BSB50618 – DIPLOMA OF HUMAN RESOURCE MANAGEMENT
BSB51918 – DIPLOMA OF LEADERSHIP AND MANAGEMENT
BSB50215 - DIPLOMA OF BUSINESS

Study Support materials for

BSBRSK501- Manage Risk

BSBRSK501 in BSB50215 includes the requirement that answer refer to the current R.M. standard. DD.

STUDENT HANDOUT

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Establish risk context	1.1 Review organisational processes, procedures and requirements for undertaking risk management in accordance with current risk management standards 1.2 Determine scope for risk management process 1.3 Identify internal and external stakeholders and their issues 1.4 Review political, economic, social, legal, technological and policy context 1.5 Review strengths and weaknesses of existing arrangements 1.6 Document critical success factors, goals or objectives for area included in scope 1.7 Obtain support for risk management activities 1.8 Communicate with relevant parties about the risk management process and invite participation
2. Identify risks	2.1 Invite relevant parties to assist in the identification of risks 2.2 Research risks that may apply to scope 2.3 Use tools and techniques to generate a list of risks that apply to the scope, in consultation with relevant parties
3. Analyse risks	3.1 Assess likelihood of risks occurring 3.2 Assess impact or consequence if risks occur 3.3 Evaluate and prioritise risks for treatment
4. Select and implement treatments	4.1 Determine and select most appropriate options for treating risks 4.2 Develop an action plan for implementing risk treatment 4.3 Communicate risk management processes to relevant parties 4.4 Ensure all documentation is in order and appropriately stored 4.5 Implement and monitor action plan 4.6 Evaluate risk management process

Introduction

The unit of competency, Manage Risk provides students with the skills and knowledge required to manage risks in a range of contexts across an organisation or for a specific business unit or area in any industry setting. Irrespective of your role within an organisation and as to whether you have responsibility of directly supervising others or not, all employees can be impacted by risk. The following student handout is broken down into four (4) key areas:

1. Establish risk context
2. Identify Risk
3. Analyse Risk
4. Select and implement treatments

However, before we explore these further, take some time to review the following definitions.

Definitions

Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). The notion implies that a choice having an influence on the outcome exists (or existed). Potential losses themselves may also be called "risks". Almost any human endeavor carries some risk, but some are much more risky than others.

ISO 31000 is intended to be a family of standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000:2009 is to provide principles and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

Currently, the ISO 31000 family is expected to include:

- ISO 31000:2009 _ Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- ISO Guide 73:2009 - Risk Management - Vocabulary

Act of God is a legal term for events outside of human control, such as sudden floods or other natural disasters for which no one can be held responsible.

A root cause **is rarely an initiating cause of a causal chain which leads to an outcome or effect of interest. Commonly, root cause is misused to describe the depth in the causal chain where an intervention could reasonably be implemented to change performance and prevent an undesirable outcome.**

Relevant Legislation

- AS/NZS 4360:2004 Risk management.
- legislation, codes of practice and national standards, for example:
  - duty of care
  - company law
  - contract law
  - environmental law
  - freedom of information
  - industrial relations law
  - privacy and confidentiality
  - legislation relevant to organisation's operations
  - legislation relevant to operation as a business entity
- organisational policies and procedures, including:
  - risk management strategy
  - policies and procedures for risk management
- overall operations of organisation
- reasonable adjustment in the workplace for people with a disability
- types of available insurance and insurance providers

In Australia, it is the responsibility of Managers to ensure a safe working environment for their staff.

Every employee is responsible for following the organisation's risk-management policies and procedures and for remaining aware of the risks they and the organisation might be exposed to and the risks to which they, themselves, might expose the organisation.

However, the ultimate responsibility for identifying and managing risk and establishing a healthy risk culture lies with the owner, managers and/or board of directors who establish the organisation's appetite for risk and risk-management policies and monitors the effectiveness of the various programs and measures that flow from the policies.

