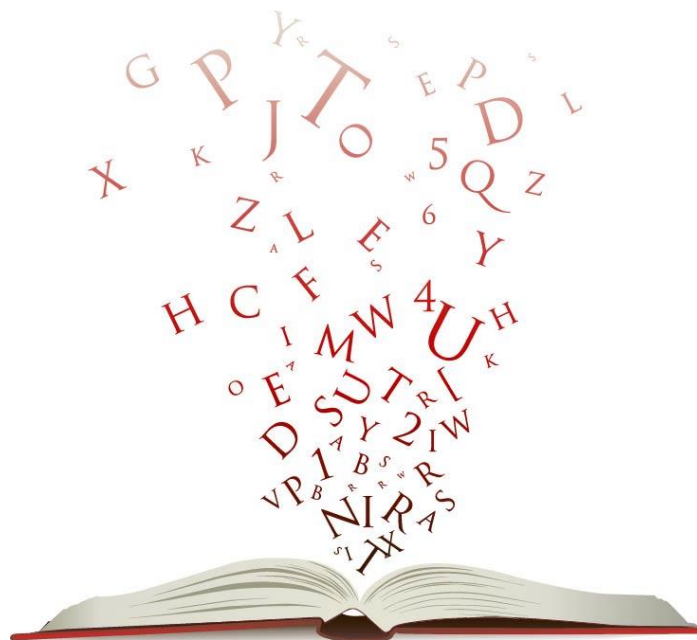




BSBRSK501 Manage risk

Learner guide



Copyright

© Raw Pixel 2015

This work is copyright. No part may be reproduced by any process without prior written permission from Raw Pixel. Requests and enquiries should be addressed to info@rawpixel.com.au

Contents

Unit of competency	3
Unit introduction	3
1. Establish risk context.....	4
1.1 Review organisational processes, procedures and requirements for risk management	4
1.2 Determine scope for risk management process	9
1.3 Identify internal and external stakeholders and their issues	9
1.4 Review political, economic, social, legal, technological and policy context	11
1.5 Review strengths and weaknesses of existing arrangements	14
1.6 Document critical success factors and objectives for area included in scope	17
1.7 Obtain support for risk management activities	18
1.8 Communicate with relevant parties and invite participation in the risk management process	20
2. Identify risks	21
2.1 Invite relevant parties to assist in the identification of risks	21
2.2 Research risks that may apply to scope	23
2.3 Use risk identification tools and techniques to generate a list of risks, in consultation with relevant parties	25
3. Analyse risks	27
3.1 Assess likelihood and consequence of risks occurring	28
3.2 Evaluate and prioritise risks for treatment	31
4. Select and implement treatments	32
4.1 Select appropriate risk treatments	32
4.2 Develop and communicate the risk treatment action plan	36
4.3 Check and store documentation	37
4.4 Implement and monitor the action plan	39
4.5 Evaluate risk management process	41

Unit of competency

The course content and assessments are designed to ensure that you have the skills and knowledge that are laid out in detail in what is known as a "unit of competency". A unit of competency covers a number of learning areas within a given subject and clearly defines what evidence, skills and knowledge are required for you to be assessed as fully competent.

You may complete one single unit of competency, or you may undertake a number of units of competencies that are part of a training package.

When you complete all the required units in a training package qualification and are assessed competent in all of them, you are entitled to a qualification for example: A Certificate II in Business.

Where you are assessed as competent in individual units you will receive a statement of attainment for the individual units, these may be used at a later date towards a full qualification.

The performance criteria for this unit of competency is set out below. You can use the details of this performance criteria to help guide you through what areas of knowledge and skill are covered in this unit and what evidence will be required from you to assess you as competent.

[The performance criteria for this unit of competency is set out in the attached document which is provided by training.gov.au](#)

Unit introduction

Risk is defined as *a situation, a problem or activity that could prevent a company, or project, from achieving its objectives.*

Risk management is central to effective business performance and is key to achieving positive results in customer satisfaction and profit.

The systematic management of risk refers to the resources, tools, principles and methods that help identify, assess, treat, monitor and review an organisations risks. In simple terms, it means the planned activities needed to effectively manage any genuine threat to the business and reduce its impacts on organisational objectives.

This unit of competency focuses on the skills and knowledge required to systematically establish the risk context, identify risks, analyse risks and select and implement risk treatments.

1. Establish risk context

Section 1 introduction

This section deals with reviewing organisational processes, procedures and requirements for risk management, determining scope for risk management process, and reviewing the PEST analysis model. It also provides information on conducting SWOT analysis, determining CSFs and objectives.

By the end of this section, you will be able to:

- Review organisational processes, procedures and requirements for undertaking risk management in accordance with current risk management standards
- Determine scope for risk management process
- Identify internal and external stakeholders and their issues
- Review political, economic, social, legal, technological and policy context
- Review strengths and weaknesses of existing arrangements
- Document critical success factors, goals or objectives for area included in scope
- Obtain support for risk management activities
- Communicate with relevant parties about the risk management process and invite participation

1.1 Review organisational processes, procedures and requirements for risk management

Introduction

The term 'risk' is described within Australian Standard/New Zealand Standard International Standards Organisation (AS/NZS ISO) 31000:2009 Risk management – Principles and guidelines, as being the *effect of uncertainty on (business) objectives*. This definition applies to all types of business threats, not just project risk.

A risk can also be any internal, external, tangible or intangible problem that may disrupt or enhance the flow of business.

An effect is any deviation from the expected or intended results which may be positive or negative. Uncertainty means the state, understanding or knowledge (including lack of) of an event, its consequence or likelihood.

Risk is influenced by potential events and consequences.

Two dimensions of risk

For many business managers, risk conjures up mostly negative connotations, such as delays, quality issues and budget blow outs.

Whilst risk can and does have negative impacts on a business' outcomes, if managed effectively, calculated risk can present positive impacts to an organisation.

Some of the positive aspects of risk can include:

- improvements to business processes
- opportunities to impact on project stakeholder satisfaction
- increased input and consultation from stakeholders
- improved planning processes
- elimination of processes causing waste and loss
- lessons and improvements are identified which can impact positively on future operations.

Systematic risk management

The systematic management of workplace risk is essential to all organisations, regardless of size, industry or scope of works.

Overview

Excellence in risk management performance does not just happen. Every business faces a range of threats that make it uncertain as to whether their goals will be achieved.

To effectively manage risk, you must understand your organisation's risks and systematically monitor their impacts as an ongoing practice.

A risk management system is defined as *the coordinated activities to direct and control the business in regards to its risk*.

Select the link below to watch a short video about the basics of risk management:

<https://www.youtube.com/watch?v=BLAEuVSAIVM>

Benefits of systematic risk management

The organisational benefits of implementing a systematic approach to risk management include:

- Increase the likelihood of achieving objectives.
- Encourage proactive management.
- Be aware of the need to identify and treat risk throughout the organisation.
- Improve the identification of opportunities and threats.
- Achieve compatible risk management practices between organisations and nations.
- Comply with relevant legal and regulatory requirements and international norms.
- Improve financial reporting.
- Improve governance.
- Improve stakeholder confidence and trust.
- Establish a reliable basis for decision making and planning.
- Improve controls.
- Effectively allocate and use resources for risk treatment.
- Improve operational effectiveness and efficiency.
- Enhance health and safety performance as well as environmental protection.
- Improve loss prevention and incident management.
- Minimise losses.
- Improve organisational learning.
- Improve organisational resilience.

Establish the risk context

Before designing a risk management process, you will need to define all of the parameters under which the organisation operates, that may give rise to different risks.

Overview

The **risk context** refers to the operating environment of the organisation.

By identifying the risk context, you will gain a better understanding of the environment under which your organisation operates and have a firm foundation for setting the scope and risk criteria for the risk management process.

The risk criteria means the *terms of reference against which the significance of risk is evaluated*.

Establishing the risk context

To understand the full details of the risk context, you will need to conduct research to define the following important details:

- the existing organisational processes, procedures and requirements for risk management
- best practice standards for risk management
- the scope for the risk management process
- internal and external stakeholders and their issues and needs
- political, economic, social, legal, technological and policy context
- review strengths and weaknesses of existing arrangements.

Review organisational risk management processes, procedures and requirements

The first step in understanding the **risk context** is to review the organisation's existing risk management system, including the processes, procedures and requirements and compare the existing set up against Australian and international risk management standards (AS/NZS ISO 31000).

For many organisations with established systems already in place, these details will be explicitly described in a risk management policy, formal risk management plan, process or procedure. Further details about risk requirements can also be located in the organisation's strategic plan.

For smaller, less structured organisations, risk management processes may be implied through verbal instructions, informal rules or form part of the standard management practices.

Details about your organisations risk management processes, procedures and requirements can be sourced from:

- company intranet/portal
- policy and procedure manual
- speaking with the business owner or operator
- speaking with senior business managers

Refer to the GSE Intranet > Policies & Procedure > Strategic & Operational Plans >

- Risk Management > '**Risk Management Policy and Procedure**'
- Risk Management > '**Risk Management Process**'
- General > '**Strategic Business Plan 2015-2018**'

Australian standards for risk management

AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines provides the benchmark standard for risk management systems within organisations. Its purpose is assist organisations in effectively identifying and treating their risks to improve business performance.

The details explained in this standard can apply to all organisations who are looking at improving their risk management processes to effectively identify, evaluate, control and manage risk in a systemic manner.

The three core elements

AS/NZS ISO 31000 establishes three core elements for managing organisational risk:

1. **Risk management principles:** The risk management process is underpinned by 11 principles that organisations can implement to manage their risk more effectively.
2. **A risk management framework:** A system of managing the risk managing process at a high level across the organisation.
3. **A risk management process:** A system for identifying, assessing and controlling internal and external risk.

