-qualitative analysis

Semi-qualitative analysis is qualitative analysis with a numerical weighting index. However, the numerical value allocated for each qualitative scale is not related to the actual magnitude of likelihood or probability of consequence. It only provides an order of magnitude for analytical purposes. It does not provide real values, as would be the case in a quantitative analysis.

There is no standard weighting index: a weight is applied by the analyst. Semi-qualitative analysis is often seen in financial analysis in relation to market sentiment trends.

Example

Using semi-qualitative analysis

Semi-qualitative analysis can be presented in table form to link quantitative data to qualitative data. For example, the rating 1.0 is given for an extremely likely occurrence (equivalent to a qualitative A rating), decreasing through 0.75 (likely, a B rating), 0.50 (possible, a C rating), 0.25 (unlikely, a D rating) and 0.1 (rare, an E rating).

As these can be multiplied out (against likelihood) to achieve a final risk rating value, generally no risk is rated '0'. The appeal (and to some the problem) of this type of analysis is that the scale can provide for 'in between' ratings, such as 'fairly possible' (i.e. between possible and likely).

Rating	Descriptor	Equates to qualitative value
1.0	Extremely likely	A
0.75	Likely	B
0.50	Possible	C
0.25	Unlikely	D
0.1	Rare	E

Quantitative analysis

Quantitative analysis uses data from a variety of sources, such as statistical data, engineering reports, sales figures, financial records, or wherever figures or 'quantities' are used or employed. The quality of this type of analysis depends on the accuracy and reliability of the values used. Essentially, quantitative analysis is a subset of mathematical statistical analysis.

Statistical analysis does not provide a numerical value to express likelihood, but rather provides figures-based evidence of the likelihood.

Using information from an audit, here is an outline of how one manager assessed the likelihood of risks occurring:

- For every 50,000 units of a food product packaged at the site, 2,500 have been found to be incorrectly sealed.
- Incorrect seals lead to the potential risk of customers becoming unwell.
- Therefore, there is a 5 per cent risk of exposure to illness.
- Statistical analysis can thereafter determine how many people exposed to the unsealed product actually become ill.

Example

Assessing the likelihood of risks

The following is an example of a manager assessing the likelihood of risks.

'The first thing I do is look at what's happened before in our organisation to see the likelihood of it happening again. For example, we already have reliable data on staff absences and movement, technology breakdowns and work health and safety incidents.

'I then look to see what's happening in the organisation's business environment. For example, we're getting a new computer system that will be backed up by our old system. At the moment a breakdown is a possible risk. After we get the new system, the risk will be greatly decreased so we'll downgrade the likelihood to unlikely. Installing previously untried new software produces a possible chance of system conflicts. Conversely, introducing a new operating system or even a major upgrade to an existing system (for example, a new version of Windows) would be likely or extremely likely to cause some type of compatibility issue with existing aftermarket software applications.'

Practice Task 8

Use qualitative analysis to identify the risk rating for the following risks. Justify each answer with a short description of your assessment.

Question 1

Your home or workplace having a catastrophic fire (being totally destroyed or severely damaged)

Question 2

Your car being stolen

Question 3

Credit card fraud impacting your company (or self)

Question 4

Someone in your workplace being sick on the Monday after a football grand final

3B Assess the impact or consequences of risks

The next step is to understand and determine all possible outcomes should the risks you have identified occur.

By identifying what might happen, you can determine and put in place measures to reduce, offset or eliminate a risk. Select a risk that has been identified, then pose the question, 'What might happen if this risk occurs?'

Assessing the consequence of risks is similar to the way you assess risk: run brainstorming sessions, seek expert help and check existing records to see what happened in the past. Risk analyses are generally directed at the negative consequences of risks. However, risk management is also able to identify and prioritise opportunities.

Here are some negative and positive consequences that may arise from risks occurring:

- Key staff might be absent due to illness. Consequently, the timelines for the activity might increase and the activity may not be completed on time.
- Staff may not have sufficient knowledge or skills to complete their assigned tasks. Consequently, the activity might not meet quality assurance standards.
- A member of your team may have relevant expertise you are unaware of (a potentially positive risk). Consequently, the activity might be undertaken and completed to a higher level of competence than originally planned.

Using a consequence scale

Consequence scales are used as a guide in determining the ranking given to a consequence.

When using consequence scales, numerical grading is applied, along with a descriptive rating scale. Make sure you're familiar with the descriptors your organisation uses. Rating terms commonly used are 'disastrous', 'severe', 'extreme', 'minimal' and 'negligible'. When referring to financial consequences, values differ according to the size and nature of the organisation. For example, in a very small organisation 'minor costs' may be any damages up to $500, while for a larger organisation this may be $15,000. When dealing with risk, it is always advisable to opt for the worst possible outcome of a risk occurrence to allow for the most accurate coverage and treatment.

1. Insignificant	▪ Little benefit, low or no financial or material gain ▪ Risk consequences are dealt with by routine operations
2. Minor	▪ Financial impact is less than $10,000 and is not fully covered by insurance ▪ Single injury ▪ Low impact on client sensitivity ▪ Minimal damage to company's image and reputation ▪ Censure by regulators ▪ Minimal impact on business and strategic objectives ▪ Risk consequences are dealt with by routine operations
3. Moderate	▪ Financial impact is $20,000–$100,000 and is not fully covered by insurance ▪ Multiple injuries ▪ Moderate client sensitivity ▪ Medium damage to company's image and reputation ▪ Fines and penalties by regulators (e.g. delay in payment to client) ▪ Moderate impact on business and strategic objectives
4. Major	▪ Financial impact is $100,000–$500,000 and is not fully covered by insurance ▪ Single death and/or multiple significant injuries ▪ Significant client sensitivity ▪ Significant damage to company's image and reputation ▪ Restriction of business by regulators ▪ Significant impact on business and strategic objectives
5. Catastrophic	▪ Financial impact exceeds $500,000 and is not fully covered by insurance ▪ Multiple deaths ▪ Very high client sensitivity ▪ Irreparable damage to company's image and reputation ▪ Cessation of business due to non-compliance with regulations ▪ Business and strategic objectives unable to be achieved ▪ Significantly harms reputation; huge financial loss

Example

Assessing consequences

The perceived consequence of a risk event is a subjective matter. One person may perceive a lesser consequence from a particular course of action than another person. For example, a criminal mind may perceive the threat of a reprimand from a magistrate as a small consequence compared to the money that could be made – or satisfaction gained – from the criminal activity. A law-abiding citizen, on the other hand, may take into consideration the blight on their criminal record and their social standing.