1. Establish risk context

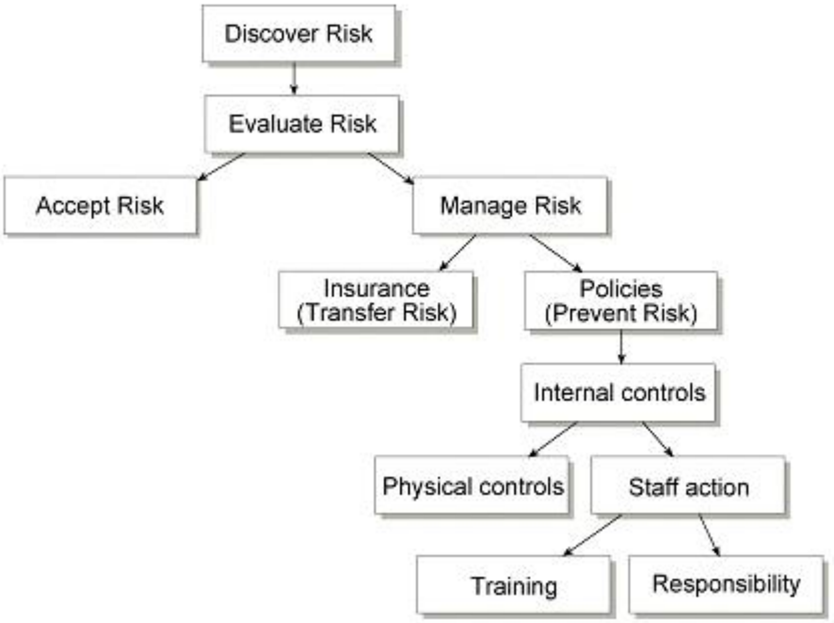
What is Risk?

Quite often, when we consider risk in the business/workplace environment we immediately think of safety (or WH&S). Unfortunately, risk management is much more than this and although it can include risk to people (as in WH&S) it also takes into consideration risk to financial assets (such as theft and fraud) and risk to the environment (such as your organisation polluting the environment or being exposed to pollutants from other businesses). In fact, the range of risks is significant and it is not until you put yourself into the role of a manager or business owner, can you truly understand the extent. The purpose of risk management is to identify the risk events for a project and then establish a Risk Management Plan to manage the risk event and minimize harm to the project.

Who does it affect?

Risk affects all of us…. Risk is everywhere. It affects everything we do and every decision we make. It can cause paralysis to our way of life, force us to become defensive and overreact, erode civil liberties, and destroy confidence. But risk is also necessary because it keeps us on our toes, forces us to check and double check our facts and positions, pushes us to innovate, leads us to seek information more hungrily, and adds the spice that makes life worthwhile.

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as *the effect of uncertainty on objectives*, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The following diagram will help you better understand the risk management process.



Source: O'Donnell 1993, p. 11

In practical terms, when applying the scope of risk management we must consider:

- The organisation (as a whole)
- The individual business units
- Defined activities, events and projects
- Business functions such as HR, Engineering, and Administration etc.

Risks can come from uncertainty in financial markets, project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. Several risk management standards have been developed including the Project Management Institute, the National Institute of Science and Technology, actuarial societies, and ISO standards. Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

The strategies to manage risk typically include transferring the risk to another party, avoiding the risk, reducing the negative effect or probability of the risk, or even accepting some or all of the potential or actual consequences of a particular risk.

2. Identify risks

Risk cannot be managed unless it is identified. Once the context of the business has been defined, the next step is to use this information to identify as many risks as possible.
The aim is to identify the risks that may affect, either negatively or positively, the objectives of the business and all its activity.

You will need to:

- Identify retrospective risks
- Identify prospective risks.

Identifying retrospective risks

Retrospective risks are seen in incidents or accidents that have occurred in the past. Retrospective risk identification is the most common way to identify risk and the easiest. A risk is easier to understand if its impact has already been experienced. It is also easier to quantify its impact and to evaluate the damage. There are many sources of information about retrospective risk including:

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

Identifying prospective risks

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

Identification should cover all risks, whether or not they are currently managed. The plan will be to record all significant risks and monitor the effectiveness of their treatment.

Methods for identifying prospective risks include:

- brainstorming with staff and external stakeholders
- researching the economic, political, legislative, technological and operating environment
- interviewing staff and clients to identify potential problems
- flow charting a process
- reviewing system design or preparing system analysis

Risk categories

Risk categories will help break down the process for prospective risk identification. It is important to remember that risk identification will be limited by the experience and perspective of those conducting the risk analysis. Problem areas and risks can be best identified by the use of reliable sources. There are many examples of risk in small business.