Risk management principles

The Standard describes 11 underpinning principles that must be imbedded into a best practice risk management system. These principles are described as:

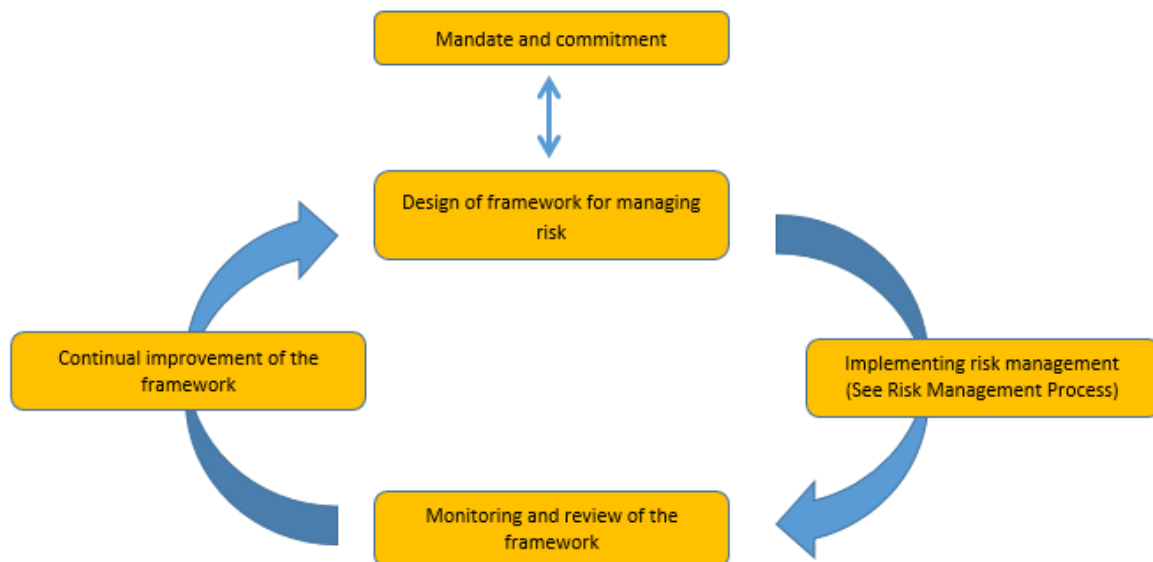
1. Risk management creates and protects value.

2. Risk management is an integral part of all organisational processes.
3. Risk management is part of decision making.
4. Risk management explicitly addresses uncertainty.
5. Risk management is systematic, structured and timely.
6. Risk management is based on the best available information.
7. Risk management is tailored.
8. Risk management takes human and cultural factors into account.
9. Risk management is transparent and inclusive.
10. Risk management is dynamic, iterative and responsive to change.
11. Risk management facilitates continual improvement of the organisation.

These 11 underpinning principles form part of the senior management's mandate and commitment to managing risk, which is at the top of hierarchy in the risk management framework.

Risk management framework

The overall structure of the risk management system as described in AS/NZS ISO 31000 can be described in the following diagram:



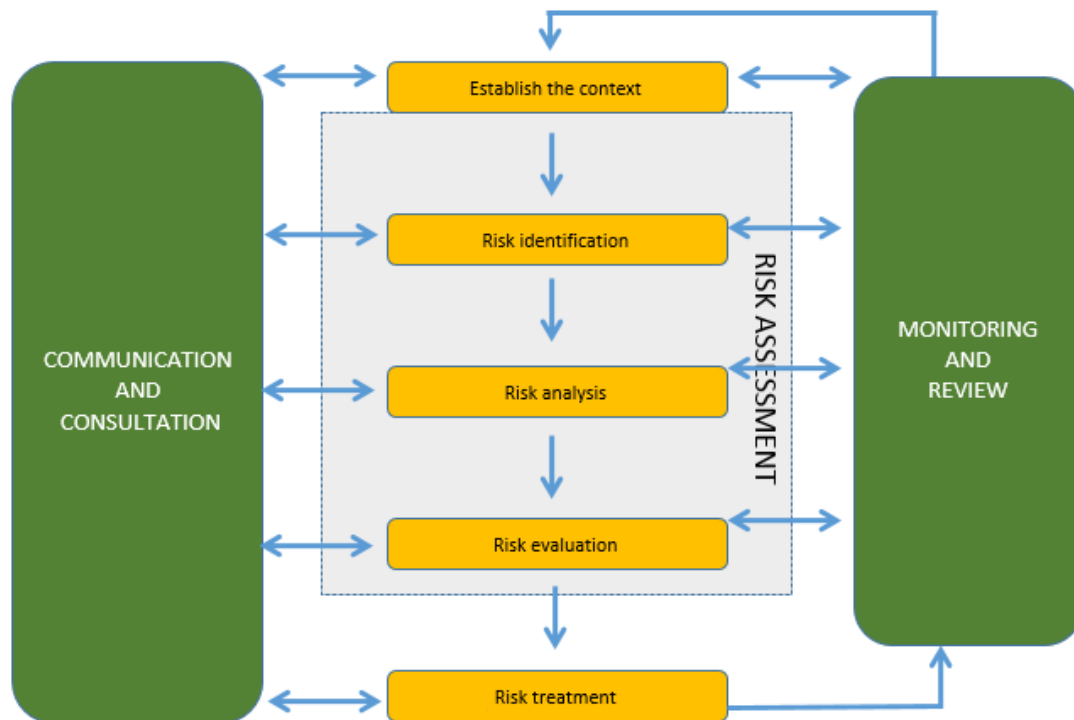
The framework explains the overall design, implementation, monitoring, review and continuous improvement requirements that are needed in an effective risk management system. It ensures that information about risk is reported and used in decision making processes.

The structure begins with the commitment of senior management who are responsible for resources, organisational direction and culture.

Risk management process

The risk management process is an iterative process comprising of seven main elements, as identified in the AS/NZS ISO 31000:2009 standard.

It consists of the following steps:



1. **Establish the context:** Establish the strategic, organisational and risk management context in which the rest of the process will take place. The context forms the foundation for setting the scope and risk criteria against which risk will be evaluated. The context refers to the internal and external operating environment of the organisation.
2. **Identify risks:** Identify what, why and how things can arise as the basis for further analysis.
3. **Analyse risks:** Determine the existing controls and analyse risks in terms of consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood may be combined to produce an estimated level of risk.
4. **Evaluate risks:** Compare estimated levels of risk against the pre-established criteria. This enables risks to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.
5. **Treat risks:** Accept and monitor low priority risks. For other risks, develop and implement a specific management plan, which includes consideration of specific policies and procedures covering such issues as avoidance/reduction/transfer of risk, insurance cover, business continuity and disaster recovery planning.
6. **Monitor and review:** Monitor and review the performance of the risk management system and changes, which might affect it.
7. **Communicate and consult:** Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process to address issues related to the risk and the process to manage it.

1.2 Determine scope for risk management process

Introduction

The risk management scope refers to *the basic parameters within which risks must be defined and managed*. The scope of the risk management process must be clearly defined early on in the risk management process, to allow for the risk criteria to be identified and addressed in later activities.

The risk criteria refer to *the benchmarks against which the significance of risk is measured in the risk assessment phase*.

Risk management scope

Risk management scope has certain elements and to determine them a few activities must be performed.

Elements of the risk scope

The risk management scope includes:

- the goals and objectives of the risks management process
- identification and responsibilities of key stakeholders
- defining frequency of the risk assessment activities
- identifying basic assumptions
- defining the inclusions and exclusions within the risk context (internal and external).

Determine the risk management scope

To determine the full extent of the scope for a risk management process, you will need to complete the following activities:

- Review the existing risk management system, including the risk management policy, procedures, processes and business requirements.
- Research and review the current risk context, threats, controls and contingency plans.
- Consult with key stakeholders such as the business owner, senior managers and risk specialists to determine the risk scope.
- Review organisational plans and strategies.
- Research the risk management systems of similar businesses in your region and industry.

1.3 Identify internal and external stakeholders and their issues

Introduction

A stakeholder is *any person who has an influence on, or is influenced by the strategic planning process*. A stake refers to *a degree of influence on the company, or someone that is impacted by the operations*.

Stakeholders have different levels of influence and interest with regards to risk and will require different levels of engagement.

They often include company directors, business owners, department managers, General Manager of Chief Executive Officer, as well as government representatives, suppliers and clients.

Internal and external stakeholders

Stakeholders needs and issues can have direct and indirect impacts on business plans and goals. The stakeholders that you focus on as part of the development of your risk management process should

include those who have a large degree of influence over the strategic planning process, or have a vested interest in the outcomes of business plans, including products and services offered to the market. These stakeholders should include internal or external stakeholders.

Internal stakeholders

The internal stakeholders include:

- company directors
- President
- franchisee/franchisor
- business owner/s
- General Manager
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- department managers such as the marketing or sales manager
- store manager.

External stakeholders

The external stakeholders include:

- clients
- major shareholders
- government representatives
- business networks and associates
- technical advisors
- consultants.

Define stakeholders and their needs

There are several techniques you can use to determine who your key stakeholders are, their issues, and what they need from you. These techniques include:

- Establishing a consultation process of two-way interaction and communication, sharing information and seeking input from the stakeholder.
- Seeking expert input from groups or individuals with specialised knowledge and training in risk management, stakeholder identification and business relations.
- Reviewing the organisational structure.
- Reviewing human resource management plans.
- Reviewing position descriptions.
- Conducting a stakeholder analysis.

Stakeholder analysis

A popular tool used to identify your key stakeholders in the strategy review process is called a stakeholder analysis.

The purpose of a stakeholder analysis

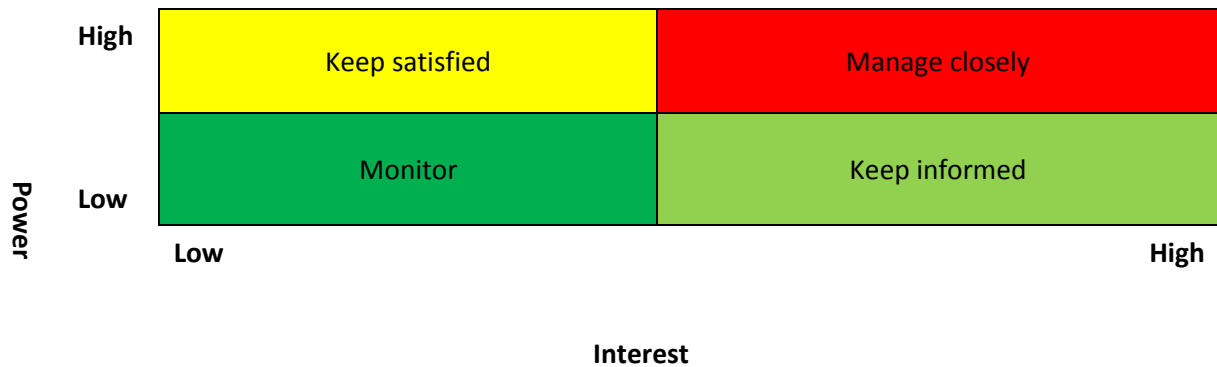
It is generally used in business to identify:

- the stakeholders level of influence and control within the business
- the level of benefit the stakeholder will gain from strategic changes and business plans
- the potential costs including time and money, of maintaining relationships with the stakeholder.