How would you perceive an event like a client being injured by your product?

There is, firstly, the legal risk. Then there is the risk to the company's reputation (or public perception of the company), which may be seen as selling 'unsaleable' or dangerous goods. It may appear easy to say 'the consequence would be minor', but determining this in dollar terms can be difficult, particularly when you're not a marketing person. Would it be only a minor consequence if one of those who had developed a negative perception happened to be your largest corporate client? What effect would this have on the company in lost sales and goodwill? We have to seek advice from marketing experts, and even conduct surveys of customers and clients to determine exactly how they would react in such circumstances.

Practice Task 9

Reflect on the risk ratings you identified in Practice Task 8. For each question, complete a consequence assessment with the added information. Consider your answers from various angles, such as 'What if the information lost or not accessible isn't urgent or very critical?' before making your assessments.

Question 1

Your home or workplace has a catastrophic fire (being totally destroyed or severely damaged), destroying all your business software records.

Question 2

Your car is stolen with a confidential business plan on the back seat.

Question 3

Credit card fraud impacts your company (or self) and empties your bank account.

Question 4

Someone in your workplace is sick on the Monday after a football Grand Final, and that person is the only one at work with access to the client orders database.

3C Evaluate and prioritise risks for treatment

When evaluating and prioritising risks for treatment, you need to begin by understanding the level of risk.

To determine how severe a risk is, combine the results of the likelihood of an event occurring with the severity of the consequence. The most significant risks are the priorities for treatment – these can be ascertained by assigning a category such as high, medium and low risk.

Here are some descriptions of typical risk categories used in business.

Extreme	▪ Risks that have the potential to be devastating to the organisation or project ▪ Require immediate action
High	▪ Risks assessed as likely to occur and severely affect (either positively or negatively) specific aspects of the organisation, such as finance, property, personnel or governance ▪ Require immediate action
Medium	▪ Risks assessed as being probable and needing treatment ▪ Require monitoring and response procedures
Low	▪ Risks assessed as having a minimal likelihood of occurring and a low impact level if they do occur ▪ Treated with routine procedures

Determining the likelihood and level of impact

Analysis matrices provide a quick graphic presentation of the likelihood and level of impact of risk.

For this type of matrix, you need to understand the alphabetical and numerical ranking levels or system your organisation uses. The following matrix defines the different rankings given to risks and their impact. For example, if a risk has been identified as having a major impact on the organisation if it occurs and it has been identified as likely (probable) to occur, then this matrix identifies that if it does happen, a high level of risk would need to be managed at a senior level.

Level of impact	A (expected)	B (probable)	C (possible)	D (improbable)	E (rare)
Insignificant	Low	Low	Low	Low	Low
Minor	Medium	Medium	Medium	Low	Low
Moderate	High	Medium	Medium	Medium	Medium
Major	Very high	High	High	Medium	Medium

Example

Typical risk assessment matrix

Different organisations may use different risk assessment matrices; some may use similar but different words, have more or fewer categories, or ratings may be numerical or alphabetical. A typical risk assessment matrix is shown below.

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost certain	High	High	Very High	Very High	Very High
	Likely	Moderate	Moderate	High	Very High	Very High
	Possible	Low	Moderate	High	High	Very High
	Unlikely	Low	Low	Moderate	Moderate	High
	Rare	Low	Low	Low	Low	Moderate

Determining the frequency of exposure to risk

A third variable – frequency of exposure to risk – must also be considered.

The likelihood of a risk occurring is directly related to the frequency of the risk occurring. When you are evaluating the frequency of exposure to risks, there are questions you should ask yourself:

- How often do people encounter the risk?
- Has it ever happened before?
- How often has the risk occurred?
- Has the risk caused any near misses?

- Is there any level of training required to perform the activity to ensure exposure to the risk is minimised?
- Have people been adequately trained to lessen their exposure to the risk?
- Have people not been trained because the training is expensive or time consuming?

Using a grading system for exposure to risk

Grading systems are used to identify the frequency of exposure to risk.

Grading systems of possible risk exposure may use alphabetical gradings as easily identifiable markers to help when documenting the potential frequency of risk exposure. Some organisations use numerical rankings.

Here is an example of a grading system used to identify the frequency of risk exposure.

Very likely	Grade: A ▪ Ranking: Very likely (expected) – will occur regularly ▪ Example of risk: personnel become ill and are off the project for a day or so ▪ Potential frequency of exposure: every project or activity
Likely	Grade: B ▪ Ranking: Likely (probable) – will occur at some stage ▪ Example of risk: deadlines are exceeded ▪ Potential frequency of exposure: a number of activities
Possible	Grade: C ▪ Ranking: Possible – could occur ▪ Example of risk: staff are injured ▪ Potential frequency of exposure: a couple of times in a year
Unlikely	Grade: D ▪ Ranking: Unlikely (unexpected) – will probably not occur ▪ Example of risk: property is stolen ▪ Potential frequency of exposure: once in five years
Rare	Grade: E ▪ Ranking: Rare – may occur but in limited situations ▪ Example of risk: a human-made disaster ▪ Potential frequency of exposure: once in 10 years

Maintaining currency of assessments of exposure

It is important to ensure your assessment of exposure to risk is up to date.

Circumstances can change and your initial assessment of exposure to a risk must change accordingly. For example, identifying the frequency of accidents happening to members of a sales team in the past can help you determine how often accidents might happen in the future. However, a number of changes may have an impact on the sales team's frequency of exposure to accidents.

Situations in which exposure to accidents could change include:

- The organisation may employ more sales people in the future.
- The staff might spend more time telephoning clients instead of travelling.
- The team may widen its geographic base.
- Road conditions could worsen.
- The condition of company cars could deteriorate.

Prioritising risk

Once your overall risk/consequence rating has been determined, you need to prioritise the risks so you can address the most severe risks first.

Prioritising risk allows for the most resources to be applied to the greatest risks, giving you the widest range of options possible. As you work down your prioritised list, resources may become less freely available and optimal treatments may have to be substituted with affordable treatments. Combine all the analysis you have conducted so far: the risk, likelihood, level of impact and level of risk based on frequency of exposure. This gives you an idea of the level of risk you are facing (high, medium or low): a high level means immediate action.