Risk categories should be considered one by one, providing a structured approach to risk identification. This enables greater focus on a particular category, stimulating thought, and increasing the opportunity of identifying a broader range of risks.

Common risk categories are:

- **Financial** – includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
- **Equipment** – extends to equipment used to conduct the business and includes everyday use, maintenance, depreciation, theft, safety and upgrades.
- **Organisational –** relates to the internal requirements of a business, extending to the cultural, structural and human resources of the business.
- **Security** – includes the business premises, assets and people. Also extends to security of company information, intellectual property, and technology.
- **Legal & regulatory compliance** – includes legislation, regulations, standards, codes of practice and contractual requirements. Also extends to compliance with additional ‘rules’ such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.
- **Reputation** – entails the threat to the reputation of the business due to the conduct of the entity as a whole, the viability of products/services, or the conduct of employees or others associated with the business.
- **Operational –** covers the planning, daily operational activities, resources (including people) and support required within the business that results in the successful development and delivery of products/services.
- **Contractual –** meeting obligations required in a contract including delivery, product/service quality, guarantees/warranties, insurance and other statutory requirements, non-performance.
- **Service delivery –** relates to the delivery of services, including the quality of service provided, or the manner in which a product is delivered. Includes customer interaction and after-sales service.
- **Commercial** – includes risks associated with market placement, business growth, product development, diversification and commercial success. Also to the commercial viability of products/services, extending through establishment, retention, growth of a customer base and return.
- **Project** – includes the management of equipment, finances, resources, technology, timeframes and people involved in the management of projects. Extends to internal operational projects, business development and external projects such as those undertaken for clients.
- **Safety –** including everyone associated with the business: individual, workplace and public safety. Also applies to the safety of products/services delivered by the business.
- **Workplace safety** - Every business has a duty of care underpinned by State and Federal legislation. This means that all reasonable steps must be taken to protect the health and safety of everyone at the workplace. Occupational health and safety is integrated with the overall risk management strategy to ensure that risks and hazards

are always identified and reported. Measures must also be taken to reduce exposure to the risks as far as possible. See Workplace Safety for more information.

- **Stakeholder management** – includes identifying, establishing and maintaining the right relationships with both internal and external stakeholders.
- **Client-customer relationship** – potential loss of clients due to internal and external factors.
- **Strategic** – includes the planning, scoping, resourcing and growth of the business.
- **Technology** – includes the implementation, management, maintenance and upgrades associated with technology. Extends to recognising critical IT infrastructure and loss of a particular service/function for an extended period of time. It further takes into account the need and cost benefit associated with technology as part of a business development strategy.

Given the complexity of risk management (and the rather long list above), the following four categories have been provided to simplify the types of risk an organisation and/or industry may face.

Risk to Physical Assets – By looking around your work environment, you will see physicality in terms of furniture and furnishings, equipment (such as computers and photocopiers), personal property and even landscaping. Here the risk comes from a range of sources including mishandling equipment due to a lack of training or poor maintenance resulting in injury

Risk to Financial Assets – These are the assets with monetary value such as cash, equities and contractual rights to receive funds into the future. Of course, burglary and theft are high on the list here but also embezzlement should be considered.

Risk to Human Assets – This is the realm of Workplace Health & Safety (aka OH&S) and significant emphasis is placed on risk minimisation here, especially given the potential for loss of life if risks are not managed appropriately. There is also the financial burden in cases of litigation (suing) and time off work for employees.

Risk to non-physical Assets – Although this may appear to be a catch-all category, non-physical assets covers the intangibles of a business and present a set of risks that have become very relevant with the advancement of technology. Information stored in an electronic environment or software developed for your business are valuable and to be protected. Instances of cyber-hacking have become a common problem and have created great concern for some business (especially those who store personal details such as credit card information).

Knowing your risk categories can assist you in risk planning and communicating risk information. They provide a structure for identifying risk and are often initially identified through a brainstorming exercise.

In addition, understanding categories assists business owners to select the best tools and techniques for risk identification and analysis. For example, if a particular risk category is technical in nature, the risk identification methodology used will involve significant research and collection of existing information about risk exposure. A risk category with a more strategic focus, such as commercial risk, may involve a structured workshop or exercise.