As a result of conducting a stakeholder analysis, you will be able to target your risk management plans in the right areas.

Conducting a stakeholder analysis

To conduct a stakeholder analysis, simply draw up a four quadrant table such as the illustration below. On a separate document, write down all of the stakeholders that have a direct impact on the plans and outcomes of your organisation. Write each stakeholder's name in the appropriate quadrant according to the level of power and interest.



1.4 Review political, economic, social, legal, technological and policy context

Introduction

The phrase 'organisational environment' simply refers to the factors that impact on the organisation's ability to achieve its strategies and goals. An organisation's environment can be internal or external.

To begin with, a thorough analysis of the external environment is required to understand the quantity, nature and impact of risks and opportunities relevant to the business.

External risk context

The outside influences that you must analyse as part of developing your risk management process include the following:

- the current political climate and potential changes
- government policy, agendas and upcoming initiatives
- current and proposed legislation, and how it can affect your company
- the state of the economy
- how trends, fads and other changes in society can negatively affect your company
- new technologies being introduced into the marketplace
- new applications for existing technologies that can invalidate existing products.

PEST analysis

Changes in your organisation's external environment can bring forth serious risks as well as great opportunities. PEST is an acronym that describes the four key elements of the external or 'macro-environment' that impacts on an organisation. PEST stands for the political, economic, sociocultural and technological forces that are outside of the control of the business.

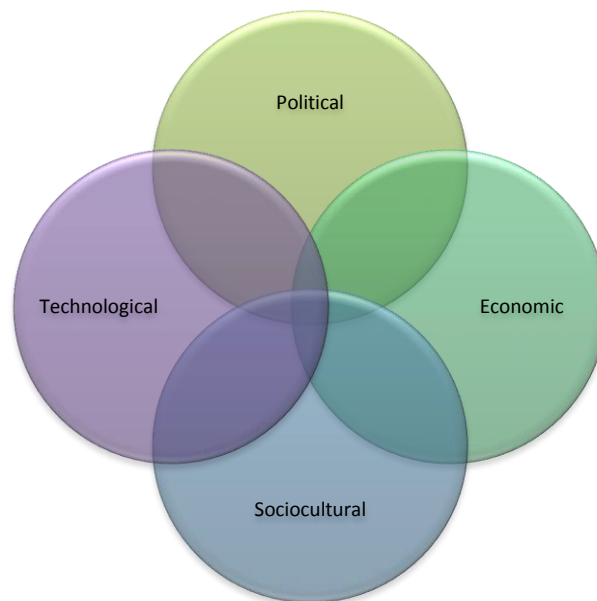
Select the link below to watch a short video about conducting a PEST analysis:

<https://www.youtube.com/watch?v=eGLFVjs1Zak>

The PEST model

The PEST model assists managers in scanning the national and international external environment and identifying the threats and areas to which the business can move into. The degree of each of these forces on the organisation's current and future position vary depending on the position in the market, industry, nature of operations, size and structure and customer target market.

The PEST model shows that each of the four external forces overlap and are interrelated. This means that issues and developments in one element will have some degree of impact on another.



Political forces

Organisations must identify and evaluate the political and regulatory environment under which it operates. Management must evaluate the political forces such as government regulations and legal issues.

These include:

- political stability
- new and upcoming government policies, including state and commonwealth
- regulatory authorities
- industrial relations and work health and safety law
- environmental protection laws and regulations
- taxation laws
- consumer laws
- intellectual property and copyright law
- trade laws
- import and export law
- relevant industry codes of practice.

Economic forces

As part of the strategic planning and risk identification process, you will need to consider the economic factors affecting the buying power and motivations of your target market.

These forces include:

- value of the Australian dollar and associated exchange rates
- value of international currencies

- international and Australian stock exchange performance
- interest rates
- Consumer Price Index (CPI)
- government interventions with the market and industry
- unemployment rates
- health and long-term prospects of the economy
- infrastructure
- domestic and international market trends
- market and trade cycles
- seasonality
- skills levels of the workforce.

Socio cultural forces

The third element in the PEST analysis model is to consider the socio cultural forces such as the demographic, cultural and social issues in the external environment. These are the key issues that impact on customer needs, preferences and priorities within a market segment.

For example:

- population growth rate
- lifestyle trends
- consumer behaviours and buying patterns
- age distribution
- attitudes toward domestic and foreign products and services
- community health
- religion
- language and ethnicity
- immigration
- attitudes towards work health and safety and the environment.

Technological forces

The fourth factor that influences the external market is that of technological advances. These can relate to:

- technological inefficiencies
- communication systems
- information management systems
- product obsolescence and maturity
- development and impact of new technologies released to the market
- research and development activity
- rate of technological change
- production and manufacturing schedules
- innovative approaches to quality and cost-efficiency.

Using the PEST analysis model

Although the initial task of scanning and assessing your external environment is time-consuming, there are eight basic steps to conducting a PEST analysis:

1. Form a focus group to discuss and analyse the external environment, led by a facilitator.
2. Gather your information and data based on all research undertaken.
3. Brainstorm the political trends and forces pertinent to your organisation.

4. Identify and discuss the opportunities that your organisation can take hold of.
5. Identify and discuss the threats that you need to take notice of.
6. Identify and discuss actions to exploit the opportunities and mitigate the risks.
7. Document the process using a chart or business report format.
8. Repeat steps 3-7 for economic, socio cultural and technology factors.

To view an example of a PEST analysis, refer to the GSE Intranet > Policies & Procedures > Strategic and Operational Plans > Risk Management > 'PEST analysis template'

Assessing the impacts

After assessing the political, economic, socio-cultural and technology impacts on your business within your brainstorming session, you will come to a conclusion as to what risks and consequences are likely to occur for your business.

Impacts from the PEST analysis will be classed as either:

- **positive impacts** – grow customer base, enhance product positioning, expand into a new territory, increase profits
- **negative impacts** – loss of customers, market share, revenue/profit, customer confidence
- **no impact** – the forces and trends will have no direct impact on your business.

1.5 Review strengths and weaknesses of existing arrangements

Introduction

SWOT is a popular analysis tool used in the risk management planning process. SWOT stands for **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats. The main difference between SWOT and PEST, is that SWOT focuses on both the internal and external environment (micro and macro) and looks at the strengths, weaknesses, advantages and disadvantages of each.

The PEST factors within the macro-environment, can be used in identifying and analysing the opportunities and threats in a SWOT analysis.

The macro and micro environment

There are two kinds of environment; macro and micro environment.

The micro-environment

The micro-environment is forces that are generally within the control of the organisation. These elements include:

- **capabilities** – what the organisation is equipped to achieve and offer its clients
- **systems** – internal systems and processes for quality, production, service and communication
- **workforce** – the skills, knowledge, experience and attitudes of staff, as well as the hours of operation, size and capabilities of the workforce as a whole
- **products and services** – the range and quality of product and service offerings, brand power and degree of demand from consumers
- **finance and resources** – the budget allocated to developing and maintaining the business and existing resource capabilities
- **suppliers** – providers of goods, their services, prices, quality and reliability of delivery

- **the marketing intermediaries**– relationships with wholesalers, other retailers and providers of trade channel services.

The macro-environment

The macro environment includes the external forces which are outside of the organisation's control. These include:

- **political and legal forces** – monetary and fiscal policies, social legislation, government policies for certain industries and legislation affecting market practices
- **demography** – the ageing population, growth in one and two person households, immigration, regional population shifts and the increasing divide between classes
- **competition** – the type of influences within the market, market structure, number of key players and intensity of the competition
- **social and cultural forces** – changes in social behaviour, cultural developments, desires, values and attitudes
- **economic conditions** – factors such as inflation, interest rates, unemployment, living expenses, exchange rates and economic restructuring
- **technology** – the acceleration of technology, the information and internet age.

SWOT Description

SWOT analysis, helps identify the strengths and weaknesses, and opportunities and threats.

Strengths and weaknesses

The strengths and weaknesses refer to the internal or micro-environment; the things that your business has most control over.

You need to consider what is going to plan and what is falling short of organisational and strategic objectives. Use consultation and internal research techniques as your basis to find this information. Once the analysis is complete, you will need to draw out the strengths and weaknesses based on internal conditions and list them in a table.

Opportunities and threats

The opportunities and threats relate to what's happening within the external or macro-environment – the things that your business has little control over.

Using consultation, market research, market intelligence and competitor analysis you will be able to identify where you are positioned in comparison to your competitors. You will need to document these outcomes according the opportunities and threats that are present in the external environment.

Conducting a SWOT analysis

Once you have defined the micro and macro environment and the associated strengths, weaknesses, threats and opportunities, you should have four separate lists.

It is common practice to display your information in a SWOT matrix with one quadrant allocated to each outcome. This will help you to get a high level picture of how your business is currently performing and what risks and issues you need to address. You can then understand the key opportunities and issues that are most important to your organisation; and work out what can be dealt with later.

Steps to conduct SWOT analysis

There are six key steps to conducting a SWOT analysis:

1. Form a focus group to conduct the SWOT analysis, led by a facilitator.

2. Gather your information and data based on all research undertaken or the internal and external environment.
3. Identify and discuss the strengths and weaknesses within your business, based on the micro environment, or internal conditions.
4. Identify and discuss your threats and opportunities within the market, based on the macro environment, or external conditions.
5. Decide upon targeted actions to build upon your strengths and address your weaknesses, consider your opportunities and guard against your threats.
6. Document your outcomes using a table or business report format.