Remember that using qualitative terms (such as 'likely' or 'expected') can be subjective so it's important you continue to consult with everyone involved to ensure the risks are viewed from a similar perspective and common understanding. For example, what one person sees as high risk, another person might see as low. Some risks may not be as high or low as originally thought after you have discussed them with others.

Once you have a list, you need to analyse it further. To prioritise, you need to use your judgment and management skills as you may need to distinguish between a risk that has a low probability of occurring but a high impact if it does, and one that has a high probability of occurring but a low impact if it does. The outcome from this is a list of risks with an agreed priorities rating. From this list, decisions can be made about acceptable levels of tolerance for particular risks and where greater effort to control the risks needs to be focused. To ensure that you prioritise well, you need to take into account:

- the controls already in place
- the cost consequences of managing risks or leaving them untreated (in terms of resources as well as health and safety)
- the benefits and opportunities presented by the risks
- the risks to be borne by stakeholders.

Example

Risk evaluation

This example shows the importance of using the analysis of your likelihood/ consequence rating to see what the level of risk is and whether an organisation should go ahead with an opportunity.

Risk	Likelihood	Impact	Level of risk
Team member is away for a short time	Very likely (Expected)	Insignificant	Low
Team member goes on extended leave	Likely (Probable)	Moderate	Medium
Team leader completes the campaign well within the timeline	Likely (Probable)	Major	High
Team member disagrees with a decision	Possible	Insignificant	Low
Team member performs poorly	Possible	Moderate	Medium
Team member disregards instructions	Possible	Moderate	Medium

Risk	Likelihood	Impact	Level of risk
Team leader resigns with minimal warning	Possible	Major	High
Team member becomes critically ill	Possible	Catastrophic	Very high
Team member causes major injury to other members	Rare (Improbable)	Catastrophic	High

Practice Task 10

Use the example scenarios from Practice Tasks 8 and 9 to prepare a likelihood/consequence matrix. In the table, rank each scenario as either low, medium, high or extreme and determine the possible outcomes.

Situation	Ranking	Possible outcome
Your home or workplace has a catastrophic fire (being totally destroyed or severely damaged), destroying all your business software records.		
Your car is stolen with a confidential business plan on the back seat.		
Credit card fraud impacts your company (or self) and empties your bank account.		
Someone in your workplace is absent on the Monday after a football grand final and that person is the only one at work with access to the client orders database.		

Summary

- Risk assessment and evaluation involves identifying the likelihood of a risk event occurring, then examining the possible outcomes (consequences) of the event's occurrence.
- Using a likelihood/impact matrix, you can generate an overall risk rating, which can be used to prioritise treatment processes.
- Make sure you are familiar with the systems and processes used by your organisation. Matrices, rating scales and terminology may differ among organisations.
- The highest priority risks are calculated by analysing your data and identifying the risks that have a 'high' rating for likelihood and consequences.

Learning Checkpoint 3
Analyse risks

Part A

1. Identify three strategies you should use to ensure you accurately identify rankings for risks?

2. Describe the following terms, using examples where appropriate:
   a) Likelihood of risk

   b) Qualitative analysis

   c) A consequence scale

   d) Frequency of exposure

3. Create a table assessing different risks. Include the following:
   - Apply a risk rating scale to the likelihood of the listed risks occurring (A–E; extremely likely to rare) using appropriate matrices.
   - Assign a consequence or level of impact value (1–5; insignificant to catastrophic) to each of the risks.
   - Assign an overall risk priority for treatment (e.g. high, medium, low).

Risk	Likelihood rating	Impact rating	Overall priority

Part B

Read the case study, then answer the questions that follow.

Case study

In analysing risk for an upcoming model range, risk management specialists at an American car manufacturing company were complacent about the American buyer. They knew that SUV-type trucks and pick-ups were big sellers, as were inefficient, fuel-guzzling V8 sedans and sports cars. The likelihood of sales lost to more fuel-efficient vehicles from another company (even though these had just been released to the market and were already making an impact) was assessed as very low, as were the consequences of these lost sales. The company appeared to ignore any possible financial difficulties despite the prevailing economic climate, which saw consumers thinking twice before spending large sums of money. Consequently, the company suffered massive losses as a result of badly misjudging the mood of the American consumer and the impact of a faltering nationwide economy.

1. List at least four risk management actions the company should have undertaken before going ahead with the new model.

Topic 4 | Select and implement treatments

4A Determine and select from options for treating risks

4B Develop a risk treatment action plan

4C Communicate, implement and monitor a risk treatment action plan

4D Evaluate the risk management process

4A Determine and select from options for treating risks

There are several methods available for treating risks.

If you determine that the level of risk is extremely high, you need to put strict measures in place to treat the risk. On the other hand, if the level of risk is negligible and you are alert to it, there is no need for action. Sometimes, you might find the expected benefits of a high-level risk outweigh possible negatives. Alternatively, the risks may be too great and you should abandon the idea altogether. Your goal is to eliminate or avoid the risk where possible, and to control the outcome should the risk materialise.

There are five options for controlling or managing risks.

Avoid	Can the risk be removed totally? For example, if the risks of moving into a new market at this time are too high or above management's tolerance for risk, can the organisation look for alternative markets to move into first? However, be aware of being too risk-aversive and making decisions to avoid risk regardless of a positive evaluation. A decision to avoid an activity can comfortably be made if the outcome is identified as high impact/high likelihood and low gain. Options to avoid risk include the following: ▪ not becoming involved in activities that lead to the possibility of the risk eventuating ▪ outsourcing risk-related tasks to contractors or specialist providers ▪ discontinuing operations that may realise the risk.
Likelihood	You can lower the likelihood of risks occurring by removing stimuli or situations likely to cause them. This may be as simple as providing better consultation or communication channels with local government to ensure planning permissions are achieved or delaying action until conditions become more favourable. Options for changing the likelihood include: ▪ removing or reducing activities that may lead to the risk being triggered ▪ reducing exposure to the risk environment ▪ ensuring risk management strategies are in place ▪ using inspection controls and quality assurance measures ▪ implementing tighter control of contract conditions ▪ ensuring timelines are realistic. For example, change the likelihood of technological breakdown by ensuring equipment is regularly serviced.