Risk Audit

Risk Audits are used to evaluate the effectiveness of the risk identification, risk responses, and risk management process as a whole.

Sample Template for a Risk Audit

Project Title: ______________________________ **Date Prepared:** _________________________

Project Auditor: __________________________ **Audit Date:** ____________________________

Risk Event Audit:

Event	**Cause**	**Response**	**Comment**
List the event from the risk register.	*Identify the root cause of the event.*	*Describe the response implemented.*	*Discuss if there was any way to have foreseen the event and respond to it more effectively.*

Risk Response Audit:

Event	**Response**	**Successful**	**Actions to Improve**
List the event from the risk register.	*List the risk response.*	*Indicate if the response was successful.*	*Identify any opportunities for improvement in risk response.*

Risk Management Process Audit:

Process	Followed	Tools and Techniques Used
Plan Risk Management	*Indicate if the various processes were followed as indicated in the risk management plan.*	*Identify tools and techniques used in various risk management processes whether they were successful.*
Identify Risks		
Perform Qualitative Assessment		
Perform Quantitative Assessment		
Plan Risk Responses		
Monitor and Control Risks		

Description of Good Practices to Share:

Describe any practices that should be shared for use on other projects. Include any recommendations to update and improve risk forms, templates, policies, procedures, or processes to ensure these practices are repeatable.

Description of Areas for Improvement:

Describe any practices that need improvement, the improvement plan, and any follow-up dates or information for corrective action.

3. Analyse risks

Risk Impact

You need to be able to evaluate the impact of each individual risk upon your business.

A simple method is to score the impact and probability of the risk and is commonly assessed on a scale of 1 to 5, where 1 and 5 represent the minimum and maximum possible impact of an occurrence of a risk (usually in terms of financial losses). However, the 1 to 5 scale can be arbitrary and need not be on a linear scale.

The probability of occurrence is likewise commonly assessed on a scale from 1 to 5, where 1 represents a very low probability of the risk event actually occurring while 5 represents a very high probability of occurrence. This axis may be expressed in either mathematical terms (event occurs once a year, once in ten years, once in 100 years etc.) or may be expressed in "plain English" – event has occurred here very often; event has been known to occur here; event has been known to occur in the industry etc.). Again, the 1 to 5 scale can be arbitrary or non-linear depending on decisions by subject-matter experts.

To help better understand this approach, two tools have been provided below.

Tools and Techniques

There are a number of tools and techniques available when undertaking a risk assessment… the most common being…

The ***Risk Register*** records details of all the risks identified at the beginning and during the life of the project, their grading in terms of likelihood of occurring and seriousness of impact on the project, initial plans for mitigating each high level risk, the costs and responsibilities of the prescribed mitigation strategies and subsequent results.

The ***Risk Impact/Probability Chart*** provides a useful framework that helps you decide which risks need your attention. The Risk Impact/Probability Chart is based on the principle that a risk has two primary dimensions:

1. Probability – A risk is an event that "may" occur. The probability of it occurring can range anywhere from just above 0 percent to just below 100 percent. (Note: It can't be exactly 100 percent, because then it would be a certainty, not a risk. And it can't be exactly 0 percent, or it wouldn't be a risk.)

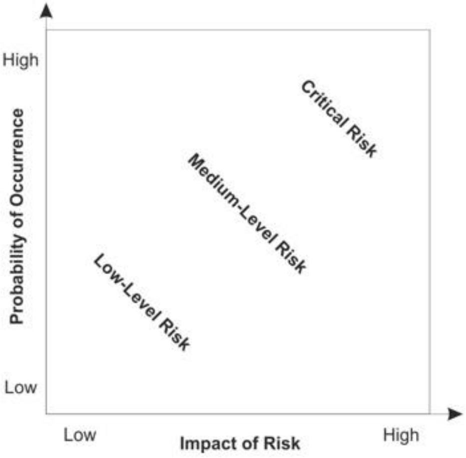
2. Impact – A risk, by its very nature, always has a negative impact. However, the size of the impact varies in terms of cost and impact on health, human life, or some other critical factor.

The chart allows you to rate potential risks on these two dimensions. The probability that a risk will occur is represented on one axis of the chart – and the impact of the risk, if it occurs, on the other.