To view an example of a SWOT analysis, refer to the GSE Intranet > Policies & Procedures > Strategic and Operational Plans > Risk management > **'SWOT Analysis Template'**

SWOT matrix

The following table shows a SWOT matrix with a range of examples for each quadrant:

Internal environment	
Strengths	Weaknesses
The strengths are: • quality product range • intellectual property ownership • unique brand awareness • operational capacity • bundled products and services • industry knowledge and experience • unique services • accreditations • strong existing customer base • renowned customer service performance • quality assurance accreditation.	The weaknesses are: • lack of skills within the workforce • poor leadership • operational limits • high customer attrition rates • small marketing budget • poor brand awareness • lack of competitive strength on price • inadequate resources • low quality of some products • lack of marketing expertise • limited money to spend on maintaining brand awareness • multiple authorisation structures to overcome.
External environment	
Opportunities	Threats
The opportunities are: • customer requests and needs • new research and knowledge • unique product offerings • social media – online presence • new opportunities in niche markets • specific niche of product suite • strategic alliances and mergers • international markets • possibility of new partnerships • global marketing.	The threats are: • emerging competition • unstable economy • international political unrest • falling value of the Australian dollar • opening of a new strong competitor • price wars • new technologies • increase in taxations • loss of vital customers • import/export laws • changing laws • government funding decreasing • natural disasters.

Select the following link to watch a short video presentation about the SWOT analysis model:
<https://www.youtube.com/watch?v=4aFB9xrkdIU>

1.6 Document critical success factors and objectives for area included in scope

Introduction

Critical success factors (CSFs) are the essential elements of activity and key results areas that must be performed well if your business is to achieve its objectives and remain competitive.

Objectives are the goals and outcomes that an organisation aims to achieve.

The process of defining CSFs and objectives is useful in risk management in terms of identifying the most important factors that organisations must achieve to be successful. CSFs and objectives can apply to a project, team, department or whole of business.

Critical success factors versus objectives

CSFs are the key results areas, conditions or variables that have a large impact on the organisation achieving its objectives. They are the factors that have the greatest impact on the organisation's overall performance.

The objectives are the goal posts – what the organisation aims to achieve. They are often stated in detailed measurable terms, such as key performance indicators (KPI).

Overview of CSF and objectives

Every organisation must perform the activities associated with critical success factors at the highest possible level in order to achieve their intended objectives and achieve their goals. This means implementing a process of managing and controlling the risks that may impact on their achievement.

Critical success factor	Objective
Maintain excellent relations with existing customers.	Achieve 75% customer retention rate.
Attract and retain new customers.	Secure 500 new customer sign-ups per year.
Maintain a competitive edge in local market.	Reach 25% market share in the local region.
Preserve ongoing financial stability.	Achieve net profit after tax of \$500,000 per year.

Importance of defining critical success factors and objectives

Based on the outcomes of your PEST and SWOT analysis, you will have discovered a range of risk sources in the internal and external operating environment of your organisation. The purpose of defining CSFs and objectives is to:

- Determine key areas of focus for risk management activities.
- Identify what needs to be protected to ensure business success.
- Establish priorities for risk controls.
- Focus resources in the areas that matter the most.

Identify CSFs and objectives

In addition to defining your organisational or department CSFs, you will need to establish or identify your business objectives. Like CSFs, the achievement of objectives are critical to the success of an organisation, department, team or project.

Objectives generally have a long-term focus (such as a minimum of 12 months), have customer and stakeholder implications and have a strong relationship with profit, market share, health and safety and financial stability.

CSFs and objectives are usually documented in strategic, organisational and operational plans.

Refer to the GSE Intranet > Policies & Procedures > Strategic & Operational Plans > General > 'Strategic business plan 2015-2018'

Critical success factors

The concept of "success factors" was developed by D. Ronald Daniel of McKinsey & Company in 1961. The process was refined into critical success factors by John F. Rockart between 1979 and 1981 (www.mindtools.com).

Types of CSFs

Rockart provided guidelines that cover four main types of CSFs. They can be used for reference when developing your CSFs as part of your risk management process:

1. **Industry:** The things that the organisation must do to remain competitive.
2. **Environmental:** These factors result from macro-environmental influences on an organisation. For example, business climate, economy, competitors and technological advancements.
3. **Strategic:** Factors resulting from the specific competitive strategy chosen by the organisation, that is, how the company decides to position itself.
4. **Temporal:** The factors resulting from the company's internal forces. For example, specific barriers, directions, challenges, etc. will determine the CSFs.

The CSFs must then be properly documented, either electronically or on hard copy, to act as reference throughout the risk management process.

Define your CSFs

The following process outlines the steps needed to identify the CSFs for your business, team, department or project:

- **Step one:** Establish/identify your mission and strategic goals.
- **Step two:** For each strategic goal, ask yourself "what area of business or project activity is essential to achieve this goal?" The answers to the question are your potential CSFs.
- **Step Three:** Evaluate the list of potential CSFs to find the absolute essential elements for achieving success - these are your CSFs.
- **Step four:** As you identify and evaluate potential CSFs, you may uncover some new strategic objectives or more detailed objectives. So you may need to define your mission, objectives and CSFs iteratively.
- **Step five:** Document your CSFs as part of the risk scope.

1.7 Obtain support for risk management activities

Introduction

Once you have defined the risk context, you must undertake the formal approval process, before you can move to the next step in the process of identifying risks. Senior managers must be aware of risk management plans and activities that impact on the operations of the business. They need to know the purpose and rationale for the process and how it will benefit the organisation.

Communicating the details of your risk management activities will ultimately influence their level of support and involvement in future risk management processes.

Seeking approval

As part of the planning and development process, you will need to gain the support and approval of senior management in order to secure approval to implement the risk management process. The plans and processes that you develop must accurately reflect the critical success factors, objectives and requirements of the organisation and its stakeholders.

The company directors and owners set the vision and provide the necessary resources from which the strategies flow. The strategic plan is the high level document that provides direction for the organisation over the next 3-5 years. Therefore, you will need to consult with the people who developed the plan to ensure your risk management activities are aligned.

Approval may be sought through a verbal confirmation, or writing by having your draft risk management plan signed by a senior manager.

Identifying your senior management

The senior management team will vary for every workplace based on the size and structure of the business.

For many business, senior management will include the following personnel:

- business owners/employer
- company directors
- HR Manager
- operations manager
- department managers
- general manager
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)

Your senior management team will be described in your organisational or hierarchical chart located on your company intranet, server or notice board.

Refer to the GSE Intranet > People and Departments > Organisational chart

Gaining support for risk management activities

There are four key points when you are attempting to gain support for your risk management activities.

1. Obtaining the appropriate executive approval and support

Identify or seek out an official sponsor for the project/risk management task. This person must be able to get things done across all departments and get people to cooperate. The sponsor must also understand the importance of the project and be enthusiastic about it. In case of trouble, the person must also step in.

2. Use only objective measurements

Quantitative measurements are advised over qualitative ones. This is because the latter is harder to prove and backup.

3. Develop concrete measures throughout the process

This is guaranteed success which will give your team and stakeholders a feeling of reassurance and encouragement. Moreover, as objectives are systematically met, progress and success become visibly measured.

4. Communicate broadly and keep all personnel informed

Keep all stakeholders informed, encourage feedback and develop 'ownership' throughout the length of the project.

1.8 Communicate with relevant parties and invite participation in the risk management process

Introduction

It is important to involve management and other key stakeholders at each stage of the risk management process.

This will allow you to gain valuable advice and feedback on organisational objectives and ensure the strategic and operational objectives are supported through your initiatives.

Involving senior management

In some cases, you will be asked to further refine or adjust the details of the risk management process or plan according to senior management's directions.

The information you present will be referred to often throughout the next step of the risk management process – therefore the information needs to be clear and accurately represent the current and future needs and risks of the business.

Communication

Communication is fundamental to organisational life.

Communicating with senior management

You should never assume that your managers know what you have planned or developed. You have a responsibility to communicate with your senior management team whenever you are conducting any tasks that impact the operations and strategies of the business.

One of the greatest skill requirements for an effective manager is communication. Effective communication means the aim of your message is successfully sent and received. It requires consistency, clarity and intention through verbal and non-verbal means. Communication is not only the spoken word; it also includes the actions and behaviours that complete the entire message.

Effective communication is not a one-way, one-off transmission of information. Rather it is a process by which two or more people interact. Without communication we would have no interaction and no organisation, only distinct groups of people.

Communication methods

A communication method must be carefully chosen to ensure the information is provided to the right people in a reasonable time-frame.

Details of the recruitment, selection and induction policy and procedure can be communicated using:

- team briefings
- holding short one-to-one meetings
- distributing a copy of the documents for discussion and review via email
- hosting a Skype or other teleconference call
- training sessions
- memorandum
- posters
- standard operating procedures
- inclusion in newsletters
- e-mail

- the organisation's intranet.

Invite participation

To ensure you fully explore the context for the risk management process, you will need to ask for input from key personnel within your organisation.

You should invite people to be part of the risk management process who have a genuine interest or experience in risk management activities, or have specialised knowledge in the critical success factors of the business, team or project.

Be clear about your expectations and what it is they you would like from the person. Allow sufficient time for employees to contribute and communicate their ideas about the risk management process.

Once you receive input, give the person feedback and thank them for their contribution. Encourage them to consider the strengths and weaknesses of their ideas.

Section 1 summary

You have reached the end of section, Establish risk context.

You should now be able to:

- Review organisational processes, procedures and requirements for undertaking risk management in accordance with current risk management standards
- Determine scope for risk management process
- Identify internal and external stakeholders and their issues
- Review political, economic, social, legal, technological and policy context
- Review strengths and weaknesses of existing arrangements
- Document critical success factors, goals or objectives for area included in scope
- Obtain support for risk management activities
- Communicate with relevant parties about the risk management process and invite participation

2. Identify risks

Section 2 introduction

This section deals with inviting relevant parties to assist in the identification of risks, researching risks that may apply to scope and using risk identification tools and techniques to generate a list of risks, in consultation with relevant parties.

By the end of this section, you will be able to:

- Invite relevant parties to assist in the identification of risks
- Research risks that may apply to scope
- Use tools and techniques to generate a list of risks that apply to the scope, in consultation with relevant parties

2.1 Invite relevant parties to assist in the identification of risks

Introduction

Once you have established the risk context, you will need use a range of tools and methods to identify your risks.

The goal of the risk identification step is to gain a comprehensive list of all risks that may cause a threat to your CSFs and objectives, including impacts to stakeholder requirements, business performance, quality, people, property or the environment.

Risk identification means *determining the sources of risk, cumulative effects of multiple risk, consequences to the business, likely events as well as their causes and potential impacts to the project.*

Consultation

Consultation can be defined as *the sharing of relevant information between key parties on risk matters using a variety of communication strategies.* To ensure the risk management process is conducted effectively, consultation must be present from the beginning.

Defining consultation– AS ISO 31000

AS ISO 31000 defines **consultation** as being a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. It is a process which impacts on a decision through influence, rather than power; and an input to decision making, not joint decision making.

The standard explains that risk can only be managed effectively when there is an emphasis on continual stakeholder feedback, expert judgement and input and reliable information sources and processes.

Elements of effective consultation

The key elements of effective consultation includes:

- communication of truthful, relevant and accurate information
- timely transfer of information
- accessibility to relevant stakeholders
- feedback on input provided
- two-way interaction.

Without ongoing consultation, the risk management process will become difficult and the end result of plans and activities will most likely fail to meet the risk management objectives.

Consultation methods

You will need to plan who you need to consult and how this will occur. Not every stakeholder can be effectively consulted using the same strategy. Therefore, consultation methods must vary depending on the type of stakeholder and the information that needs to be discussed.

Examples of consultation methods include:

- one-on-one meetings
- group meetings
- email
- telephone/teleconferences
- Skype/webinar sessions.

The consultation method that you select must allow for effective two-way communication and feedback in a timely and fair manner.

For more information on effective consultation strategies, refer to the GSE Intranet > Policies & Procedures > Work Health and Safety > General > **‘Work Health and Safety Consultation Policy’**

Benefits of effective consultation

Effective internal and external consultation should make sure that those who are accountable for implementing the risk management system understand the basis on which decisions are made, and the reasons why specific actions may be necessary.

Effective consultation with internal and external stakeholders will achieve the following outcomes:

- Identification of a clear risk context
- Various perspectives and knowledge on risks and their effects on business objectives
- Needs and interests of stakeholders are understood and met
- Greater input and expertise in identifying, assessing and treating risks
- Greater endorsement and support from stakeholders for risk management implementation plans
- More risks will be identified and appropriately treated
- Enhanced change management processes during the implementation phase.

Consultation in the risk management framework

Consultation is an underpinning principle and a key aspect of the risk management framework contained within AS ISO 31000. It is required as a continuous and repetitive activity that must be conducted throughout all aspects of the risk management system, including:

- **Establishment of the risk context** – determining the internal and external operating environment from which risks are birthed and establishing the risk criteria
- **Identifying risk** – finding, recognising and describing risks
- **Analysing risk** – understanding the nature and level of risk
- **Evaluating risk** – determining whether the risk is acceptable or tolerable
- **Treating risk** – eliminating or controlling risks.

Knowledge and expertise

Where possible, you should draw on the knowledge and expertise of key personnel within your organisation. This may include members of the senior management team that can provide you with detailed information on the risks faced by the organisation.

Your organisation may use contractors, employees or a combination of both. Their advice about potential risk as well as solutions can be invaluable. By engaging employees and contractors in discussions about potential risks you may be able to determine the risk sources, new or emerging risks, the consequence and likelihood of risk and the best strategies for reducing the risk.

2.2 Research risks that may apply to scope

Introduction

According to AS/NZS ISO 31000:2009 Risk management principles and guidelines, the risk assessment process includes three (3) key stages:

1. **Risk identification:** The process of gathering together a comprehensive list of all risks that may cause harm to people, processes, property or the environment.
2. **Risk analysis:** The process of considering the causes and source of risk, their potential consequences and probability of harm occurring.
3. **Risk evaluation:** The process of allocating a priority number to each risk.

This three part process enables you to determine what actions (risk treatments), if at all, need to be taken to minimise the impact on project objectives. Each of these stages are explained in full detail over the next series of lessons.

Sources of risk

Risk is the possibility of harm or loss of injury in relation to a business or project and its people, processes, property or environment. A source of risk is defined as *anything tangible or intangible that has the ability to give rise to risk*.

Risk source is commonly grouped according to internal (controllable) and external (uncontrollable) risk. The risk sources will come from the key areas identified in your PEST and SWOT analysis. There are internal and external risks.

Internal risk	External risk
The examples of internal risks are: • workforce • revenue/budget restrictions • operational limits • small marketing budget • operational capability • health and safety incidents • resource constraints.	The examples of external risks are: • new technologies • emerging competition • unstable economy • political instability • loss of vital customers • changes in legislation • changing customer needs and interests.

Common sources of risk

Some common sources of risks are provided here.

Risk category	Examples of risk
Competitor activity	The examples of risks are: • merger activity • market acquisitions.
Economic performance	The examples of risks are: • the economic cycle (recession and prosperity) • changes in exchange rates.
Financial markets	The examples of risks are: • access to reputable sources of funds • funding contingencies.
Legal matters	The examples of risks are: • contract administration • conflicts and dispute resolution.
Marketing appeals	The examples of risks are: • release of competing products or services • market share.
Organisational practices	The examples of risks are: • initiatives to outsource, re-engineer, restructure or downsize • existing standard operating procedures, policies and processes.
Political agendas	The examples of risks are: • legislation • documentation and record keeping.
Resource capability	The examples of risks are:

	• skills shortages in key areas • limited availability.
Stakeholders	The examples of risks are: • unknown needs and expectations • unfulfilled expectations.
Technology impacts	The examples of risks are: • product inefficiencies • product obsolescence.

2.3 Use risk identification tools and techniques to generate a list of risks, in consultation with relevant parties

Introduction

There are many different types of tools and methods available to identify your organisational, team or project risks.

These tools should take aim at the source, based on the risk context identified in the previous step. Once you have identified the risks, you will need to generate a draft list, in preparation for the next stage of the process which is risk analysis.

Risk identification tools and techniques

Below are explanations for some proven risk identification tools and methods.

- **SWOT analysis:** SWOT tool enable managers to scan their internal and external environment to analyse the positive and negative risks. SWOT stands for strengths, weaknesses, opportunities and threats. Strengths and weaknesses are internal to an organisation's environment. 'Opportunities' and 'threats' on the other hand, involve assessing the organisation's external environment for any opportunities and threats it poses.
- **PEST analysis:** PEST is an acronym that describes the four major elements of the external or 'macro-environment' that impacts on an organisation. PEST stands for the political, economic, socio cultural and technological forces that are outside of the control of the business. PEST is also used when conducting a risk assessment.
- **Competitor analysis:** A formal review of the key competitors in the industry, their strengths and weaknesses and how they threaten and present opportunities to your project.
- **Project scope management plan:** A broad document designed to capture the essential inputs, assumptions and constraints at the concept stage of the project. It will define project boundaries, including potential variations, constraints, risks and assumptions.
- **Cost-benefit analysis:** A detailed analysis of the financial inputs and the associated benefits for the monies invested.
- **Feasibility studies:** A range of feasibility studies can be conducted to determine the viability of a project and its impacts on the organisation (positive and negative). The process will usually include estimating start-up and working capital requirements, forecasting a return on investment, and estimating profitability.

- **Porter's Five Forces framework:** This is a useful tool in analysing a particular environment of an organisation. The five (5) factors that it analyses are the forces that influence industry performance. The five (5) forces relate to:
 1. Competitive rivalry
 2. Power of suppliers
 3. Power of buyers
 4. Threat of substitutes
 5. Threat of new entrants.
- **Consultation:** Consultation means meeting with key people within and outside of your business who have a firm understanding of the project and its associated risks. These people may include the risk manager, WHS Manager, project sponsor, project administrator, program manager, Subject Matter Experts, and environmental officers, etc.

Risk identification tools and techniques

Explanations for proven risk identification tools and methods are continued below.

- **Brainstorming:** Brainstorming combines a relaxed, informal approach to risk identification and analysis using group problem-solving with lateral thinking. It requires people to generate assumptions and ideas about risk that can at first seem to be a bit left of centre. The aim is to develop a comprehensive list of risks relative to the task at hand.
- **Delphi technique:** This is a qualitative forecasting process whereby a panel of experts are invited to provide their input and expertise on a range of risk topics and questions. The process is run by a facilitator, who poses the same questions using a pre-determined questionnaire to each panel member. After each round of questioning, the facilitator provides the panel members with an anonymous summary of the panel's total responses as well as the reasoning behind the forecasts. The panel members are then given an opportunity to revise their responses based on the general consensus and input of other panel members. After the prescribed numbers of rounds (up to three rounds) have been completed, the facilitator analyses the data to develop mean and median scores of the revised responses.
- **Internal research:** Conducting research into organisational and project documents including the strategic plan, operational plan, risk management policy, activity cost estimates, quality management policy and human resource management plan.
- **External research:** Conducting research into industry and regulatory based-risks. Sources of information may include:
 - Work Health and Safety regulator website
 - Business.gov.au website
 - manufacturers and suppliers can provide information about hazards associated with specific plant, substances or processes including safety data sheets
 - technical specialists who are regarded as experts in a particular type of equipment, task or industry
 - external specialists and consultants who specialise in risk management systems
 - Standards Australia who are responsible for developing, maintaining and distributing a range of Australian Standards in products, services and systems.
- **Cause and effect diagram:** A cause and effect, Fishbone or Ishikawa, diagram is a way of identifying all the possible causes related to a problem. In many situations, an event can be

produced by multiple causes and multiple combinations of causes. These are mapped in a diagrammatic view to show project team members the range of risks and their sources.