Consequences	By understanding the potential consequences of a particular course of action, you may be able to find opportunities to allow the organisation to proceed in a different direction to achieve its goals. A contingency plan is a valuable tool for helping reduce the impact or consequence of a risk event. It means you can react quickly and calmly to anything that threatens progress and ensure disruptions are limited. Contingency planning may include: ▪ establishing measures to control or minimise damage if the risk is realised, such as fraud control planning, public relations, disaster recovery planning, pricing controls ▪ developing administrative measures, controls, policy or procedures to provide guidance.
Share	If a risk is too great to take on alone, a partnerships or strategic alliance can allow the risk to be shared. International expansions by large companies are seldom successful unless they partner with local businesses to share risk and gain greater market understanding. Sharing the risk may also involve external investors, such as venture capitalists or insurers and underwriters, and may include joint ventures, partnering arrangements or underwriting investor participation. Insuring against an event occurring includes all forms of insurance such as liability, indemnity, life, workers' compensation cover, third party and hedging.
Retain	Not all risk is bad, and some 'bad' risk may be at an acceptable level where the likelihood and consequences can be adequately managed in the organisation. For example, if your company specialises in moving hazardous liquids and has extensive safety, environmental, personnel and hazard-handling procedures in place, you may choose to accept and retain this risk.

Considering the context

Considering the context of an activity is essential when allocating controls.

When determining what measures to apply to control risks or enhance opportunities, make sure you look at the activity as a whole and see how it fits into the organisation's strategic planning. The bigger picture may influence your decision about what measures to adopt. For example, it may be wise to pursue an activity despite its potential for a negative outcome – as long as you put plans in place to control the risks. The activity may be crucial to your organisation's continuing relationship with another organisation or it may be essential if your organisation is to expand into a new market or increase its profit.

Analysing the control measures

The control measure selected should be based on the resources you have, the time it takes to implement the measure and the cost involved.

You should also identify whether you need to do a cost–benefit analysis – it may be more cost-effective not to treat the risk. It is crucial that the risk treatment complies with legal requirements and organisational and government policies, especially those regarding access and equity, ethics and accountability. These criteria will influence your decision. Be flexible and keep in mind the alternatives available to you if your first choice proves unsustainable. Seek advice from colleagues who have experienced a similar situation. Use or adapt the following questions to approach decision-making in a systematic way.

- Is the treatment option feasible?
- What is the cost of implementing the control measure?
- Are there any benefits to be gained by not reducing the risk?
- What resources are needed to control the risk?
- Does the treatment mean more risks are identified or does it lead to additional benefits?
- Is the control measure sustainable or is it only a short-term fix?
- Are there any rare but severe risks that need to be treated regardless of cost?

Selecting risk treatments

The control measures you implement should treat the cause, not the result of the cause.

To ensure you're choosing the right control measures, you should revisit the risks you've identified and look closely at their causes. First look at all available options for each risk. Available options are influenced by:

- the priority of the risk
- the cost and other resources available
- the timeliness required in addressing the risk
- legal implications
- sustainability of controls
- stakeholder sentiment and preferences.

The importance of insurance

Organisations share the risks they have identified with a third party (insurance providers) to provide protection where unforeseen circumstances or events occur, such as a break-in, fire, staff accident, vehicle accident, project delays, cost overruns or litigation.

Types of insurance include liability, indemnity, life, workers' compensation cover, third party and hedging. Depending on your role and responsibilities and the nature and size of the organisation, you may have several responsibilities in regard to insurance. For example, you may need to seek advice from financial or insurance experts to ensure that insurance cover is adequate; insurance may have been appropriate at the time the risk strategy was developed but may now be inadequate.

Responsibilities involving insurance can include:

- being familiar with the types of insurance available
- identifying the type of insurance the organisation currently has and the reason for the insurance
- identifying the current insurance providers
- maintaining a database of preferred insurance providers
- inviting guest speakers, such as insurance brokers, to present to senior management on the benefits of insurance coverage
- keeping copies of insurance documents in the company's safe.

Example

Risk treatment measures

Here are some examples of risk treatment measures you could apply to specific circumstances.

Increased competition
Risk cannot be avoided and is not within the organisation's control. Minimise consequences by: ▪ clearly defining organisational strategy and performing it well ▪ continually researching competitor actions and assessing their impact ▪ developing contingency plans.

Declining demand for products or services

Help avoid risk by:

- continually monitoring sales performance
- conducting research into customer needs to ensure the products meet these needs to reduce the likelihood of declining demand
- continually researching alternative products to suit changing economic conditions or customer needs
- reviewing pricing models to attract increased demand.

Expenditure over budget

Risk cannot be avoided but can be reduced with control measures such as:

- regular financial analysis
- effective budget planning and reporting
- developing contingency plans
- carefully researching expected expenditure before developing budgets.

Inadequate IT system

Help avoid risk by:

- researching software requirements and developing a detailed brief before purchasing the system
- sharing the risk by engaging an expert to define requirements and select the system, including software, as part of an overall systems leasing package that allows regular updating.

High staff turnover

Risk cannot be avoided but measures to reduce turnover may include:

- conducting exit interviews and implementing staff retention programs
- interviewing existing staff to understand frustrations
- paying competitive rates and offering good conditions.

Litigation

To eliminate the risk of litigation:

- take out professional indemnity insurance (e.g. for lawyers and medical practitioners)
- outsource highly technical operations to experts (e.g. subcontracting work health and safety reviews)
- take out various forms of insurance (e.g. vehicle insurance)
- initiate joint ventures with technical experts (e.g. establishing a joint venture with a childcare organisation to provide a staff day care facility)
- take out workers' compensation cover.

Directing the treatment to the appropriate person

In addition to knowing the risk treatment options available, you need to know who to direct the treatment to.

The following table shows how a large retailer incorporated risk levels and management options.

Minor risk	Can be managed by administrative procedures or processes
Moderate risk	Will need specified management
Major risk	Requires attention by senior management
Catastrophic risk	Requires immediate action; detailed planning required at senior levels to prepare for and capture opportunity

Example

Applying risk treatments

Here is an example of a risk treatment process for controlling the risk of transportation delays.

Identified risk	Transportation delays in product delivery to customers
Consequence	Damage to company reputation and subsequent loss of business
Treatment options	You cannot totally avoid this risk but there are control measures that can be put in place.
Can we change the likelihood?	Yes – increase inventory holdings, employ or contract more delivery drivers, open more (smaller) local distribution centres
Can we change the consequences?	Probably not. Delays in delivery, particularly where they occur frequently, give the company the reputation of being an unreliable supplier
Can we share the risk?	Possibly. If you contract a courier company and include either performance incentives or non-delivery penalty clauses with 'delivery guarantees', you can offer customers similar guarantees or other incentives where delays materialise.
Can we retain the risk?	Probably not. Unless you have a dominant market position and can afford to lose some disgruntled customers, reputation is everything in business.

Practice Task 11

Question 1

Think of a situation where a business recognises they have an identified liability risk with one of its lines of products that may, in rare circumstances, cause injury to a user. Identify two risk treatments that could be applied to this situation.

4B Develop a risk treatment action plan

An action plan is a clearly articulated and documented plan that defines how the risk management process will be conducted.

The content of an action plan is dictated by organisational policy and the size and nature of the business. Some action plans are basic documents outlining actions to be taken, responsibilities and timelines, while others are more complex and cover a wide range of risk areas, multiple risks and control measures, and regular monitoring and review strategies. Of course, you cannot do this in isolation, and your action plan needs to be completed with input from your stakeholders and participants.

Your action plan should address the following questions for each identified risk.

What risk areas have been identified?
Categorise your plan into risk areas appropriate to your organisation such as personnel-centred, finance and market-centred.
What are the identified risks?
Define the risks in clear terms so they are easily understood.
What are the risk levels?
Define the likelihood, frequency of exposure and impact. List the risk prioritisation.
What actions are required?
Detail the treatment required, including resources and specialist personnel, and strategies for providing access to risk management processes and resources.
Who is taking responsibility?
Identify the person or group responsible for ensuring the actions are completed.
What are the timelines?
Following consultation, include a realistic and achievable timeline with milestones on the way to completion.
How will you monitor the processes?
Identify how and at what point you can determine progress and completion benchmarks to ensure compliance with the action plan.

Additional information to include in the action plan

In some cases, there may be other information that needs to be included in the action plan, such as:

- policy references
- participants in implementation
- documentation requirements
- resource allocations
- a communication plan.

Documenting the plan

To document the plan, use your organisation's risk treatment template or develop your own treatment plan to suit the nature of the activity.

You could use a spreadsheet format that allows you to record multiple risks, although a vertical format may be more suitable for a small-scale activity. You might use a separate sheet for each risk. Follow the plan carefully as you implement the treatment. While the plan is a valuable support tool, do not be afraid to change it if you discover a treatment is not working.

Example

Documenting a risk management plan

Here are two examples of risk management plans, showing how they can be formatted.

Risk	Risk level	Action	
Delay in project completion	Major	Ensure underwriting includes project completion insurance to cover cost overruns caused by delays	
Resources	**Responsible person**	**Review by**	**Review date**
Insurance cover	Finance manager	Project manager	12/08/16

The risks	Non-payment of accounts	
What can happen and how		
The consequences of an event happening	**Consequences**	Cashflow difficulties May need higher provision for doubtful debts Lower profits
	Likelihood	Possible Low $ value of bad debtors recorded to date
Adequacy of existing controls	Adequate – debt collection policy and process in place	
Consequence rating	3 (Moderate)	
Likelihood rating	P (Possible)	
Risk rating	M (Moderate)	
Action taken / future strategies **Date for review**	Ensuring clients adhere to stated payment terms or, if necessary, reviewing to improve existing payment schedules Restrict approval of client accounts Follow-up collections system in place Credit limits in place Non-payers are red flagged on system	

Storing documentation

Make sure all documentation associated with your risk management process is correct, and that it is saved and stored appropriately.

Documents may include risk audits and assessments, meeting minutes, and draft and final copies of the risk management action plan.

Associated documents that link with the risk management plan may include:

- document reviews and reports
- an asset register listing the organisation's current assets
- a blank template for a risk matrix

- the emergency evacuation plan
- a list of current work safety officers
- insurance policies
- training records
- contracts, agreements and memoranda of understanding (for example, alliance or partnership contracts and purchase agreements).

Documentation must be retained for a number of reasons. The most obvious reason is that a risk management action plan provides senior management with a plan that identifies and prioritises all risks the organisation is exposed to. Supporting material such as meeting minutes demonstrates that the risk management process has been conducted properly and in line with the scope.

Currency and accuracy

Check that all documentation associated with the risk management plan is current and accurate. You may be required to revisit these documents to check that training has been provided or in a court case to show how the organisation planned and carried out its risk treatment strategies.

Documents must be current and accurate to:

- communicate risk management activities with all stakeholders, participants and employees
- facilitate ongoing process monitoring and evaluation of the risk management strategy
- provide an accountability mechanism that supports the organisation's corporate plan
- provide an audit trail for the follow-up of key actions identified in the action plan.

Retaining or destroying documentation

There may also be a legal or legislative requirement to retain certain documents and records for a specified period or destroy documents for confidentiality reasons. Make sure you know the regulations and what documents are involved, especially the documents that your organisation needs to retain. Ask your manager if you are unsure.

Documents that may need to be retained include:

- risk assessments
- risk management plan
- insurance cover
- incident report forms
- litigation records
- alliances
- contracts and memoranda of understanding
- training records.

Storage options

Security of storage is crucial given you're likely to be dealing with commercially sensitive information. Make sure you're familiar with the procedures the organisation follows for document storage.

Electronic storage of documentation is the most common way to retain information. Make sure you understand the file paths and other storage implications, such as whether the folders must be password protected. For example, your organisation may allow access to current working documents only for specific people, whereas you might store general information on the intranet.

You may need to electronically scan and store written documents such as legal documents. If you receive written or printed documentation that you need to keep but cannot scan, you may need to consider other security options including lockable filing cabinets, safes or secure server storage. It is also advisable to retain valuable or important electronic documents backed up to off-site media; for example, an external server, removable/securable hard-disk drives or single-use media such as writeable DVDs or Blu-ray discs.

Example

Document management systems

Brett Michaels has recently been appointed managing director of a small delivery company. As part of his responsibilities, he has overseen the development of an updated risk management plan. Managers and staff have been informed and trained where necessary in relation to the storage of all risk management documents.

Here are the key elements of the document management system:

- The document management system includes a folder on the organisation's computer network titled Business Support. Inside this folder is a Risk Management folder. Inside this folder is a range of clearly named folders and files containing documents such as the company's asset register, the current risk management plan, past risk management plans, the emergency evacuation plan, a blank template for a risk audit, completed risk audits and risk assessments, a list of current and prior work safety officers, insurance coverage and a blank template for a risk matrix.
- Electronic copies are created as PDFs to ensure they can't be altered.
- Back-up copies are stored on an external server in the company's off-site location.
- A final copy of the current risk management plan is stored electronically in the Business Support folder as well as on the company intranet. A master copy is stored in the company's Publications Master Copies folder labelled Risk Management Plan.
- A hard copy of the risk management plan is available in the company's library.
- Electronic copies of risk management documents available only for senior staff are password protected.
- A copy of appropriate risk management documents for all staff (the risk management plan, risk audits and risk analyses) is made available on the company's intranet under Policies and Procedures.
- The version of all risk management documents is clearly indicated.
- Copies of the insurance documents are held in the company's safe.

Practice Task 12

Question 1

List three examples of document storage facilities (on/off site) that can be used in an organisation?

Question 2

Identify an example of a back-up and/or archive facility that can be used for risk documents.

Question 3

Provide three examples of procedures to follow for document storage?

4C Communicate and implement a risk treatment action plan

Implementation of the action plan requires significant communication skills.

Although your job is to manage the process, you may not be involved in the day-to-day implementation of the control measures. Participants must be briefed on their roles to ensure they understand their required duties and the part they play in the overall success or otherwise of the risk management strategy.

There are five key steps to follow when implementing a risk treatment action plan.

1	Develop a communications plan to provide relevant information to target audiences. This is particularly relevant to key personnel who are performing tasks associated with the action plan.
2	Promote the plan to raise awareness among all personnel in the organisation through various media. Open channels of feedback to allow concerns to be raised, providing ownership and inclusivity to all staff.
3	Motivate participants by keeping them aware of the progress of the risk management processes. Meet regularly with participants in the process to ensure they are motivated and on schedule. Reward success.
4	Monitor and evaluate the plan performance for achieving milestones and to provide insight into potential shortcomings.
5	Modify the plan if or when the need arises. If the risks change or as new risks emerge, allow the plan to be flexible enough to incorporate change effectively.

Choosing communication strategies

Your choice of communication strategies depends on your target audience.

Those responsible for managing the plan and ensuring it is accurate and comprehensive may need to meet regularly. Senior management may need specific meetings at which the draft action plan is presented, opportunities are provided for feedback where appropriate, and authorisation for the plan is given. General dissemination to staff may involve presentations to ensure they understand the plan and their role.

Here are some suggestions for communication strategies:

- Risk management committee or team: regular, direct progress meetings
- Senior management, financiers, shareholders, insurers: presentations; website; targeted briefings; corporate plans
- Staff: workshops; information sessions; staff information booklets; newsletters; flyers or posters; intranet articles and periodicals.

Example

Communicating the risk management plan

Here is an example of how an experienced manager communicated a risk management plan to workers.

'At all stages of the risk management process, we communicated our progress to staff so that by the time we wrote the risk treatment action plan, everyone understood the potential risks and had contributed to suggestions for treating the risks.

'When the risk treatment action plan was completed, we called a staff meeting and provided everyone with a copy of the proposed plan. Absent and deployed members were emailed a copy of the plan for comment.

'Feedback was accepted from meeting attendees, and some new ideas for risk treatments were provided to the management team.

'Follow-up meetings were held with both internal and external stakeholders to finalise the plan. Support material for the plan included notices that we displayed around the organisation and an article on our intranet, which aimed to assist with the implementation of the plan.'

Communicating and implementing the plan

No risk management strategy or plan is workable unless all stakeholders and participants are aware of what's required to implement it and make it work.

An important aspect of your role is to communicate information about the implementation of the plan and designated responsibilities because, in many cases, you will not personally be implementing all aspects of the plan.

Effective communication helps everyone feel they are part of the process. A communication plan outlines how you will let everyone know about the risk management plan and their roles and responsibilities. It should also describe how to obtain their commitment, identify additional risks and concerns throughout the implementation process, inform relevant personnel about changes to work practices and gather feedback. Each target audience requires a key message.

When implementing a plan, you need to address the following questions:

- What is risk management, and what is the organisation's strategy?
- How is it being implemented, and what is my role in its implementation?
- What benefits should I expect to see?
- How can I actively participate to ensure successful implementation?

Overcoming implementation difficulties

You may encounter a number of difficulties when implementing a risk management plan. Make sure you have contingency plans in place to eliminate or reduce the impact of the difficulties. For example, if staff have misunderstood their responsibilities, you will need to provide additional information at a meeting by way of a presentation or with handouts written in plain English or in a community language.

Here are some examples of solutions that could be employed to overcome implementation difficulties:

- Ensure there are sufficient financial resources available to execute the plan in case of expenses for recruiting additional staff, changes to budgets or higher-than-expected costs.
- Ensure that all staff understand the risk treatment processes by preparing a list of questions to ask and observing them to confirm their understanding.
- Ensure the action plan provides strategies for managing changes to organisational structure in case there are changes to key personnel (management changes, new stakeholders or staff changes).
- Ensure there is sufficient insurance cover in the case of unexpected events and emergencies.
- Provide a variety of risk options in case the desired one is not successful.

Practice Task 13

Question 1

Research different communication techniques by talking to experienced practitioners. Are there any other media or methods that could be used to communicate your risk management process to an audience? What are they?

Question 2

List some tips for communicating risk management processes.

4D Monitor and evaluate the risk management process

An evaluation allows you to learn lessons from the process: what worked well, what could have been done better, and what didn't work at all.

While regular monitoring is essential for ensuring control measures are being implemented effectively, a formal review process also needs to be implemented on a regular basis to determine the effectiveness of the risk management process itself. Most organisations review their risk management strategies annually so they can be sure their strategic plans meet the current environment but allow for ageing risks and future potential risks to be identified.

Monitoring the plan

Monitoring the action plan is an ongoing process that ensures you manage the control measures effectively.

You need to check that controls are reducing or managing the identified risks or, alternatively, increasing the identified opportunities. This is essential because risks by their very nature are not static – circumstances can change quickly and render the treatment you have chosen ineffective.

When monitoring a risk action plan, you may have to:

- revise an inappropriate option
- recognise other risks that can arise and need to be treated
- understand that risk treatment priorities might change.

Benefits of regular monitoring

Regular monitoring helps you determine whether the impact and likelihood have been reduced, the risk is occurring less often and the treatment is cost-effective.

Include all stakeholders, staff and other relevant personnel in your monitoring, as they are able to report their findings from a perspective that may be different from yours. Make sure you document any findings you make as you monitor the process. New treatments identified from monitoring results should be included in the action plan. An inflexible, stagnant action plan is unable to meet the changing needs of the organisation.

Monitoring methods

Monitoring to check on the success of control measures needs to be done on a regular basis.

You can monitor and check the success of control measures by using:

- self-assessments
- observation and physical inspections
- customer feedback
- audits and reassessment of risk
- reviews of policies, strategies and documentation.

Using established monitoring criteria

You might use a set of established criteria to provide a concrete measure of success against which you can judge the effectiveness of the treatments. In this way you can compare actual performance with the desired outcome. When establishing criteria around the development of risk treatments, it is essential that you understand how the success of risk controls will be measured.

Established criteria may include:

- cost
- reduction in impact
- reduction in likelihood
- reduction in occurrence.

Key monitoring questions

For a thorough, consistent monitoring process, you need to go back to your risk identification chart, your risk analysis, the risk register and the risk treatment plan. Key monitoring questions to ask yourself and others when regularly monitoring the risk management action plan include:

- Are the risk treatments effective in minimising the risks?
- Are the risk treatments cost-effective and time-efficient in minimising the risks?
- Do the performance outcomes address the key elements for risk treatment?
- Are the assumptions made about the organisation's environment, technology and resources still valid?
- Are the management and financial controls adequate?
- Do the risk treatments comply with legal requirements and government policies such as accountability, ethics, access and equity?
- How can improvements be made?

What is evaluation?

Evaluation is the systematic determination of value or performance against set criteria, benchmarks or standards.

Evaluation offers you the opportunity to review performance and constantly improve your organisation's overall approach to systems, processes and procedures.

There are three main approaches to evaluation: goals-based, process-based and outcomes-based. The ideal methodology is the one that best suits your needs and desired outcomes.

These three types of evaluation offer different perspectives and are designed for different purposes. Generally, where your goals are to reduce loss or reduce risk, you use the goals-based method, with the scope to also use elements from process- and outcomes-based evaluation.

Goals-based evaluation

Goals-based evaluation determines the extent to which a program meets pre-set goals or objectives. In a risk management process, these goals are defined in the preparation of the project or process scope.

Questions to ask when designing an evaluation include:

- How were the program goals and objectives derived?
- Was the process effective, and were the goals SMART?
- What is the status of the organisation's progress towards achieving the goals?
- Were the goals achieved according to the timelines specified in the program implementation or operations plan? If not, why?
- Did personnel have adequate resources (time allocation, money, equipment, facilities, training, etc.) to achieve the goals?
- How should priorities be changed to put more focus on achieving the goals?
- How should timelines be changed? Be careful about making these changes. Know why efforts are behind schedule before timelines are changed.
- Should any goals be changed? Should any goals be added or removed? Why? Understand why efforts are not achieving the goals before changing them.
- How should goals be set and defined in the future?

Process-based evaluation

Process-based evaluations provide an understanding of how a program works and how it produces results. Process-based evaluation can be applied to longstanding or ongoing programs or processes. It can address a number of questions relating to the subject program, project or process. The questions you develop depend on what you specifically want to know about the performance of the process.

Here are some key questions to ask yourself when designing process-based evaluation:

- On what basis do staff and/or stakeholders decide what is included in the program?
- What is required of staff/stakeholders in order to implement the risk management program?
- How are employees trained or informed about the program?
- What input is required of stakeholders?
- What are the general processes customers or clients go through with the product or program?
- What do stakeholders consider to be strengths of the program? What typical complaints do they have?
- What do participants and staff recommend to improve the risk management program/processes?
- On what basis do employees and/or stakeholders decide the risk management program/processes are no longer needed?

Outcomes-based evaluation

An outcomes-based evaluation allows you to see whether the program or process is achieving the outcome required by management or directors.

General steps for accomplishing an outcomes-based evaluation	
1	Identify the major outcomes of the program. Ask yourself, 'What processes are we carrying out now?' and then for each activity ask, 'Why are we doing that?' The answer to this 'Why?' question is usually an outcome.
2	Choose the outcomes you want to examine and prioritise. If time and resources are limited, pick the top two to four most important outcomes to examine first.
3	Specify observable measures, or indicators, for each outcome to help you evaluate whether you are achieving the required performance.
4	Specify a target level or goal of achievements; that is, how often the risk management program succeeded based on the criteria identified in Step 3.
5	Identify the information needed to show these indicators, such as statistical records of decreasing downtime or losses, increased productivity or higher profit.
6	Decide how information can be efficiently and realistically gathered; for example, program documentation, observation of program personnel and stakeholders in the program, questionnaires and interviews about clients' perceived benefits from the program, case studies of program failures and successes.
7	Analyse and report the findings.

How to conduct an evaluation

For a thorough evaluation you will need to collect good quality information.

The data-collection method you choose to use can depend on the purpose of your evaluation.

Here are six data-collection methods. They are not exclusive, and it is a good idea to use a combination of methods to ensure data validity and depth.

Questionnaires, surveys and checklists	**Purpose** Quickly and/or easily get lots of information from people in a non-threatening way **Advantages** ▪ Can be completed anonymously (allows for more candid responses) ▪ Inexpensive to administer ▪ Easy to compare and analyse ▪ Can gather large samples ▪ Can get answers to lots of questions at once **Disadvantages** ▪ Might not provide carefully considered feedback ▪ Wording can bias clients' responses ▪ Impersonal ▪ May need sampling expertise ▪ Doesn't get the full story (cannot capture emotion, peripheral events, etc.)
Interviews	**Purpose** Fully understand someone's impressions or experiences, or learn more about their answers to questionnaires **Advantages** ▪ Can get full range and depth of information ▪ Develops relationship with stakeholders and relevant parties ▪ Can be flexible to meet interviewees' needs **Disadvantages** ▪ Can take a great deal of time ▪ Can be hard to analyse and compare even similar answers ▪ Can be costly (due to time) ▪ Interviewer can bias responses with personal opinions or perspectives

Documentation reviews	**Purpose** Understanding how a program operates without interrupting the processes by reviewing finances, correspondence, outputs/outcomes, memos and minutes **Advantages** ▪ Get comprehensive current and historical information ▪ Doesn't interrupt process ▪ Information already exists ▪ Statistical data means few biases occur **Disadvantages** ▪ Often takes a lot of time ▪ Information may be incomplete ▪ Need to be clear about what you are looking for ▪ Not a flexible means to get data; data is restricted to what already exists
Observations	**Purpose** Gathers information about how processes work in a program **Advantages** ▪ Can view steps of a process as they are actually occurring ▪ Can adapt to events as they occur **Disadvantages** ▪ Can be difficult to interpret seen (and unseen) behaviours ▪ Can be complex to categorise observations ▪ Observers can unwittingly influence behaviours of program participants ▪ Can be expensive (time)
Focus groups	**Purpose** Explore a topic in depth through group discussion; for example, about reactions to an experience or suggestion, understanding common complaints, etc. **Advantages** ▪ Quickly and reliably get common impressions ▪ Can be an efficient way to get a wide range and depth of information in a short time ▪ Can convey key information about programs **Disadvantages** ▪ Can be hard to analyse responses ▪ Need a good facilitator for safety and closure ▪ May be difficult to schedule 6 to 8 people together

Case studies	**Purpose** Understand or depict experiences in a program and conduct comprehensive examination through cross-comparison of cases. **Advantages** ▪ Fully depicts experience in program input, process and results (outcomes) ▪ An effective way to portray processes to external stakeholders **Disadvantages** ▪ Usually quite time-consuming to collect, organise and describe ▪ Represents depth of information, rather than breadth

Timeliness

Generally, a timeline is established before conducting an evaluation.

It is not practical for an evaluation to be a drawn-out process, as findings of an evaluation should be integrated back into the process as a form of 'fine-tuning'. Maintaining an evaluation schedule can be difficult, particularly where respondents to questionnaires take too long to return them or don't complete them at all. The onus is on the evaluator to encourage timely returns and chase up slow respondents. To assist your planning, Gantt charts are a common timeline development tool that can be produced in any spreadsheet software. For more information on producing Gantt charts, an internet search can provide many examples as well as tips and hints for use.

Reporting

An evaluation report is a standard report format document that includes data results, draws conclusions on performance and makes recommendations.

As a minimum, an evaluation report should include the key items shown here.

Purpose	What was the purpose of the evaluation?
Target	What was being evaluated?
Process	What were the steps in the evaluation process?
Findings	What data was collected and what was found?
Interpretation	What do the findings mean? What issues are emerging?
Lessons learnt	What has been learnt from events as they unfolded?
Recommendations	What should happen now?

Example

The value of regular evaluation

During ongoing monitoring and evaluation of a recently implemented risk management process at a large, exchange-listed furniture manufacturer and retailer, it was found that a new risk had emerged since implementation of the plan. This was the unexpected entry into the local market of an interstate competitor that had previously indicated it had no intention of expanding. Announcement of the planned expansion caused investor uncertainty and a subsequent loss in share price, and the company's institutional investors were concerned.

Luckily for the company, its risk management implementation plan included sufficient allowances for such unforeseen risks to be adequately assessed and included in an update, acknowledging that such occurrences, no matter how unlikely, can still materialise. Sufficient resources were kept in reserve to allow the board of the company to develop and integrate new risk management processes into the existing action plan. Although there were some losses, the company retained a dominant market share in its operating areas and continues to return shareholder value.

Practice Task 14

Question 1

Obtain a copy of a risk treatment plan currently being used in your organisation, or one that you are familiar with. If you were monitoring the plan, what would you be checking for?

Question 2

Evaluation can be defined as a systematic assessment of worth or merit. Explain what you would be checking for using goals-based, process-based and outcomes-based evaluation methods.

Summary

- Select the appropriate risk treatment, considering priorities and your resources. You can choose to remove the risk, reduce the risk/consequence, share the risk or accept it.
- An action plan establishes the responsibilities and timelines for implementing risk treatment measures.
- Communicating the process via the most appropriate means to stakeholders and participants is essential. This might involve presentations, meetings, flyers, newsletters, information sessions or placing information on the intranet.
- During every step of the process you must maintain documentation for compliance, governance, accountability, auditing and to assist future risk managers.
- Implementing an action plan involves communication, making people feel enthusiastic about the task and monitoring the performance of the plan so that it can be modified when needed.
- Evaluation allows you to refine and improve on the risk management process by evaluating what worked well, what could have been done better and what didn't work at all.
- You can use different evaluation methods such as goals-based, process-based or outcomes-based techniques when performing an evaluation.

Learning Checkpoint 4

Select and implement treatments

Part A

1. Why is it necessary to select and apply appropriate risk treatments to identified risks?

2. Research what type/s of risk reduction or sharing strategies may be applied or are available if you are looking to address the risk of litigation from the actions or inactions of you or your staff.

3. Give three reasons why documentation associated with risk management must be accurate and stored appropriately.

4. List the information you would include in a risk management action plan and explain the purpose of this information.

5. Explain the role a manager plays in monitoring and evaluating their risk management action plan and storing the information.

6. Provide two reasons why you need to maintain communication with stakeholders and/or participants throughout the risk management process.

7. Describe two contingency plans you might have in place for difficulties that could arise when implementing a risk management plan.

Part B

Read the case study, then answer the questions that follow.

Case study

The company

PolyVeya Pty Ltd is a publicly listed Queensland-based plastic forming company that makes components for the automotive industry. It is well established in Coolangatta and has just finished upgrading to a new warehouse and forming machinery that will allow it to take on extra capacity. It has 250 staff.

The situation

The Board of PolyVeya Pty Ltd has approached several large boat builders with the intention of expanding into marine plastics, a relatively mature sector. The approaches are well received, with some reservations regarding the company's experience in the salty, high-UV marine environment. PolyVeya is well financed (underwritten) but is carrying some debt and has minimal cash reserves. There is a quality leadership team in place, but it has little experience with marine plastics.

The risks

The risk management team at PolyVeya Pty Ltd conducted a risk assessment and found several areas of risk that could affect its move into the new market. These include:

- Technology risk – assessing suitability of the new material for production
- Product risk – evaluating the appeal of the new product to the market
- Financial risk – evaluating what financial difficulties in production may emerge with minimal reserves and some debt from the upgrades
- Reputation risk – considering how the diversification may impact brand perception
- Commercial/market risk – evaluating potential product performance in a competitive market environment
- Management risk – evaluating the level of management capability and agility to adapt if the new product underperforms in the marine sector.

1. List five types of risk treatment options available to the business and explain how they may use these options to provide risk coverage for the identified risks.

2. List the types of risk for PolyVeya Pty Ltd and appropriate risk treatments for each risk. Provide a brief explanation justifying your decision on one of the treatments you have suggested for each of the risks.

Risk	Treatment measures	Justification

3. As you prepare a risk treatment action plan, what do you need to consider to ensure your plan is effective?

4. Prepare a draft risk treatment action plan for the CEO of PolyVeya Pty Ltd using this table.

Risk	Risk level	Action	Resources	Responsible person	Review by	Review date