You use these two measures to plot the risk on the chart. This gives you a quick, clear view of the priority that you need to give to each. You can then decide what resources you will allocate to managing that particular risk.

The basic form of the Risk Impact/Probability Chart is shown in figure 1, below.

Figure 1 – The Risk Impact/Probability Chart



The corners of the chart have these characteristics:

- Low impact/low probability – Risks in the bottom left corner are low level, and you can often ignore them.
- Low impact/high probability – Risks in the top left corner are of moderate importance – if these things happen, you can cope with them and move on. However, you should try to reduce the likelihood that they'll occur.
- High impact/low probability – Risks in the bottom right corner are of high importance if they do occur, but they're very unlikely to happen. For these, however, you should do what you can to reduce the impact they'll have if they do occur, and you should have contingency plans in place just in case they do.

- High impact/high probability – Risks towards the top right corner are of critical importance. These are your top priorities, and are risks that you must pay close attention to.

A more detailed approach (adapted from **http://www.mapl.com.au/risk/risk4.htm**) is as follows:

NOTE: Please use this method in analysing the risk in your second assignment task.

In developing a risk management process some of the useful tools include:

- Likelihood scale
- Consequences scale
- Level of risk scale
- Risk matrix
- Scale for evaluating risk

Likelihood scale

One key task in analysing risks is to estimate the likelihood of an event. To do this you will need a likelihood scale. Likelihood scales will need to be tailored to the risk management process.

An example of a likelihood scale is:

Level	**Likelihood**	**Description**
A	Almost certain	e.g. will occur at least once a year or more often
B	Likely	
C	Possible	
D	Unlikely	
E	Rare	
F	Very rare	
G	Almost incredible	e.g. once in 100,000 years

You will need to describe the likelihood in terms of a rate, for example, 'almost certain' could mean 'will occur at least once a year or more often' and 'almost incredible' could mean 'once in 100,000 years.

The likelihood scale and the way it is described may vary with the type of risk.

Consequences scale

It is useful to have a consequences scale for a given category or risk. An example of a consequences scale for 'health and safety' and 'financial risk' consequences are:

Level	Health and safety consequences	Financial (economic downturn) consequences
1.	No medical treatment required	No impact
2.	Minor medical treatment required	Min. impact – Issue addressed without notice
3.	Hospitalisation required	Some impact – noticed but structure remains
4.	Minor disability resulted	Minor impact – changes to organization structure
5.	Major disability resulted	Major impact – many redundancies
6.	Death resulted	Significant impact – possible sale of business
7.	Multiple deaths resulted	Catastrophic – Bankruptcy

The consequence scale will vary with each type of risk.

Level of risk scale

A scale for the level of risk is very useful for prioritising risks. For example.

Level of risk
Very high
High
Medium
Low
Very low
Negligible

Level of risk matrix

The level of risk is the combination of the consequences and the likelihood for a specific risk.

Examples of low risks include:

- An event that is likely to occur but has minimal consequences
- An event that is extraordinarily unlikely to occur but has moderately severe consequences.

Examples of high risks include:

- An event that is likely to occur and has moderately severe consequences
- An event that is extraordinarily unlikely to occur but has catastrophic consequences.

The following table is a risk matrix and shows the relationship between *Likelihood*, *Consequence* and *Level of risk*.

In the table:

- A1 is certain to happen but has small consequences so is a low risk.
- A7 is certain to happen and has very large consequences so is a very high risk

- G1 is very rare and has small consequences so is a negligible risk
- G7 is very rare but has large consequences so is a medium risk.

	Likelihood (Certain to very rare)						
Consequence (small to large)	A	B	C	D	E	F	G
1	Low	Low	Low	Low	Low	Very Low	Negligible
2	Medium	Medium	Medium	Low	Low	Very Low	Very Low
3	High	Medium	Medium	Medium	Low	Low	Very Low
4	High	High	Medium	Medium	Medium	Low	Very Low
5	Very high	High	High	Medium	Medium	Medium	Low
6	Very high	Very high	High	High	Medium	Medium	Medium
7	Very high	Very high	Very high	High	High	Medium	Medium

Specific risks can be located on the matrix. Risks can be compared with each other so they can be prioritised for treatment.