- **Checklists:** A formal checklist can be developed to guide the process of conducting a risk identification on a piece of equipment, tool or work package.
- **Hazard hunts:** A group hazard identification process whereby members form the health and safety committee or a work group will stop work to search the work area for health and safety hazards and risks. Any risks found are then documented and a risk assessment is performed by the group to establish the potential and consequence of harm and priorities for controlling the hazards.
- **Job safety analysis(JSA):** Any new or job task is assessed to identify its hazards and risks. Following this, a safe work procedure is developed to ensure that workers have a safe process to follow, they are aware of the risks and how to control them to prevent an injury. This is also known as a Job Hazard Analysis (JHA) or Task Hazard Analysis (THA).

Who is involved in risk identification?

The risk identification process should involve key people such as management, SMEs and team members, who are usually involved in business operations.

These people may also include:

- project team members
- risk management team/specialists (if applicable)
- clients
- SMEs
- experts from outside of the organisation
- end users
- department managers
- line managers.

Section 2 summary

You have reached the end of section, Identify risks.

You should now be able to:

- Invite relevant parties to assist in the identification of risks
- Research risks that may apply to scope
- Use tools and techniques to generate a list of risks that apply to the scope, in consultation with relevant parties

3. Analyse risks

Section 3 introduction

This section deals with assessing likelihood and consequence of risks, evaluating and prioritising risks for treatment.

By the end of this section, you will be able to:

- Assess likelihood of risks occurring
- Assess impact or consequence if risks occur
- Evaluate and prioritise risks for treatment

3.1 Assess likelihood and consequence of risks occurring

Introduction

The next step of the risk assessment process is to **analyse the risks** identified from the previous step. Risk analysis is about *understanding the risk in terms of whether it should be treated, monitored or dismissed*. It involves the consideration of the causes and source of risk, their potential consequences and probability of harm occurring.

Risk analysis

An event can have multiple consequences and varying degrees of impact to the organisation, team or project.

Oftentimes, the outcomes will be unclear and each person conducting the analysis will have varying perceptions as to what could happen.

In such cases, it is important to take an objective view as much as possible and make decisions based on factual data such as reports, plans, forecasts, past incidents and statistics, rather than personal opinions.

Types of risk analysis techniques can be undertaken based on three (3) techniques:

1. **Qualitative:** Use of questioning and personal judgement to gather information and make a decision about the risk level. These may include brainstorming, specialist knowledge, questionnaires, personal observations, client feedback or intuitions to classify and assess the risk impact and likelihood. A qualitative risk analysis prioritises the identified project risks using a pre-defined internal rating scale. Risks are scored by one or more person based on the probability or likelihood of an event occurring and the impact on project objectives. Qualitative risk analysis techniques are quicker and easier to perform and are used for projects that carry a lesser value and importance, have budget restrictions or have been identified as having a lower risk level.
2. **Quantitative:** Methods that aim to use research and/or measurement tools to make a decision. The process uses forecasting and estimating to determine the probability and impact of risk. These techniques may include: probability and consequence analysis, data collection, modelling, statistical analysis, decision trees and event tree analysis. Quantitative risk analysis is more complex and time consuming to perform and is commonly used in projects where the expertise and resources are available, risk data is easier to obtain, the project is more complex with a greater array of risks, impacts and probability and the project is of much higher value to the organisation.
3. **Semi-quantitative:** Methods that give a quantitative ranking to a qualitative decision such as low risk, medium risk or high risk. This is the most common technique used in risk management systems as it enables a more accurate analysis of the risk impacts than that of qualitative analysis techniques. The risk score matrix, layers of protection analysis (LOPA) and risk score nomogram tools are all a form of semi-quantitative analysis.

Risk attributes

The main outcomes from the risks analysis task is to define the **attributes** of the identified risk. Risk attributes are the key characteristics of the risk that help to understand its potential impact on the business.

These attributes mostly include:

1. **Consequence:** The nature and impact of harm that may occur on people, processes, property or the environment.
Likelihood: The probability of harm that may occur on people, processes, property or the environment.

Both of these attributes are identified using risk analysis methods. When combined, they will determine a **risk level** – the magnitude or exposure based on the combined effect of its consequence and likelihood assessments. The risk level is then used to determine priorities and appropriate controls to manage their impacts on the project.

Risk analysis processes

There are a wide variety of risk analysis processes used within industry to determine the likelihood and consequence of risks. There is a 5x5 **risk score matrix** (semi-quantitative) method of analysing risks.

Consequence of harm

The table here shows the consequence of harm.

Risk consequence	Value descriptor	Explanation
5	Catastrophic	Extreme scale of impact. Death, off-site release with detrimental effect, huge financial loss
4	Major	Large scale of impact. Extensive injuries, loss of productivity, off-site release with no detrimental effects, major financial loss
3	Moderate	Manageable scale of impact. Medical treatment required, on-site release contained without outside assistance, high financial loss
2	Minor	Some impact would be noticeable. First aid treatment, on-site release immediately, medium to low financial loss
1	Insignificant	Inconsequential impact. No injuries or financial loss

Probability of harm

The table here shows the probability of harm.

Risk probability	Value descriptor	Explanation
5	Almost certain	100% possibility of change occurring. Is expected to occur in most circumstances
4	Likely	Most probable that change will occur. Will probably occur in most circumstances
3	Possible	Reasonable to consider change would occur. Might occur at some time
2	Unlikely	Slight possibility of change occurring. Unlikely to occur, but history of event exists within the business
1	Rare	1 in a 100 chance of change occurring. May occur only in exceptional circumstances

		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

Risk score = 1-Very high, 2-High, 3-Moderate, 4-Low

Gather reliable information to ensure you are thorough in your risk analysis, you will need to gather and review a range of internal and external information, based on reliable sources.

Internal sources	External sources
The internal sources include: • project management plans • strategic and operational plans • evaluation results of products and other deliverables • past action/improvement plans • records of analysis • past issues logs/registers • past quality assurance audit results • schedules and timelines and variances from baseline schedules • complaints • testing/monitoring results.	The external sources include: • manufacturer/suppliers website • WHS regulator website • industry associations • external marketing consultants • talking to your clients • industry magazines • blogs and reviews • statistics and data compiled by the Australian bureau of statistics • media articles and statistics published in newspapers, radio, television, etc.

Risk criteria

AS ISO 31000 defines the risk criteria as the “*terms of reference used to evaluate the significance or importance of an organisation’s risks*”. In other words, it is the benchmarks to determine the level of harm a risk may cause to the business and whether action needs to be taken.

Overview

The risk criterion is important to define, in order to determine whether a threat and specified level of risk is acceptable or tolerable. The outcomes will impact on your priorities for controlling identified hazards and risks – taking action to eliminate or minimise the risk.

Defining the risk criteria

The establishment of risk criteria is used to calculate the significance of the risk that has been identified. The criteria must be relative to your project’s internal and external context and should be developed in view of Australian standards for risk management, legislation as well as project and stakeholder requirements that the organisation must meet.

Risk criteria should also be aligned with your organisation's:

- vision, mission and values
- policies and procedures
- risk management objectives.

Nearly all activities in the project involve risk in some way or the other, and there is no universally agreed criteria for what levels of risk are acceptable. Therefore, it is up to each project management team to establish and agree on their own risk criteria.

The ALARP principle

A widely used principle for determining criteria for acceptable and residual risks is the ALARP principle. ALARP stands for 'As Low As Reasonably Practicable'. This means that risks should be controlled to ensure the impacts on the project are minimised as best as possible.

Under the ALARP principle, risks that are identified should be actioned according to:

- likelihood of the risk resulting in harm to the project
- degree of harm that may be caused
- any existing knowledge about the risks
- availability of resources to control the risk
- cost versus benefit and whether the cost associated with controlling the risk is grossly disproportionate to the outcomes achieved
- the level influence and control over the risk.

3.2 Evaluate and prioritise risks for treatment

Introduction

As a result of risk analysis process, you should be able to determine the priorities for addressing each identified risk that may impact on the business.

You will need to either take action to eliminate or minimise the risk, monitor the risk or dismiss the risk.

Since it is impossible to control every risk, it is important to analyse and evaluate each risk against your agreed criteria and rank each risk accordingly.

Risk evaluation

The third and final step of the risk assessment phase is to **evaluate each risk** by assigning a rating, number or rank. The goal of conducting a risk evaluation is to help make decisions as to how to treat the risk, including whether action is required and how quickly treatments need to be applied.

Risk evaluation involves comparing the outcomes from the risk analysis with the risk criteria established when the context was identified in the first step of the process. Based on this outcome, appropriate treatments/controls can then be agreed upon.

Defining risk priorities

Decisions on risk priorities must be made in consultation with internal and external stakeholders as well as strategic and operational plans to ensure consistency, alignment and agreement, where possible.

Risk priorities must focus on the **Critical Success Factors (CSFs) and objectives** of your organisation, project or team.

Additional considerations in a risk evaluation

When performing a risk evaluation you may also need to consider the following:

- nature of the risk
- prior knowledge of any incidents and harm relating to this or other similar risks
- current control measures in place
- costs involved in actioning the risk treatment and the level of influence or control over the hazard
- the level of exposure, including how much, how often and how long the business is exposed to the risk
- inter-relationships and impacts of other risks

Section 3 summary

You have reached the end of section, Analyse risks.

You should now be able to:

- Assess likelihood of risks occurring
- Assess impact or consequence if risks occur
- Evaluate and prioritise risks for treatment

4. Select and implement treatments

Section 4 introduction

This section deals with selecting appropriate risk treatments, developing and communicating the risk treatment action plan. It also deals with checking and storing documentation, implementing and monitoring the action plan and evaluating risk management process.

By the end of this section, you will be able to:

- Determine and select most appropriate options for treating risks
- Develop an action plan for implementing risk treatment
- Communicate risk management processes to relevant parties
- Ensure all documentation is in order and appropriately stored
- Implement and monitor action plan
- Evaluate risk management process

4.1 Select appropriate risk treatments

Introduction

Depending on the stage of the project, you may have existing risk controls in place to manage the likelihood and consequence of damage. If this is the case, you will need to evaluate these controls as part of the risk management process.

A risk can have a positive or negative impact on project objectives. For the outcomes that are negative, these must be eliminated or minimised, using a range of controls.

Risk controls and treatments

Risk controls and treatments are established and demarcated by the International Standards Organisation (ISO Guide 73:2009). Although in this standard the two terms are defined separately, in many circles, they are often used interchangeably.

Risk control

A measure that is being used to modify risk. Examples include any process, policy, device, practice, or other actions which modify risk.

Risk treatment

A process used to modify risk after controls have been implemented. Examples include avoidance, taking risk to pursue an opportunity, removing the risk source, changing the likelihood, changing the consequence, sharing the risk with another party, retaining the risk by informed decision.

Similarities between control and treatments

Both controls and treatments exist to modify the risk by reducing the likelihood of negative risks occurring and/or reducing the consequence of negative risks should they occur (or, conversely, increasing likelihood and consequence if positive risks). In addition, controls and treatments both aim to address the root cause of the risk and may not always apply the intended effect in modifying the risk.

Differences between control and treatments

The difference between a control and a treatment exists in whether they are established at the time of the risk assessment or after.

The following table explains the key differences between risk controls and treatments.

Controls	Treatments
Existing strategies and processes currently in place such as systems, policies, procedures, standard business processes, practices. Some examples of controls include: Employee Code of Conduct, budget management, media and public relations protocols, delegation authorities, and security access to buildings. A risk may have more than one control, and a control may address more than one risk.	Additional strategies/activities we need to develop and implement should the risk level be unacceptable after controls are applied. Should a control be assessed as ineffective or where there are control gaps to modify the risk, a treatment plan may include strengthening the controls or developing new controls. Generally treatments are specific to a risk. A treatment only becomes a control after it has been fully implemented and deemed effective in modifying the risk to an acceptable level.

Existing risk controls

When deciding on what risk treatments to apply, you must take into consideration the existing risk controls. These may include a process, policy, use of equipment, work practice, or other action that aims to modify (eliminate or minimise) the risk.

Categories of existing risk controls

Risk controls can be grouped according to the following categories:

- change/reduce the likelihood of risks
- reduce/change the consequence of risks

- reduce both the likelihood and consequence of risk
- share/transfer the risk in part or in whole to a third party - for example to insurance providers, joint ventures or partnerships
- retain/accept the risk and do nothing - resource requirements feature heavily in this strategy.
- avoid the risk by changing business practices
- retaining the risk and managing it.

Evaluate existing risk controls

Each existing risk control needs to be evaluated to ensure that it is effective in achieving its purpose. When controls are working as intended, they will reduce the risk level to an acceptable or 'tolerable' level. In project management, excessive or inadequate controls may hamper the progress of the project and may give rise to new risks that must be addressed.

- To evaluate a control, consider the following factors: Is the control still relevant to current conditions?
- Is the control being used correctly by the workforce?
- Is the control 'fit for purpose' for example, design effectiveness?
- Does the control work as practically as intended for example, operational effectiveness?
- Is the control documented?
- Is the control regularly monitored and up to date?

If an existing control is ineffective, then improvement processes must be proposed and documented in the risk treatment plan.

Risk treatment following your risk control evaluation, there may be **residual risk** left over that needs to be addressed. Residual risk refers to *any risk remaining after a control or treatment has been implemented*. Where residual risk remains, there may still be a reasonable threat to business CSFs and objectives that must be addressed through additional controls called "risk treatments".

Risk treatment options include elimination of the risk altogether, risk mitigation, risk reduction and risk transfer.

Eliminate the risk

Where risks with a negative impact have been identified, they must be **eliminated or avoided altogether – where possible**. This can often be achieved for internal risks, such as human resource, financial or process related risks. Examples include: changing a vendor, disposing of a defective material or terminating a team members' employment contract.

For other risks, including external based events, risks can be avoided, reduced or transferred using risk treatment options.

- Factors in considering the validity of this option include: What will happen if the activity is not undertaken?
- Is the risk level too high to proceed /continue with the activity?
- Is the cost of the required controls higher than the benefit of the activity?
- Will the failure of the activity have critical consequences for other areas of the business?

Mitigate the risk

Risk mitigation involves *any action taken to alleviate the severity and consequences of a risk*.

Examples may include increased training, human resources or finance, delayed deployment of staff, fast-tracking a scheduled task, etc.

Mitigating actions must be documented on the risk management plan or risk register. If a risk is classed as “high”, then mitigating actions must be documented. If a risk is classed as “medium”, then mitigating actions are recommended, but not required. If a risk is classed as “low”, then mitigating actions are not required.

Reduce the risk

Risk reduction means *reducing the likelihood and or the consequences of the risk occurring*.

Factors in considering the validity for this risk treatment strategy include:

- Can the likelihood of the risk occurring be reduced? (through preventative maintenance, or quality assurance and management, change in the company’s systems and processes)
- Can the consequences of the event be reduced? (Through contingency planning, minimising exposure to sources of risk or separation/relocation of an activity and resources)

Transfer the risk

This strategy may be achievable through *moving the responsibility to another party or sharing the risk through a contract, insurance, or partnership/joint venture*.

Be aware that a new risk arises in that the party to whom the risk is transferred may not adequately manage the risk.

Select the link below to find out more information about how to control your business risks:

<https://www.business.qld.gov.au/business/running/risk-management/risk-management-plan-business-impact-analysis/treat-risks-business>

Residual risk

Residual risk refers to *the level of risk remaining after new risk treatments/controls have been applied*. The process of calculating residual risk is exactly the same as the way in which you calculated your risk level prior to implementing any risk treatments. It should be based on the risk criteria established earlier in the project risk management system process and use the same risk assessment tools, such as a risk matrix, rating system, nomogram or (layers of protection analysis) LOPA.

Calculating residual risk

Calculating the residual is important in terms of identifying whether the risk treatments are going to be effective in controlling the risk and reducing its level to something that is tolerable.

For example:

- **Risk** = Excessive manual lifting required from workers on site. The tasks involve lifting 1.1x1.1m pallets by hand over a period of 3 hours per day.
- **Risk rating** = Very high – may lead to serious spinal injury, loss of vital human resources and impacts on the project costs and schedule.
- **Proposed risk treatments** = Training workers in safe lifting techniques, introduce use of powered pallet trucks, regular supervision, warning signs around prominent areas and encouraging team lifting.
- **Residual risk** = Low.

Consult with stakeholders

Consultation with project stakeholders and risk management specialists must be conducted throughout the whole risk management process.

To ensure the consultation process is effective, you will need to consider **who** you need to consult with and **how** this will occur. Not every stakeholder can be effectively consulted using the same

strategy. Therefore, consultation methods must vary depending on the type of stakeholder and the information that needs to be discussed.

Examples of consultation methods include:

- One-on-one meetings
- Group meetings
- Email
- Telephone/teleconferences
- Skype/webinar sessions.

The consultation method that you select must allow for effective two-way communication and feedback in a timely and fair manner.

4.2 Develop and communicate the risk treatment action plan

Introduction

The process of evaluating existing risks and developing risk treatments must be documented in a risk treatment plan. This may be a single document, part of the risk management plan or an inclusion in the project management plan.

Once these details are recorded, you can prepare for the implementation process to ensure that treatments are appropriately integrated into the work plan.

Risk action plan

Following your risk identification and assessment, you will have consulted with your stakeholders and developed appropriate methods to modify the risk to ensure the effective performance of the organisation, team or project.

A risk action plan will list and explain the following details:

- the identified risks in accordance with the appropriate ranking process
- risk levels for each risk based on an assessment of the consequence and likelihood of harm occurring and the possible outcomes in terms of impacts to people, processes, property and environment
- the current risk controls (if applicable) that are in place
- description of new risk treatment actions and activities you will need to implement to either (a) accept, (m)itigate, (t)ransfer, or (e)liminate the risk,
- the calculated residual risk
- responsible persons for each risk
- a proposed end date that the treatments need to be actioned by.

To view a copy of a risk treatment plan, refer to GSE Intranet > Policies & Procedures > Project Management > Templates > Project Risk Management Plan > See section entitled “Risk Treatment Strategy”

Communicate risk management processes and plans

A common complaint in business is that employees do not know the processes and plans of the organisation that they work for. This issue generally comes from a lack of engagement and poor communication.

Overview

Although project team members do not need to know all of the details of a plan, it is important that they learn about and understand the intentions of the management plan and how it applies to them.

In simple terms, the secret to risk management planning is in the implementation. Therefore, you need to know **how** to communicate the plan to the organisation and **who** needs to know **what** information.

Guidelines to effective communication

You should never assume that your team members or managers know what is expected of them. Everyone needs to understand what is required of them as part of the risk management plan and process however the level of information should vary depending on your audiences.

- To ensure information is communicated effectively, follow these guidelines: Identify the people throughout the project organisational chart and group them into segments.
- Identify the information needs of each segment.
- Determine the range of appropriate communication strategies that could be used for each audience group.
- Identify when the audience group needs the information by.
- Identify who can be utilised to disseminate the information across the organisation.
- Consult with management teams to develop an appropriate communication strategy.

Communication methods

A plan or process not yet communicated has little value. It has no power to change the performance of the business, inspire workers or command a new direction that is needed to meet the necessary changes.

A communication method must be carefully chosen to ensure the information is provided to the right people in a reasonable time-frame.

Details of the risk action plan and process can be communicated using:

- team briefings to engage front-line workers
- newsletters/e-letters
- holding short one-to-one meetings with key stakeholders across the organisation
- distributing a copy of the plan via email
- posting highlights of the plan on the front page of the staff portal
- displaying the objectives and requirements in prominent locations across the organisation
- producing a video presentation explaining the plan and posting it on the company intranet.

4.3 Check and store documentation

Introduction

This risk management system is iterative – in other words, since the risk context (internal and external operating environment) is constantly evolving, the risk management process itself never ends.

As such, risk management plans and documents need to be checked and updated to ensure they accurately reflect the current conditions, treatments and risk levels encountered within the business.

Risk management plans and objectives

The overall aim of a risk management action plan is to describe the process of effectively identifying,

assessing and mitigating business risk.

Overview

Risk in a business environment cannot be totally eliminated. Therefore, the objective of a risk management process is to reduce the impact of unplanned incidents on the organisation, team or project by identifying and addressing potential risks before significant negative consequences occur.

The risk management action plan acts as a core document in this process.

Important of risk documentation

Documentation of the risk management process is needed to:

- Demonstrate that the process is correctly managed.
- Provide evidence of a systematic approach to risk identification and analysis.
- Complete the knowledge database.
- Provide decision makers with a risk management plan for approval.
- Provide an accountability mechanism and tool.
- Facilitate monitoring and review.
- Provide an audit trail.
- Share and communicate information.

Check and store risk plans

Any changes and additions to the risk management action plan must be checked for accuracy, relevance and validity. It must be updated reflect current risks as relevant to the risk context.

A risk management action must be stored correctly on the portal, computer network or other system to ensure you and your stakeholders have the most current, reliable and accurate information in order to track progress and make informed decisions.

When naming files and folders you should use names that make sense and relate to the data that is stored within the file. Within many large organisations you may find there are specific guidelines to be used when naming and storing files and folders and you should be aware of these, and follow the guidelines.

This is especially important when you're working within a large team, so that the naming of files and folders is consistent between each member of the group.

Refer to the GSE Intranet > Policies & Procedures > Style Guides & Templates > General >

'Instructions for Electronic Filing'

Risk register

A risk register database is a common tool used to manage and monitor business risk. It is also commonly used in work health and safety risk management.

It contains a ranked list of risks, references to associated risk action plans and names of individuals responsible for each risk. Regular updating of the risk register should be part of the ongoing risk management process.

Refer to the GSE Intranet > Policies & Procedure > Project Management > Templates > **'Project Risk Register Template'**.

4.4 Implement and monitor the action plan

Introduction

Once the risk management action plan has been completed, you will be ready to implement the proposed risk treatments to either eliminate or minimise the risks.

The implementation process can often make or break the success of the risk management process. Many plans have good intentions but tend to fail based on how poorly they are introduced into work practices.

The successful implementation of risk treatments requires a sound knowledge of the risk management process, effective communication and sufficient support.

Risk management implementation

Successful risk management systems don't just happen. They require careful planning, consultation, research and a methodology for implementation. The implementation process should therefore be planned to consider how the risks will be identified, assessed, controlled and monitored from a holistic view point. A standard risk management implementation plan will usually include the following elements.

Resource allocation

Resource allocation comprises of:

- **time** – release from usual work duties to attend meetings or training or to plan meetings
- **money** – release of finance to purchase equipment, hire additional staff or pay overtime loading for training
- **people** – access to consultants and experts in the field of risk management
- **physical equipment** – machinery, computers, medical supplies, health monitoring tools, testing equipment or substances.

Task schedule

Based on the proposed actions, a time-line of events should be developed stating when each risk treatment must be implemented, with a deadline date that the plan will work towards.

Consultation and communication

A consultation and communication strategy that explains who needs to be consulted/communicated with, what needs to be communicated and how information will be disseminated and fed back to key stakeholders and workers affected by the risk management activities.

Training and support

On-the-job supervision, coaching and availability of supervisors if workers have queries or concerns that need to be raised. Training must be competency-based (outcome-focussed) for all workers that are affected by the new risk management process.

Reporting and monitoring requirements

A strategy detailing the key stakeholders that need information about risk management activities, their key information requirements, frequency of reports and how they will be distributed. This should also describe the positive performance and outcome indicators that will be used to track and measure performance of risk management activities.

To view a copy of a risk management implementation plan, refer to the GSE intranet > Policies & Procedures > Work Health & Safety > Templates > **'WHS Risk Management Implementation Plan'**

To view a copy of a risk implementation plan, refer to GSE Intranet > Policies & Procedures > Project Management > Templates > **‘Project Risk Management Plan’** (see section entitled “Implementation Strategy”)

Monitor risks

Risk monitoring and control is the next stage of the risk management process. It is the process of tracking identified risks, monitoring residual risks, identifying new risks and evaluating risk processes.

Overview

This stage is perhaps the most important part of the risk management process as it ensures that all risk treatments that have been applied, are in fact effective and any new risks are managed accordingly.

The overall aim of monitoring and reporting on a risk management system is to identify, address and reduce deficiencies in risk treatment and process performance.

Components of risk monitoring stage

The risk monitoring stage should include:

- ensuring that risk controls and treatments are effective in both design and operation
- looking at improvements in the overall risk management system
- analysing lessons learned from events
- identifying changes in the internal or external context
- identifying emerging risks.

Data and information collection methods

To help in monitoring the risk management process and ensure the currency of risk plans, you will need to collect reliable data and information.

Examples may include:

- completing risk monitoring checks
- consulting with project team members
- updates of the risk register
- speaking with workers who are using the risk controls
- conducting a follow-up risk assessment to confirm residual risk
- conducting follow-up hazard hunts and site audits/inspections
- investigating and responding to unplanned events and documenting corrective actions
- conducting an internal audit against the criteria set out in AS ISO 31000.

Frequency of monitoring processes

Monitoring and review processes must be carefully considered as part of the risk management action plan.

A risk review process can be performed either:

- **Periodically** – Weekly, monthly, quarterly or at the completion of each milestone
- **On an ad hoc basis** – Random reviews or following an incident/unplanned event.

Modify risk plan

The information resulting from your new evaluation of the risk context must be recorded on a risk template such as a risk register, or directly into the project risk management plan, or project management plan.

The documentation process is crucial in risk management, monitoring and reporting purposes. This ensures the relevant documents are up-to-date and accurate and provides the necessary assurance to stakeholders and the client that the project management team is doing all it can to address its project risks.

4.5 Evaluate risk management process

Introduction

To evaluate the risk management process, you will need to gather quality data and information about the performance of your risk management activities. Once you have gathered your information, you will need to work with your key stakeholders to analyse the differences between the actual performance and the planned performance.

As part of your evaluation, you will need to determine strengths, successes and areas for improvement and discuss and agree upon corrective actions to ensure the same issues do not repeat in future projects.

Risk review criteria

Review the following list of considerations when reviewing risk management activities.

- Alignment of the risk management process with AS/NZS 31000:2009 Risk Management – Principles and Guidelines
- Accuracy of risk identification and assessment processes
- Effectiveness of risk treatments in protecting CSFs and objectives
- Summary of the risk challenges that were faced over the course of the project or reporting period
- Performance of risk monitoring processes
- Impact of changes in risk context on organisational, team or project performance
- The client's acceptance and satisfaction with organisational, team or project outputs (products or services)
- Performance of the organisation, team or project and how well or poorly the risk management system assisted in achieving these outcomes

Risk management lessons

Risk is not a one-off event, nor will every risk management action or process be effective each and every time.

Lessons can be valuable in the continuous improvement process. These lessons may be large or small and can come from a variety of sources, not just the final review. Lessons may be identified from changes, mistakes, successes, feedback and failures.

- Some of the lessons gained from a review of your risk management system may include: Avoid using a risk control.
- Invest more time into risk identification processes.
- Ensure a more quantitative risk analysis process.
- Schedule more regular reviews of the risk context throughout the project.
- Do not use a particular supplier for the next project.
- Stick closer to the risk management plan.
- Implement more resources into specific areas.
- Monitor risk treatments more closely.

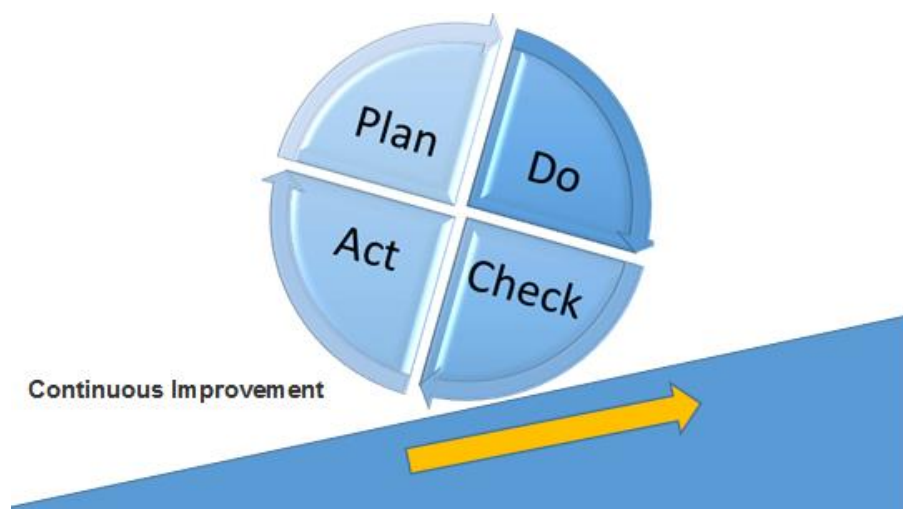
Documenting the evaluation

The outcomes of the formal evaluation must be recorded to ensure the process has been completed and to aid in the decision making and continuous improvement processes.

The discussion points, actions, lessons and agreements are usually recorded in a formal business report and distributed to your key stakeholders.

The Plan-Do-Check-Act process

Australian Standards for risk management has a large emphasis on continuous improvement – an ongoing commitment to improving a business' systems, products and services. The P-D-C-A model provides a framework for managers to follow to enable effective planning, implementation as well as areas for improvement. The P-D-C-A cycle provides a simple recipe for how risk improvement actions should be conducted from start to finish. The monitoring and evaluation process is based on the third key element of P-D-C-A (Plan-Do-Check-Act).



Plan

Develop a strategy for implementing the risk treatments into including communication, documentation, responsibilities, resources, training, support and how you are going to review the plan.

Do

Implement the risk treatments, with the knowledge that you may possibly miss the mark in one or more areas.

Check

Collect useful data and assess the results of the risk treatments. Test and measure results to identify what worked well and what didn't. Decide how it could be done differently. You may find that a single risk treatment requires a small or major adjustment.

Act

Identify the key learning's from the process. Decide whether to adopt the changes and introduce it in its entirety, abandon it, or run through the cycle again with slightly changed conditions.

Select the following link to watch the video and learn more about PDCA:

<https://www.youtube.com/watch?v=wLOk0UXo70g>

Section 4 summary

You have reached the end of section, Select and implement treatments.

You should now be able to:

- Determine and select most appropriate options for treating risks
- Develop an action plan for implementing risk treatment
- Communicate risk management processes to relevant parties
- Ensure all documentation is in order and appropriately stored
- Implement and monitor action plan
- Evaluate risk management process