For example:

- Risk of fire burning a building down could be located at E7 (rare but very significant consequences and so a high risk
- Violence during home visits could be located at B4 (likely with serious consequences and so a high risk).

Scale for evaluating risk

When evaluating the level of risk, i.e. deciding whether it is an acceptable risk or not it is useful to have a scale on which to base judgments, for example:

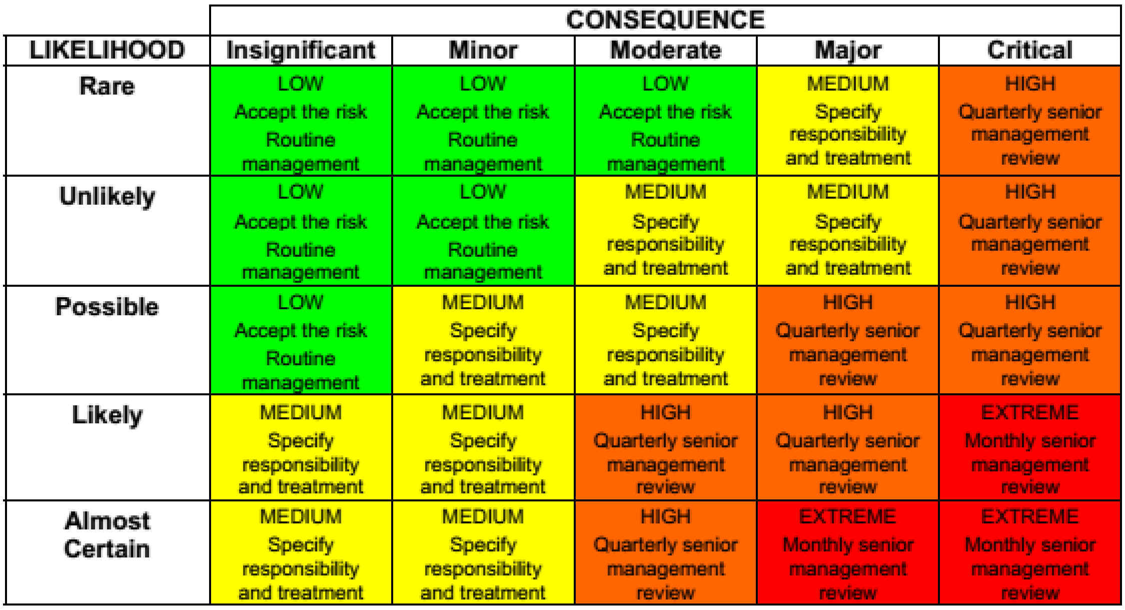
	Level of risk	**Description**
i)	Broadly acceptable level of risk	The situation is not of concern
ii)	Best achievable level of risk	Achieved with best practice
iii)	As low as reasonably practicable(ALARP)	Must be achieved (minimum standard)
iv)	Generally intolerable level of risk	Not tolerated

For a given risk one will need to make a judgment of where the cut off points are for levels i) to iv) in the table. When is an occupational health and safety risk broadly acceptable? When is it intolerable? What is the level or risk the organisation wants to achieve? As low as reasonably practicable?

Risk Treatment

At the risk of muddying the waters, the next example of a risk matrix takes a further step in the overall ‘risk management’ process and includes ‘risk treatment’.

Detailed risk matrix example



	CONSEQUENCE				
LIKELIHOOD	**Insignificant**	**Minor**	**Moderate**	**Major**	**Critical**
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost Certain	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

As you have no doubt noticed, this matrix has some subtle differences to the example addressed in the previous section. But most importantly, it provides us with a treatment level. Risks that are determined green require routine management whereas risk that are red must have continual 'monthly' monitoring and preferebly by Senior Management.

Using this matrix (or the ones presented earlier), an action plan can be developed and implemented ensuring that not only is the risk analysed and categorised according to its likelihood and consequences, but when the risk should be reviewed and by whom.

Helpful websites
http://www.iso.org/iso/home/standards/iso31000.htm

http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/721/Managing-risks-to-health-fact-sheet.pdf

https://success.clarizen.com/hc/communities/public/questions/203996208-Risk-Management-Useful-Tools-and-Techniques

https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf