Risk management

About this free course

Intellectual property

Contents

Introduction and guidance

Introduction and guidance

Welcome to this free course, *Risk management*. The course lasts eight sessions, with approximately three hours of study each session. You can work through the course at your own pace, so if you have more time one session there is no problem with pushing on to complete another session's study.

You will be able to test your understanding of the course through the interactive quizzes, of which Sessions 4 and 8 will provide you with an opportunity to earn a badge to demonstrate your new skills. You can read more on how to study the course and about badges in the next sections.

After completing this course, you will be able to:

- identify and understand the risks faced by organisations
- assess and measure the impact of risks on organisations
- understand the different ways that risks can be managed or mitigated
- understand how organisations can apply 'Enterprise Risk Management'
- understand the importance of effective monitoring and reporting of risks.

Moving around the course

In the 'Summary' at the end of each session, you can find a link to the next session. If at any time you want to return to the start of the course, click on 'Course content'. From here you can navigate to any part of the course. Alternatively, use the session links at the top of every page of the course.

It's also good practice, if you access a link from within a course page (including links to the quizzes), to open it in a new window or tab − that way you can easily return to where you've come from without having to use the back button on your browser.

The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations for the course before you begin, in our optional start-of-course survey. Participation will be completely confidential and we will not pass on your details to others.

What is a badged course?

While studying *Risk management* you have the option to work towards gaining a digital badge.

Badged courses are a key part of The Open University's mission *to promote the educational well-being of the community*. The courses also provide another way of helping you to progress from informal to formal learning.

To complete a course you need to be able to find about 24 hours of study time, over a period of about 8 sessions. However, it is possible to study them at any time, and at a pace to suit you.

Badged courses are all available on The Open University's OpenLearn website and do not cost anything to study. They differ from traditional Open University courses because you do not receive support from a tutor. But you do get useful feedback from the interactive quizzes.

What is a badge?

Digital badges are a new way of demonstrating online that you have gained a skill. Schools, colleges and universities are working with employers and other organisations to develop open badges that help learners gain recognition for their skills, and support employers to identify the right candidate for a job.

Badges demonstrate your work and achievement on the course. You can share your achievement with friends, family and employers, and on social media. Badges are a great motivation, helping you to reach the end of the course. Gaining a badge often boosts confidence in the skills and abilities that underpin successful study. So, completing this course should encourage you to think about taking other courses.

How to get a badge

Getting a badge is straightforward! Here's what you have to do:

- read each session of the course
- score 50% or more in both of the two badge quizzes in Session 4 and Session 8.

For all the quizzes, you can have three attempts at most of the questions (for true or false type questions you usually only get one attempt). If you get the answer right first time you will get more marks than for a correct answer the second or third time. Therefore, please be aware that for the two badge quizzes it is possible to get all the questions right but not score 50% and therefore be ineligible for the badge on that attempt . If one of your answers is incorrect you will often receive helpful feedback and suggestions about how to work out the correct answer.

For the badge quizzes, if you're not successful in getting 50% the first time, after 24 hours you can attempt the whole quiz, and come back as many times as you like.

We hope that as many people as possible will gain an Open University badge – so you should see getting a badge as an opportunity to reflect on what you have learned rather than as a test.

If you need more guidance on getting a badge and what you can do with it, take a look at the OpenLearn FAQs. When you gain your badge you will receive an email to notify you and you will be able to view and manage all your badges in My OpenLearn within 24 hours of completing the criteria to gain a badge.

Session 1: Living in a world of risk

Introduction

In this session you will explore risk in the world around you, and be introduced to risk management as a professional discipline. You will see everyday examples of risk, as well as case studies that highlight the causes and impacts of risk in businesses that you may have already seen in the news.

This session includes:

- what is risk?
- examples of the 'real world' impacts of risks
- risk-based decision making
- a brief review of the historical background to the emergence of risk management by organisations
- an introduction to common risk management standards.

By the end of this session, you should be able to:

- explain what a risk is (and its different definitions)
- understand the importance of managing risk
- understand how risk-based decisions are part of everyday life.

The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations for the course before you begin, in our optional start-of-course survey. Participation will be completely confidential and we will not pass on your details to others.

Now begin Session 1.

1 What do we mean by risk?

There are different definitions of risk. The dictionary definition is:

> A situation involving exposure to danger.
>
> Oxford English Dictionary (OED)

However, there are other definitions of risk:

> A situation involving exposure to danger, the possibility that something unpleasant or unwelcome will happen, a person or thing regarded as a threat or likely source of danger, a possibility of harm or damage against which something is insured, a person or thing regarded as likely to turn out well or badly in a particular context or respect, the possibility of financial loss.
>
> OED source

> Risk: effect of uncertainty on objectives.
>
> > Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
> >
> > Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.
> >
> > Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
>
> ISO 31000 (2018)

> An uncertain event or set of circumstances that, should it occur, will have an effect on achievement of one or more objectives.
>
> Association of Project Managers (APM)

As you study this course you will find that there are differences – often quite subtle – in the way that individual organisations define various risks. Such differences have become less common in recent years with the adoption of internationally recognised standards for risk management – particularly those standards laid down by the International Organization for Standardization (ISO) in its ‘ISO 31000’ directive and those laid down by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Watch Video 1 to learn from the experts what ‘risk’ means.

Video content is not available in this format.

Video 1 What does ‘risk’ mean?

2 The importance of managing risk

Now watch Video 2 from the experts on why risk management is important.

Video content is not available in this format.

Video 2 Why is risk management important?

Risk management is considered so important that many professional disciplines are encouraged to manage risks as part of their professional code.

As a good example take a look at the ‘Guidance on Risk’ set out by the UK’s Engineering Council (2011). The guidelines are as follows:

- Apply professional and responsible judgement and take a leadership role.
- Adopt a systematic and holistic approach to risk identification, assessment and management.
- Comply with legislation and codes, but be prepared to seek further improvements.
- Ensure good communication with the others involved.
- Ensure that lasting systems for oversight and scrutiny are in place.
- Contribute to public awareness of risk.

Indeed all UK companies listed on the Stock Exchange are expected to apply effective risk management as part of their compliance with the UK Corporate Governance Code.

3 Risk in everyday life

Risk is all around us. We take risks when we eat and drink, travel, enjoy hobbies, invest money and do many other things. Risk may be something you think about a lot when doing any of these things, or it may be something that never enters your mind. Take a look at the activity below and try to describe your approach to risk in these areas.

Activity 1 Considering risks in everyday life

Allow approximately 10 minutes

Interactive content is not available in this format.

Interactive content is not available in this format.

Interactive content is not available in this format.

Hopefully you will have taken the opportunity to think about your and others' personal approach to risk, known as personal risk appetite, and appreciate how people can have different approaches to risk in different parts of their lives. For example, someone who skydives and likes travelling solo around the world may not like a lot of risk in their financial investments. But it is also true that some people are big risk-takers most of the time, and take a lot of risks generally, while some are risk-averse and avoid taking risks as much as possible.

Getting the balance right between when and how much risk to take can often be tricky. Taking too many risks, or one really big risk in a personal hobby may mean we get injured. In personal investments, taking more risks could be a good way to earn more money, but it is also a good way to lose money – balance is the key. In pensions, for example, young people are often encouraged to take slightly more risk in their investments, but people closer to retirement are advised to be risk-averse and take as little risk as possible.

4 Managing risk: a brief history of risk management

The word ‘risk’ is thought to derive either from the Arabic word ‘risq’ or the Latin word ‘risicum’. The two possibilities quite neatly combine to give us the meaning for the English term in this context. The Latin word originally referred to the challenge presented to seafarers by a barrier reef and so implied a possible negative outcome. The Arabic word, on the other hand, implies ‘anything that has been given to you (by God) and from which you draw profit’ and has connotations of a potential beneficial outcome.

A twelfth-century Greek derivative of the Arabic risq related to chance outcomes in general with no positive or negative implications. The definitions above can be combined to derive a concept of risk as being ‘an uncertain future outcome that will improve or worsen our position’.

There are two implied elements about this definition that should be noted:

- it is probabilistic – the likely outcome can be assessed, but is not known with certainty
- it is two-sided – the outcome may be favourable or adverse.

Strictly speaking, the ‘favourable or adverse’ aspect of the definition does not necessarily imply ‘symmetry’, where the ‘upside’ and ‘downside’ are of an exact equivalent magnitude. Indeed in many risk situations the outcomes may be skewed – for example, more ‘downside’ than ‘upside’.

The French word ‘entrepreneur’ first appeared in the French dictionary in 1723 to describe a person who organises and operates a business by taking a financial risk. Good risk management isn’t about not taking any risks: it is about taking the right risks where there is an appropriate reward. It is about protecting assets and adding value.

Risk is all around us, and always has been. In that regard it can be considered to have always been a part of human life, and even as a profession its roots go back a long time. Some forms of mutual aid existed in ancient societies and these are considered the forerunners of modern insurance companies, which are fundamentally reliant on risk-based assessments and decisions. Ideas of modern professional ‘risk management’ as a separate discipline grew from the insurance companies of the mid-twentieth century who sought more control over the risks they were insuring against, and branched out into other areas of loss-prevention in their companies, thereby reducing the levels of risk their own businesses faced in other ways than just insurance.

Today risk management is well recognised and widely practised and it takes many different forms. Some of this is driven by regulation – for example, Section 414C of the UK Companies Act, which is applicable to all companies incorporated in the UK, regardless of size, requires that ‘The Directors’ strategic report must contain a description of the principal risks and uncertainties facing the company’. Consequently, many organisations have recognised that value can be derived by managing their risks, reducing the probability of downsides and increasing the probability of upsides. In fact most organisations today have a Chief Risk Officer (or similar role) and many senior roles are, in large part, accountable for managing an organisation’s biggest risks. The Institute of Risk Management (IRM) indicates some of the potential careers open to risk professionals (Institute of Risk Management).

5 Business impacts

When risks do happen the impact can often have a serious effect on a business. Take a look at these case studies that describe some impacts of businesses getting risk management decisions wrong in different ways.

Remember to open these links in a new tab (right-click on the link and click on the option to open the document in a new tab or window) so you can look at them in relation to the course, and get back to the course easily.

- Piper Alpha timeline (Extended Version)
- Piper Alpha timeline (Day of explosion)
- Kodak timeline

Now take a look at Video 3, which is the Rolls-Royce timeline.

Video content is not available in this format.

Video 3 Rolls-Royce timeline (Please pause the video when you need to, to ensure you can read through all of the text on-screen. A transcript is also available.)

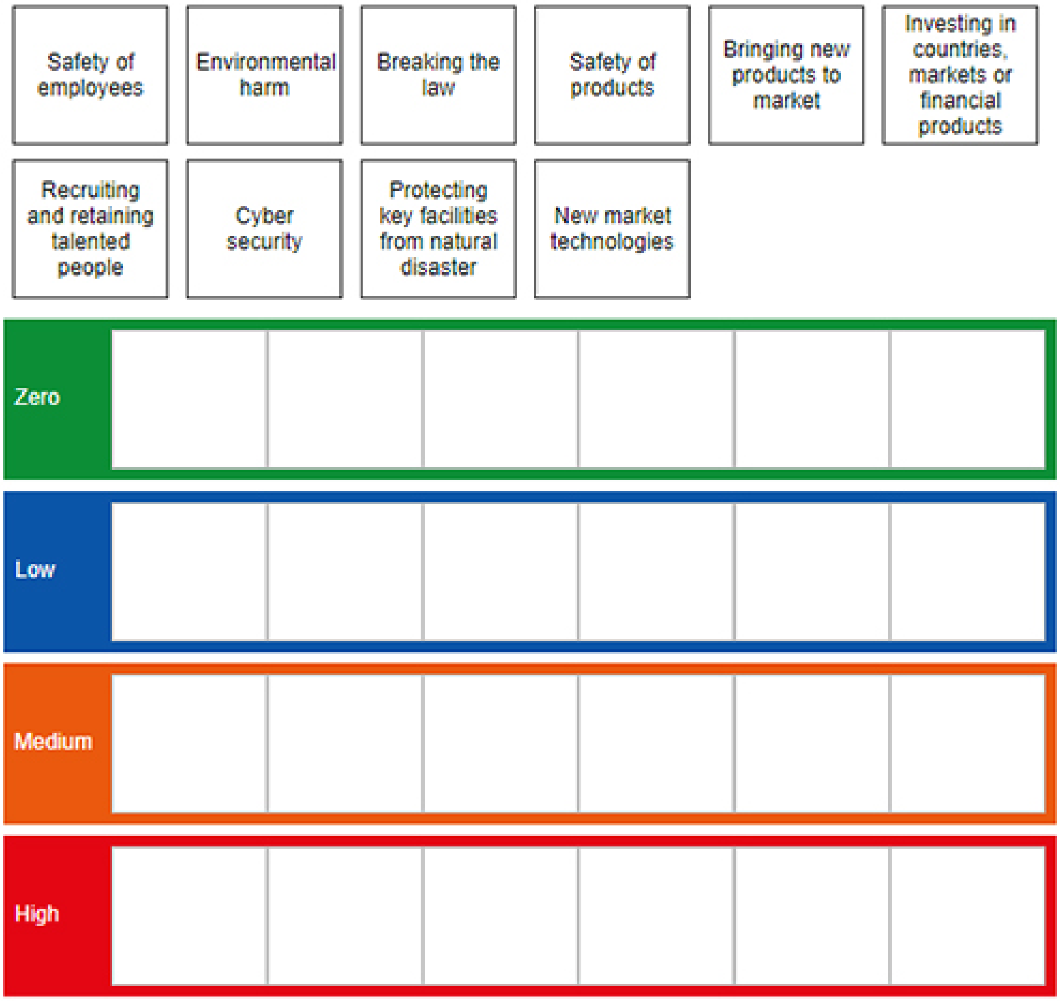
Now have a go at Activity 2.

Activity 2 Risks to scale

Allow approximately 10 minutes

Click on the link below to load this interactive activity. Place these risks on the scale provided based on your work experiences of taking risks. For example if you think that organisations should normally aim to make an aspect of their business (say, cyber security) ‘low risk’ then select ‘low’.

Interactive content is not available in this format.



Safety of employees

Environmental harm

Breaking the law

Safety of products

Bringing new products to market

Investing in countries, markets or financial products

Recruiting and retaining talented people

Cyber security

Protecting key facilities from natural disaster

New market technologies

Zero

Low

Medium

High

Discussion

Table 1

Zero	Low	Medium	High
	Breaking the law	Investing in volatile countries, markets or financial products	New market technologies
	Safety of employees	Recruiting and retaining talented people	
	Environmental harm	Bringing new products to market	
	Safety of products		
	Cyber security		
	Protecting key facilities from natural disaster		
	Changes to regulations, tariffs or access to markets caused by governments		

- Zero: While you might want ‘Zero risk’ for something (e.g. a zero risk attitude to employee safety) in practice the only way this can be achieved is to remove the risk completely, therefore in many cases achieving ‘zero risk’ is impossible.
- Desire to take little risk: Although ‘zero risk’ is impossible, there are many areas where risk exposure should be minimised. These would typically be risks where we could harm people or the environment or break laws or regulations. However, there may be critical business activities that should not be exposed to high levels of risk: protecting facilities and IT might also be areas where risks are not wanted.
- Ability to accept some risk: There will then be areas where some risk is acceptable in order to achieve goals. When investing in countries it might be desirable to operate in areas with high growth and easy access to the necessary resources, but it would be considered an unacceptable risk to operate in areas with high corruption and low ethical standards. Similarly in recruiting and retaining talent, taking the steps to obtain the best people is key but exploiting individuals or using labour practices that might be viewed as unfair would be an unacceptable risk.
- Accepting high risks: There will be some areas where the company is prepared to take high risks. In bringing a new product to market, especially if the product is essential to the success of the company, the company may be willing to put a vast amount of investment behind the project. Similarly in investing in new technology, if a company believes the technology is a ‘game changer’ it may try to ensure significant capital is available, the stakes for not doing so may be too high not to invest (see Rolls-Royce or Kodak earlier).

Throughout this activity it is important to recognise that risks do not occur in isolation. This means that a company will have differing risk appetites across and even within its activities. For example it may have a high-risk appetite for introducing new technology, so will do everything it can to bring it to market, but because it has a low-risk appetite for breaking the law, ‘doing everything it can’ excludes breaking any laws.

6 Understanding and expressing risk

You can see from the case studies that a clear understanding of risk is important. Kodak did not appreciate the size of the risks that digital photography posed to them; the owners of Piper Alpha either did not appreciate or ignored the operating and safety risks of cost-cutting; and Rolls-Royce did not factor the risk of rising costs into their fixed-price contracts. But how best to understand and express these risks? This question will be addressed throughout the course, but for now, consider the following question:

Which is riskier – handling explosives on a building site, or driving to work?

More people die in road accidents than from explosions, so is driving the riskier activity? There are many things to consider here. One important thing to think about in this example would be the accident rate per activity undertaken, which gives you a better understanding of how likely you are to suffer an accident doing either activity. This is an assessment of probability.

However, it still does not tell the whole story. Imagine if the accident rate per activity were exactly the same for both activities. Would you rather suffer an accident while driving or while handling explosives? Your answer to this question concerns the impact of the risk event. The impact of an accident while handling explosives is more likely to be serious (probably death) than an accident while driving, which could lead to many comparatively minor consequences. To fully understand the risks involved you need to understand both the probability and the impact of the risk. This will be revisited when discussing assessments later in the course.

7 The risk management process

There are a number of formal risk management processes, which will be covered in more detail in Session 2. They are typically written at a high level and it is recommended that the detailed approach followed is adapted to fit the task. However, there is a set of commonly recognised process steps. In this case, and for the rest of this module, the International Organization for Standardization (ISO) 31000:2018 standard will be referred to.

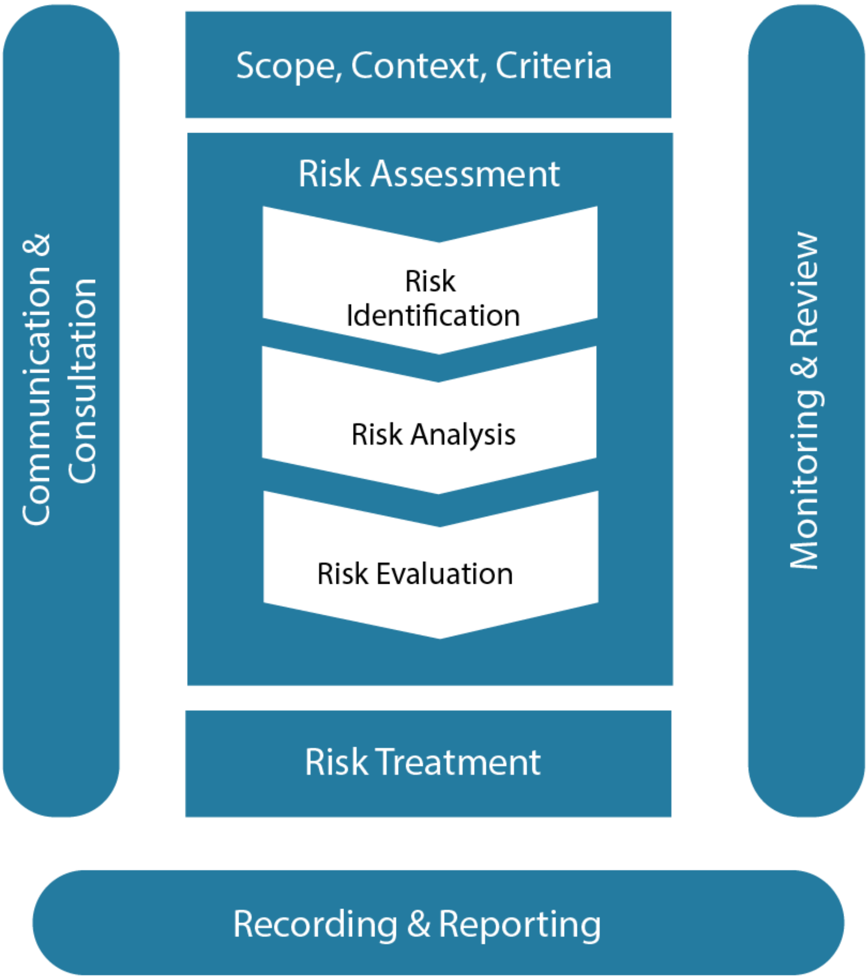


Figure 1 ISO 31000 diagram

The process is iterative and when performed properly has multiple feedback loops between the different process steps. Unlike many processes, the risk process can operate at any (and all) levels of an organisation, works for any activity and applies to all types of risk. You will explore each of these steps in more detail in the coming sessions.

Box 1 COSO and ISO 31000

There are many similarities between COSO and ISO 31000. They share many common principles. Both focus on identifying, assessing and treating risks and monitoring them on a regular basis. They also both focus on the importance of good governance and culture to enable good risk management.

The main differences stem from their backgrounds. COSO evolved from a focus on financial reporting, whereas ISO evolved from a quality management system focus – so has more of a process or quality system focus.

COSO therefore has a greater focus on strategic risks and loss prevention (i.e. predominantly threat (downside) risks). It is aimed at the board (and senior leaders) and focuses on controls as the main treatment activity.

ISO on the other hand takes a much wider scope, looking to work for all risks (threat and opportunities) at all levels of an organisation. It looks to understand the risks to all objectives.

The terminology used is similar (but not the same) so firms looking to apply both approaches should understand the differences and potential conflicts between the two.

8 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 1 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

9 Summary of Session 1

You are almost at the end of Session 1 so it's a good time to recap what you've covered and take a look at what you will cover in the rest of the course.

The main learning points that have been covered in this session are:

- what is risk?
- examples of the 'real world' impacts of risks
- risk-based decision making
- a brief review of the historical background to the emergence of risk management by organisations
- an introduction to common risk management standards.

You have seen that there are different definitions for risk, but the one typically used in business is 'the effect of uncertainty on objectives'.

You have looked at some examples of where risks have happened (from now on these will be called 'incidents') and the impact that this can have. You have seen that the ultimate consequence of bad risk management can be companies going out of business, catastrophic damage to the environment and even people losing their lives.

Because of these consequences certain professional bodies require their members to consider risks, and corporate governance codes place an onus on a company board to understand and manage risk.

You have taken a look at some of the day-to-day decisions people take that involve risk and noted that different people are prepared to take different levels of risks. This concept will be revisited in future sessions when you look at 'risk appetite' (the level of risk people are prepared to accept).

Looking forward: In future sessions you will dig more deeply into the different steps in the risk management process; you'll explore ways in which to systemise this and build it in to the day-to-day running of a business; you'll look at some of the behavioural factors that can cause things to go wrong; and you'll hear from experts on their real-world risk management experiences.

Session 2: Establishing the context

Introduction

In Session 1 you started learning about risk management. It defined what is meant by 'risk', and discussed why managing risk is important, what happens when risk is well managed and what can happen when it isn't. You learned about risk in everyday life and how different people choose to take different levels of risk.

In this session you will build on last session's ideas by exploring 'Enterprise Risk Management' and start to think about applying risk management in an organisation. You will determine prerequisites for risk management, explore first steps, and focus on how to set a scope and framework for your risk management activities.

By the end of this session, you should be able to:

- explain what Enterprise Risk Management is
- understand risk appetite
- describe the components of a risk management framework
- produce a document that sets out the scope and context for activity (a Risk Management Plan, or RMP).

Now begin Session 2.

1 Enterprise Risk Management (ERM)

In Session 1, you considered big risks involved with events that had happened and had serious impacts on the affected organisations. For a long time, businesses have managed specific types of risks. A manufacturing firm would typically look at health and safety risks, a bank its credit risks and a hospital the risks to patient safety. But doing a good job of managing one set of risks does not mean that the organisation has a good grip on managing all of its risks: it does not mean that all of the risks to the 'enterprise' are being managed.

Increasingly organisations have recognised the value of understanding and managing all of the risks that they face – this approach is called 'Enterprise Risk Management'. But what is meant by 'Enterprise Risk Management' (ERM)?

In response to a number of high-profile corporate failures (Enron, WorldCom, etc.) regulators have introduced standards that apply to large listed companies. The United States set up a commission (the Treadway Commission) which subsequently published guidance on the essential elements of risk management. This is commonly called COSO (Committee of Sponsoring Organizations).

This activity will help you to understand COSO's definition of ERM.

Activity 1 COSO framework

Allow approximately 10 minutes

Look at the text from COSO and use the drop-down options to fill in the correct words.

Interactive content is not available in this format.

Now watch this video about how experts define ERM.

Video content is not available in this format.

Video 1 How do experts define Enterprise Risk Management?

2 Risk appetite

One key concept that is central to risk management – and which is referred to by COSO – is ‘risk appetite’. The appetite that an organisation has for risk reflects, among other things, its financial strength and also its culture for taking risks. Take a look at Video 2 to get an understanding of the factors that determine risk appetite.

Video content is not available in this format.

Video 2 Overview of risk appetite

Now watch Video 3 to learn what risk appetite means for experts.

Video content is not available in this format.

Video 3 What does risk appetite mean?

3 Why is an Enterprise Risk Management framework needed?

A key part of ERM is identifying how much risk you are prepared to take (your risk appetite). You have also seen that ERM is a process that requires board involvement and the involvement of other people in an organisation. Enterprise Risk Management reaches strategic, compliance, financial reporting and operational aspects across an organisation.

This wide-ranging scope of ERM means that many companies find it helpful to design a framework, wherein the different elements are complementary and supportive of one another. In the best organisations, risk management is built in to other activities rather than being a bolt on, and so their ERM framework is interwoven with other elements of the way they do business.

4 The components of a company-wide ERM framework

An ERM framework covers the whole organisation. It includes: process, tools, governance, measures and people, all underpinned by an appropriate culture. Take a look at the elements of an ERM framework.

First take a look at Video 4 and hear what the experts say should be in a risk management framework.

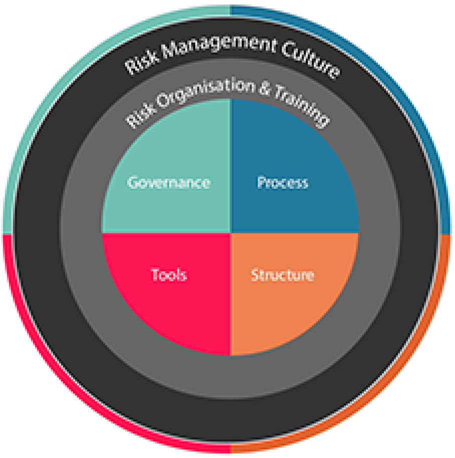
Video content is not available in this format.

Video 4 What would be in a risk management framework?

Now have a look at Video 5, which covers an Enterprise Risk Management framework.

Video content is not available in this format.

Video 5 An Enterprise Risk Management framework



Before moving on to the next section you should recognise there is no ‘one right way’ to do risk management and most of the standard guides and codes refer to the need to ‘customise’ the approach to fit each organisation. The example given in the next two sections relates to practice used in Rolls-Royce, but these will not necessarily work in whole or even in part in other organisations.

5 The Risk Management Plan (RMP)

This framework will be looked at again in later sessions, but for now consider a specific approach for the first risk management activity. The first task in setting up risk management for any new activity is to create a document called a ‘Risk Management Plan’ (RMP). The purpose of an RMP is to set a standard and ensure consistent and seamless application of risk. This step, referred to as Scope, Context, Criteria in the ISO 31000 risk management process, sets the tone for what will follow.

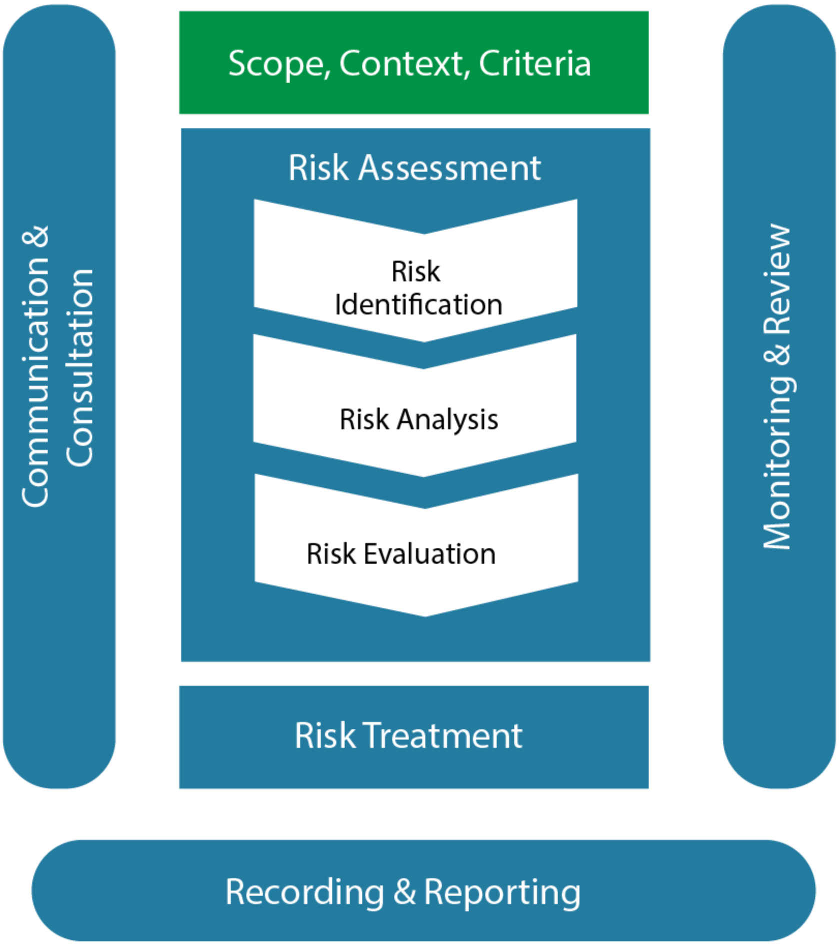


Figure 1 ISO 31000 diagram – Scope, Criteria, Context

RMPs can exist for small activities all the way up to risk activities for an entire organisation. An organisation-level RMP will be partly driven by the regulatory requirements, which will define some minimum requirements for governance and reporting. Listed companies in certain countries have to comply with corporate governance codes which may set a minimum requirement for the things the risk management system needs to cover. Corporate governance requirements are discussed further in Session 7.

6 The key components of an RMP

Context and Scope: In many cases, the scope of the activities needing risk management will be broadly defined by something else – a project plan, a set of objectives for a team, or the work of an entire business. In any of these cases, it is still worth referencing the scope of the activities in the RMP, just so it is clear. In doing so, you may also need to consider:

- Is there a budget for these activities? If so, what does the budget cover?
- What activities are you responsible for?
- What decisions do you have the authority to make (and which are outside your authority)?
- What is not included?

At this point it may help to visualise a governance structure, or a work breakdown structure.

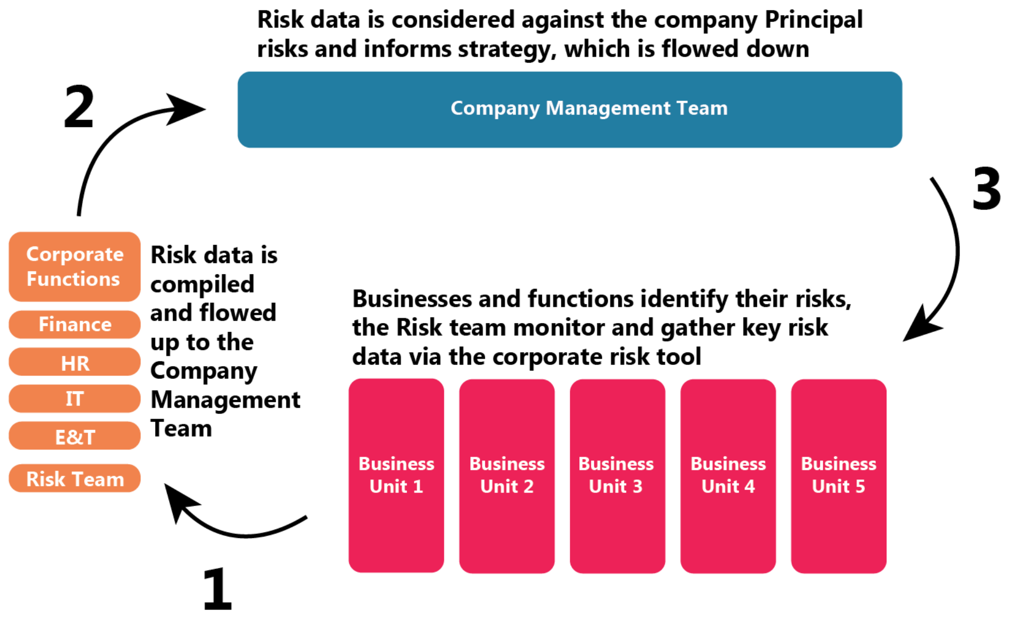

Risk data is considered against the company Principal risks and informs strategy, which is flowed down
2
Company Management Team
3
Corporate Functions
Finance
HR
IT
E&T
Risk Team
Risk data is compiled and flowed up to the Company Management Team
Businesses and functions identify their risks, the Risk team monitor and gather key risk data via the corporate risk tool
Business Unit 1
Business Unit 2
Business Unit 3
Business Unit 4
Business Unit 5
1

Figure 2 A governance structure used to scope a risk management activity

Table 1 Key components of an RMP

Key components	Explanation
Roles and responsibilities	Who is accountable for risk management and are there any delegations of this accountability?
Risk reviews	How will they be carried out? When will risk reviews happen? Who is part of them? How will the output of them be communicated and to whom? Beyond that, levels depend on the size and complexity of the business or function.

Risk scoring scheme	The units of measurement and ‘graduations’ (these are, in effect, gradations of severity of a risk) by which risks will be measured and categorised. This is often referred to as a risk matrix or a Probability and Impact Diagram (PID). These concepts will be explored in greater detail in Session 4.
Communication and reporting	Understanding the organisational structure within the relevant business area is key to locating superseding RMPs and risk registers which you will need for escalations. But it is not just a matter of locating the superseding RMPs: it is also crucial to examine them and, in particular, to identify what level of risk(s) trigger an escalation of a risk management issue to these superseding RMPs.
Other logistical considerations	The RMP states where your risk register will be located.

While this may seem like a lot of information, in reality for many areas much of the work is defined once in the organisation RMP and reused within the organisation. This is because the risk requirements flow down from the centre of the organisation to business units and functions, and from business units to sub-business units and projects, with lower levels expected to comply with the requirements set out in the higher-level documents. This means that typically only those things that are different need to be described, meaning the RMPs are often quick and easy to prepare. For example, consider the RMP example below.

Remember to open this link in a new tab so you can look at it in relation to the course, and get back to the course easily. RMP example

7 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 2 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

8 Summary of Session 2

In Session 2 you have started to explore what risk management involves in an organisation. You have explored Enterprise Risk Management (ERM) and looked at what is contained in a risk management framework.

You have been introduced to the key concept of risk appetite, and considered how risk appetite is used in an organisation to define how much risk an organisation is prepared (or able) to take to achieve its objectives.

Finally, you looked at planning risk management activities, in particular who needs to be involved and how Risk Management Plans (RMPs) are created to ensure the right information is documented and the right activity takes place.

The main learning points that have been covered in this session are:

- Enterprise Risk Management
- risk appetite
- the components of a risk management framework
- the scope and context for a Risk Management Plan, or RMP.

Session 3: Risk identification

Introduction

Watch Video 1, which covers when to start risk management.

Video content is not available in this format.

Video 1 When to start risk management

In Session 1 you looked at some definitions of risk. Revisit these for a moment:

> A situation involving exposure to danger, the possibility that something unpleasant or unwelcome will happen, a person or thing regarded as a threat or likely source of danger, a possibility of harm or damage against which something is insured, a person or thing regarded as likely to turn out well or badly in a particular context or respect, the possibility of financial loss.
>
> OED source

So, as discussed in Session 1, a risk must have some degree of uncertainty. In the risk process identifying that uncertainty takes place in the risk identification phase:

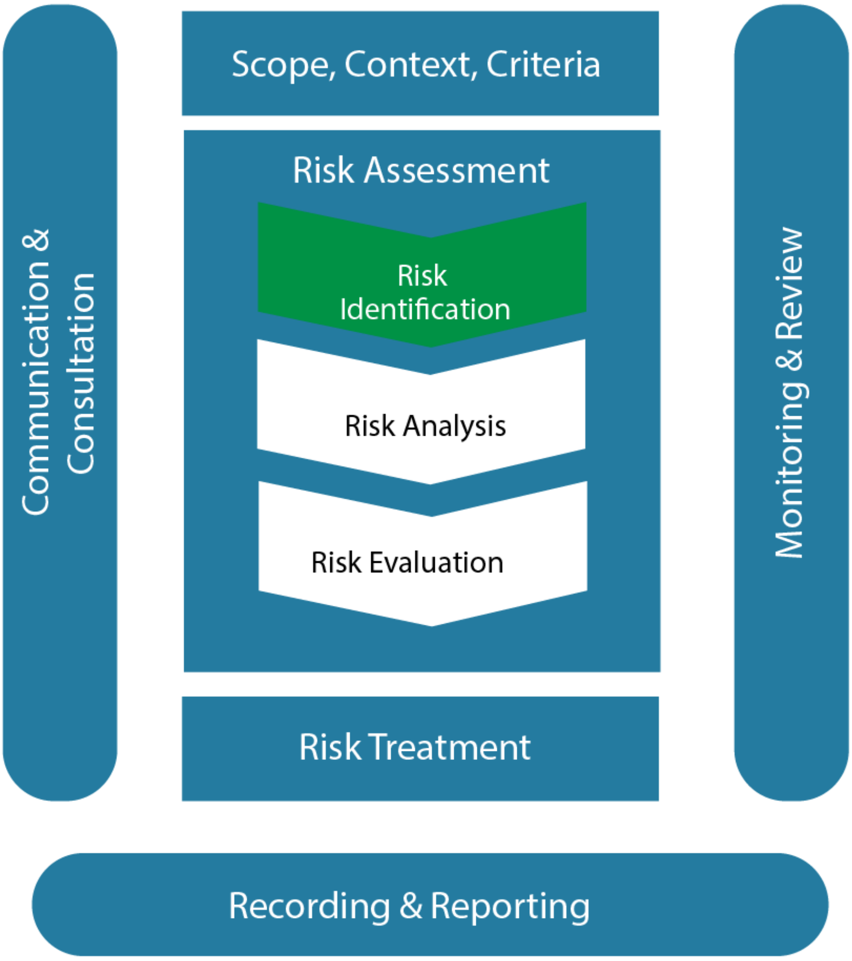


Figure 1 ISO 31000 diagram – risk identification

Activity 1 Uncertainty statements

Allow approximately 10 minutes

For each question below select the statement which relates to a current business uncertainty (as opposed to a fact or a concern about a possible emerging risk).

Question 1:

○ In the last 5 years a supplier has only had a delivery issue once and this was due to factors outside of their control.

○ There is a possibility that a key supplier may fail, leading to raw materials not being supplied.

○ Cyber actors are increasingly looking outside of their primary targets for ways in, including the supply chain.

Question 2:

○ A competitor has just launched a new product ahead of us that is more advanced and it looks like it uses our intellectual property.

○ At some point a technology company will create an offering that will side step our main product range and could leave us as a niche player.

○ Because of strong competition the business might not win the contract with a big customer.

Question 3:

○ Our main warehouse is built on a flood plain, there have been two floods in the town in the last 20 years.

○ A fire could break out in one of our facilities, if we don't take the right precautions.

○ Automation of the workforce is something we will have to manage in the next 10–20 years.

Question 4:

○ There is a chance that the government may introduce new regulations that would limit how the company could trade.

○ There has been a coup in a country we operate in, leading to civil unrest in major towns and cities.

○ Climate change will impact the market for our product, how we produce and where we can sell.

Question 5:

○ Sometimes our sales team make mistakes and this, if not properly managed, can lead to errors in the order processing system.

○ There is an error in our order fulfilment system that leads to some lines going to the wrong dispatch centre; we don't fully understand the scale of this yet.

○ The internet will change how our customers place orders in the future.

Answer

	These were the uncertainties (simple risk statements) all focused around tangible activities that the company presently faces	**These were 'facts' that related to 'incidents' (either recent or historic) that may require action or give an insight into risks that may need to be managed**	**These are sometimes referred to as 'concerns' that are potential areas for risk where the concepts are broad and the company may want to undertake further work to understand the risks faced. These are often referred to as emerging risks. (See horizon scanning in Session 8.)**
Question 1	There is a possibility that a key supplier may fail, leading to raw materials not being supplied.	In the last 5 years a supplier has only had a delivery issue once and this was due to factors outside of their control.	Within the next 10 years we will have to shift our supply chain away from the current raw materials to remain cost competitive.

Question 2	Because of strong competition the business might not win the contract with a big customer.	A competitor has just launched a new product ahead of us that is more advanced and it looks like it uses our intellectual property.	At some point a technology company will create an offering that will side step our main product range and could leave us as a niche player.
Question 3	A fire could break out in one of our facilities if we don't take the right precautions.	Our main warehouse is built on a flood plain, there have been two floods in the town in the last 20 years.	Automation of the workforce is something we will have to manage in the next 10–20 years.
Question 4	There is a chance that the government may introduce new regulations that would limit how the company could trade.	There has been a coup in a country we operate in, leading to civil unrest in major towns and cities.	Climate change will impact the market for our product, how we produce and where we can sell.
Question 5	Sometimes our sales team make mistakes and this, if not properly managed, can lead to errors in the order processing system.	There is an error in our order fulfilment system that leads to some lines going to the wrong dispatch centre; we don't fully understand the scale of this yet.	The internet of things will change how our customers place orders in he future.

By the end of this session, you should be able to:

- construct a meaningful risk statement (Cause / Event / Consequence)
- understand methods of identifying risk – brainstorming, interviews, checklists, PESTLE, SWOT
- understand different types of risk
- understand risk registers.

Now begin Session 3.

1 The basics of risk identification (What do I need to identify?)

There is a range of approaches for identifying risks, but first consider what it is you are looking to identify.

Activity 2 Identifying a risk

Allow approximately 10 minutes

Select the terms that, when set out in the boxes below, define the process of risk identification. Drag the correct terms into the three boxes.

Interactive content is not available in this format.

Discussion

The short answer is the Root Cause, the Event and the Consequence, or more precisely the Root Causes, Event and Consequences. The addition here is really important: where possible you need to understand all of the causes of a risk and all of the potential consequences. This is critical because only by doing this can you ensure that your treatments are comprehensive.

- **Root Causes** – Root Causes are the elements that can lead to the event taking place.
- **Event** – Events are the point at which control is lost but consequences have not happened.
- **Consequences** – Consequences are the outcomes that can happen downstream of the event.
- **Hazard** – A hazard is the set of circumstances in which the risk is present (e.g. there is a risk of explosion when filling a car petrol tank).
- **Controls** – Controls are not part of a risk statement: controls are treatment of the risk. It is not uncommon for a control failure to be mistaken for a risk.
- **Incidents** – An incident is a risk that has occurred. Incidents may provide ‘clues’ as to what risks may exist, but incidents may not provide the whole picture.
- **Concern** – A concern relates to a set of circumstances that may result in a risk. However, they are often too poorly defined to allow for a risk to be created. Therefore further work is often required to establish the risk present.
- **Cost** – Cost is not part of a risk statement, but it is often used as a way to measure risk.
- **Issue** – An issue – similar to an incident – is a risk that has occurred, but typically may have more of an enduring nature (e.g. a fire (an incident) leads to a prolonged unavailability of computer servers (an issue)).

2 What should a ‘well written’ risk statement contain?

A risk must also have certain key elements, which generally are, as a minimum, root cause(s), an event and consequences. Recognising and identifying these elements is what constitutes a risk statement.

- **A root cause** – This is the origin of the risk, the reason(s) the risk exists. As an example, consider the root cause(s) of a fire – a supply of oxygen, a source of heat and a source of ignition. One interesting method of drilling down to the root cause of a risk is to keep asking ‘why’ in response to the feedback on a question. This interrogative technique is called the ‘Five Whys’ technique and is attributed to Sakichi Toyoda, the founder of Toyota Industries.
- **An event** – This is the risk itself, and normally the point where ‘control’ has been lost but the consequences have yet to occur. For example, the event for a fire is the fire breaking out, but no property being damaged or people harmed. In the business example the event will be a failure in awareness of contract liabilities.
- **A consequence** – This is often described as the ‘so what?’ of risk management. These are the ‘events’ that occur as a result of the risk. Consequences should be measurable against the organisation’s objectives. The consequences for a fire may be damage to property, injury or loss of life, financial losses to repair and financial losses due to not being able to operate. It is important to note that a risk may have more than one root cause and more than one consequence. You need to capture all root causes and all consequences when identifying a risk and also recognise that the same root cause may drive more than one event and that the same consequences may arise from more than one event.

It is also important to identify risk ownership. In most cases the owner of the risk is the person who feels the impact of the consequences. However, this doesn’t mean that the risk owner has to personally complete all of the activities to treat the risks, which will be discussed in Session 5. There are often a number of other parties who support the risk owner to manage the risk.

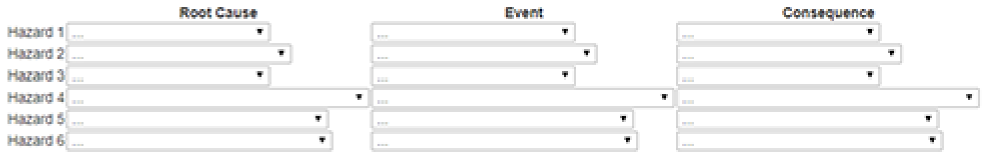
Activity 3 Risk statements

Allow approximately 10 minutes

Put the following elements of some risk statements into the correct categories.

Click on the interactive to start selecting your answers from the drop-down options.

Interactive content is not available in this format.



	Root Cause	Event	Consequence
Hazard 1	...	...	...
Hazard 2	...	...	...
Hazard 3	...	...	...
Hazard 4	...	...	...
Hazard 5	...	...	...
Hazard 6	...	...	...

3 Different risk identification approaches

Identification answers the question, ‘what are the areas of uncertainty?’

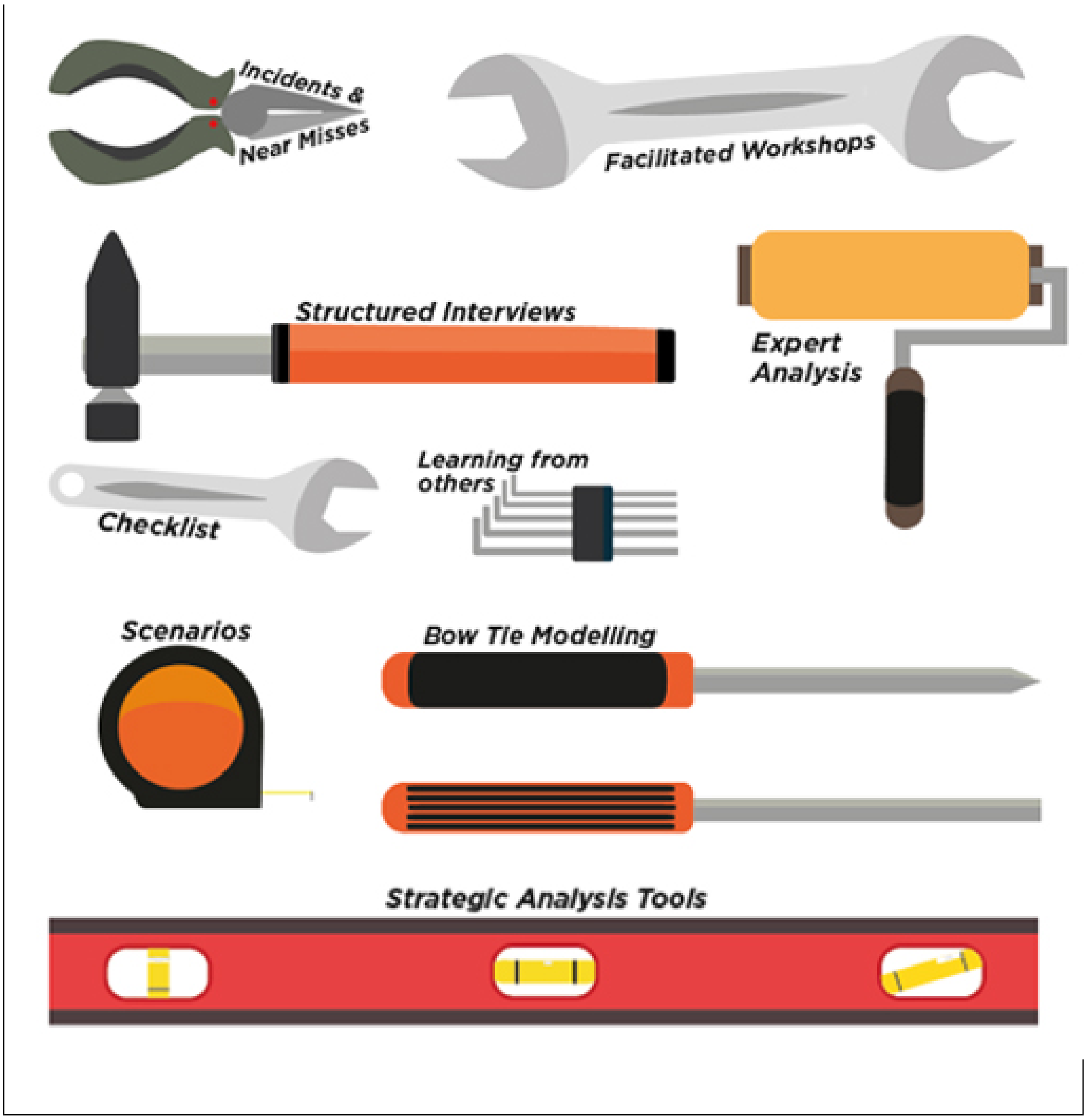
According to ISO 31000:

> the purpose of risk identification is to find, recognise and describe risks that might help or prevent an organisation achieving its objectives. Relevant appropriate and up-to-date information is important in identifying risks.
>
> The organisation can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:
>
> - tangible and intangible sources of risk;
> - causes and events;
> - threats and opportunities;
> - vulnerabilities and capabilities;
> - changes in the external and internal context;
> - indicators of emerging risks;
> - the nature and value of assets and resources;
> - consequences and their impact on objectives;
> - limitations of knowledge and reliability of information;
> - time-related factors;
> - biases, assumptions and beliefs of those involved.
>
> The organisation should identify risks whether or not the root causes are under their control. Consideration should be given that there may be more than one type of outcome which may result in a variety of tangible or intangible consequences.
>
> ISO 31000

There are often many different ways to identify risks. Explore some of them now.

Click on the tools for more information.

Interactive content is not available in this format.


Incidents &
Near Misses
Facilitated Workshops
Structured Interviews
Expert
Analysis
Checklist
Learning from
others
Scenarios
Bow Tie Modelling
Strategic Analysis Tools

4 Styles of risk management

When considering their approach to risk management, organisations need to consider what operational approaches work for them. The next four subsections examine certain styles of these approaches.

4.1 Top down v. bottom up

All organisations will need to decide to what degree their risk register is derived from senior management 'top down' activity or from working level 'bottom up' activity. In reality, any risk register will be influenced by both. Some risks will be recognised at the working level of the organisation and may need senior management involvement to bring together the generic risk theme faced by the organisation, while other risks may be recognised at the top of the organisation and be mandated or otherwise directed down through the organisation. Organisational risk structures must allow for both approaches to be successful.

4.2 Standardised risk approach

An organisation may choose to define some risks that are present in large parts of (or the entirety of) the organisation in a standardised way that can be applied consistently across the organisation. The benefits of doing this are:

- Creation of a consistent view of the root causes and consequences.
- Greater awareness of the presence of the risk in the organisation.
- Opportunities to reduce silos and seek best practice across the organisation.
- Reduced waste in documenting risks.
- It ensures risks are owned in the right place.
- Greater potential for common treatment and sharing of best practice.

There are, however, some potential pitfalls to be aware of:

- Business areas may adopt the risk without considering if there are any different circumstances.
- If the completeness of the risk isn't identified then the weakness persists across the organisation.
- Reduced ownership and accountability can occur.
- Users can become 'blinkered' to only the outlined set of risks and may fail to identify other risks.

4.3 Standardised elements – controls, root causes, consequence

As organisations grow their structures, employee numbers will also inevitably grow; however, the nature of the risks they face may not change at all or be similar enough to still be managed consistently. Consider the example of a fast-food restaurant chain: whether it is a chain of 10 restaurants or 100 restaurants, each restaurant will still have the same risk of fraud, business interruption (fire, flood, cyber security) or employee safety. Managing these risks in a consistent way allows for the pooling of knowledge and best practice, while reducing wasted effort.

To facilitate the creation of standardised risks, the organisation may go one step further and create standardised root cause, events, consequences and even treatments, which will be covered in greater depth in Session 5. In doing so, the organisation effectively creates a ‘catalogue’ of risk elements that can come together to create a set of risks. Technology permitting, a readily searchable database can be created to allow risks to be easily generated by those tasked with risk management within the business. Prior to this point, as part of risk planning, the organisation will have established a standardised approach to evaluate consequences (which will be covered in Session 4) allowing for a streamlined risk process.

4.4 Categorising different types of risk

Many organisations find it helpful to put their risks into categories – for example, whether the risk event is internal or external to the organisation. It is also common to categorise by the type of risk (e.g. financial, operational, compliance, etc.). The reasons for doing this can generally be described as follows:

- To allow the organisation to understand the types of risks it has at a macro level.
- To consider priorities, if, for example, a particular categorisation appears with greater significance and frequency than others.
- To consider combining efforts in particular areas (e.g. if common risk types emerge can common treatments be defined?). This is covered more in Session 5.
- To engage company specialists on the particular risk types.

Many organisations find it helpful to create other categories based on root cause or other businesses themes, and will often have their own strategic objectives, principal risks or priorities to align with.

5 Documenting the risk (‘risk registers’)

It is common practice to capture all of the information about a risk in one place. The information will typically include the items listed below, some of which will be covered in greater detail in future sessions:

- A description of the risk.
- A risk statement describing the root causes, the event and the consequences.
- An assessment of the impact and probability of the risk.
- An identified individual to own the risk.
- Treatment measures and their status.

The document or sets of documents in which all of this information is stored is commonly referred to as a ‘risk register’.

Activity 4 Risk register

Allow approximately 15 minutes

Using what you have learned so far – and particularly during this session – you can now start to create a risk register of your own. This can be based on the organisation where you currently work or on one where you previously worked. Click below to access the risk register document. You can save this and return to it later to add further details as you work through the course. Now create a risk register.

6 Human factor elements in risk identification

As with many other areas of life your view of matters is often limited by your perspective, and getting a diverse perspective on the risk means identifying risks that might otherwise remain hidden. The following activity demonstrates this.

Activity 5 Say what you see

Allow approximately 10 minutes

Now take a look at the video below and count the number of times the red clipboard is passed to another person.

Video content is not available in this format.

Video 2 How many times is the red file passed?

Discussion

In the first clip did you notice the mouse? No? Replay the clip and this time look for the mouse. Studies have found that about 30% of people who watch videos set up like this experiment failed to spot the mouse (or similar; the original test had a person dressed in a gorilla suit). The authors of the original experiment have concluded that most people believe they will notice something that is visible and distinctive but their experiments have shown that these intuitions can often be wrong. It is important to recognise these blind spots so that measures can be put in place to mitigate them.

Look at the picture and write down what you see here.

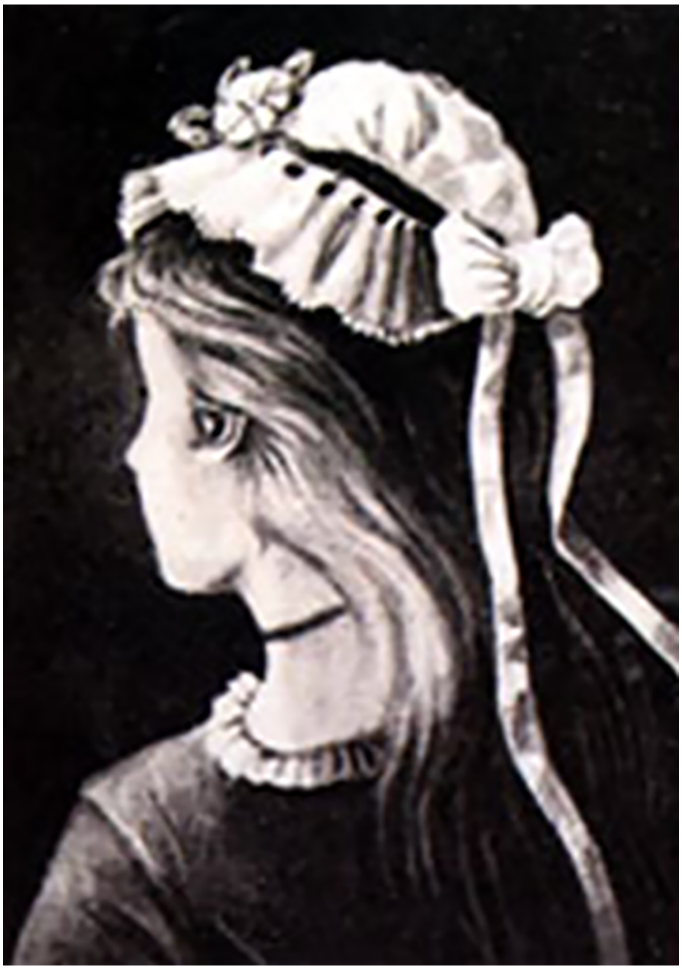


Figure 2

Discussion

In the picture in the second example did you see the old woman? Perhaps you saw the young woman? Take another look. The key thing to note here is that not everyone sees the same thing, and even different people looking at the same thing don't always agree on what they see.

7 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 3 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

8 Summary of Session 3

In Session 3 you have looked at risk identification and the importance of creating a comprehensive risk statement, covering all root causes of a risk, the risk event and all the consequences of a risk. You have also looked at risk categorisation and its benefits. You have considered the use of standardisation in the risk identification activity to support improved understanding of risks.

Moving on from the risk statement, you also looked at how individuals, groups and organisations can identify risks. The risk toolkit covered the use of a number of methods by which risk could be identified from simple ‘brainstorming sessions’ to more advanced risk ‘bow ties’.

Concluding Session 3 you covered best practice in documenting risks using a risk register and looked at some of the human factors involved in risk identification.

The main learning points that have been covered in this session are:

- risk statement (Cause, Event, Consequence)
- methods of identifying risk – brainstorming, interviews, checklists, PESTLE, SWOT
- different types of risk
- risk registers.

Session 4: Risk assessment

Introduction

In the last session you looked at how to identify a risk and considered the importance of understanding all of the root causes and the consequences of a risk. Thorough risk identification is a fundamental precursor to what will be covered in Session 4 – assessing a risk. Assessing the risk is the next step in the ISO 31000 standard, referred to as analysis and risk evaluation. In particular you will cover:

- the different points at which risk can be assessed
- the importance of time when making an assessment
- how to assess risks in a quantitative and qualitative way
- why using consistent units of measurement is important in assessing risk
- why it is important to understand the impact and probability of each consequence
- the iterative nature of risk assessment and risk treatment
- complexity and connectivity of risks and how to deal with risks that have more than one consequence and with risks that can have the same consequences (aggregation).

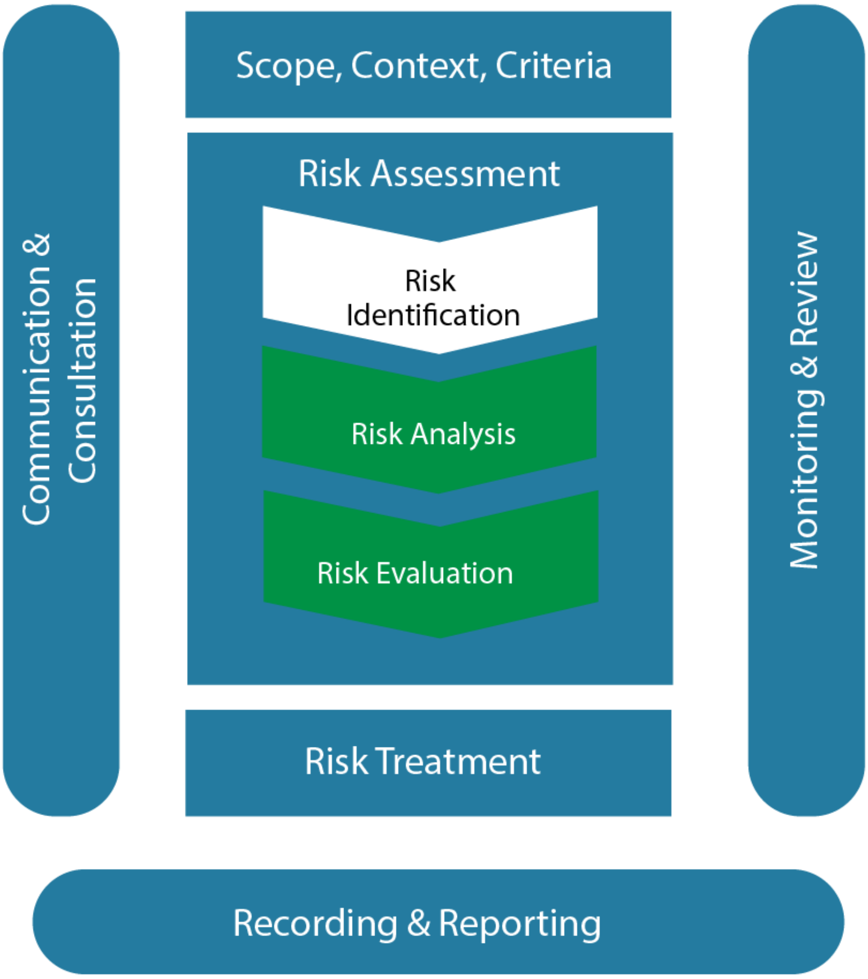


Figure 1 ISO 31000 diagram – risk analysis and risk evaluation

By the end of this session, you should be able to:

- understand the process of arriving at an ‘assessment value’ for the risk – scores and Probability and Impact Diagrams (PIDs) (gross, current, residual)
- understand how to assess risk events (basic probability and impact assessment)
- understand ‘basis of estimate’ – including the Programme Evaluation and Review Technique (PERT)
- have an awareness of risk modelling – including Monte Carlo analysis and Schedule Risk Analysis (SRA).

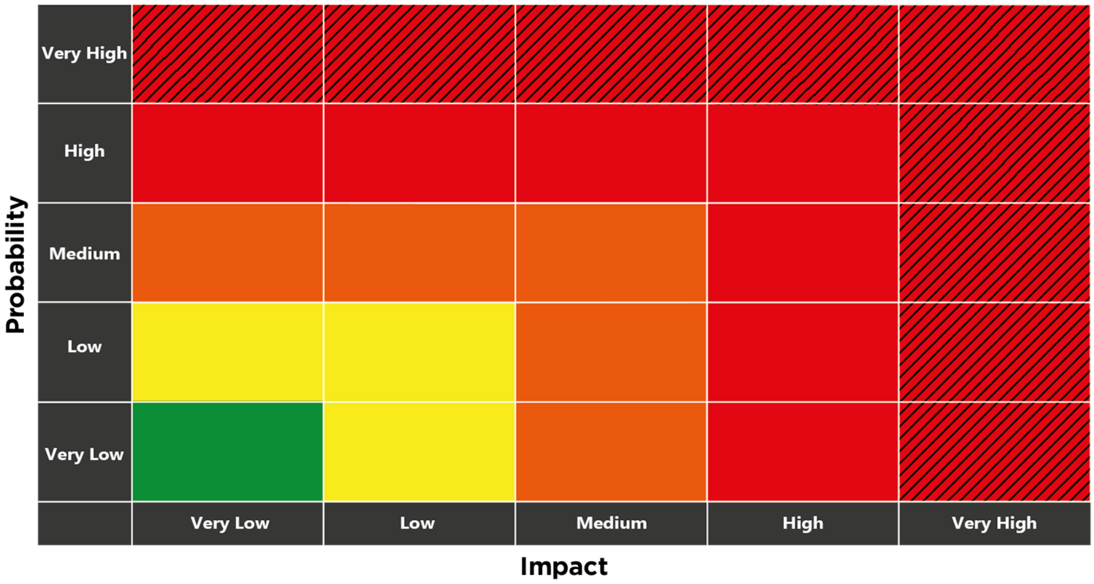
Now begin Session 4.

1 Basic elements of risk assessment

Risk assessment is the activity of understanding the extent to which potential events can affect the organisation's ability to achieve its objectives.

In many situations, organisations do not have the resources to deal with all of the risks they face. By ranking them in relative order of importance, organisations can prioritise the treatment of risks. Risk assessment is the first step in prioritising risks.

Risk assessment can be both qualitative and quantitative, based on highly complex mathematical models or 'gut feel'. Both approaches have their merits, but in its most basic form the aim is to understand what is the relative order or importance of the risks.



	Very Low	Low	Medium	High	Very High
Very High	▨	▨	▨	▨	▨
High	🟥	🟥	🟥	🟥	▨
Medium	🟧	🟧	🟧	🟥	▨
Low	🟨	🟨	🟧	🟥	▨
Very Low	🟩	🟨	🟧	🟥	▨

Figure 2 Probability and Impact Diagram (PID)

The most common approach to assess a risk uses two dimensions: impact and probability. This approach is usually displayed in a risk matrix (sometimes referred to as a Probability and Impact Diagram, or PID). It is also common practice to assign a value to each 'cell' in the risk matrix and this is commonly known as the risk score.

The risk impact(s) is the outcome of the consequences, which you examined in Session 3 when you looked at risk identification. For an organisation, risk impacts are often expressed in financial values, but may also be expressed in other values that are important to the organisation (e.g. health & safety, compliance, reputation). As an example, you may have identified a risk that a project may overrun with consequences that will cause late delivery and incur financial penalties. The impact would be the value of these financial penalties and a measure of the reputational impact of the late delivery.

The probability is the extent to which those impacts are likely to occur. The probability must be related to impacts otherwise the assessment is invalid; the two elements exist as one complete risk assessment.

It should be noted that other valid combinations of impact and probability may exist for the risk. To ensure correct risk assessment, organisations should set out rules defining how risks should be recorded. Some organisations use the 'most probable' approach, while others use 'severe but plausible'. Whichever method is used, it must be consistent across the organisation to avoid potential confusion. Consider the simple example of the risk of fire. It may be equally valid to state that in the UK there are a large number of small fires, and therefore a ‘high’ probability of a small fire, but there are also a small number of very large fires and therefore a ‘low’ probability of a very large fire.

Some organisations may choose to look at additional measures, the most commonly used being:

- Timing of impact – when the risk could occur.
- Velocity (or speed of onset) – how quickly the risk could occur.
- Vulnerability – how susceptible the organisation is to the particular impact.

It is important to set out some prerequisites before moving forward. If you consider risk management as an isolated activity then the measures used to assess risk can be tailored specifically to that activity. However, having a bespoke way to assess risks in each individual area in an organisation with two or more activities is problematic. Look at a simple example, where Risk Managers compare three risks, each assessed on a different basis.

Audio content is not available in this format.

Audio 1 Comparing risks

As shown in the example above, without a common approach to scoring, with everyone using the same scoring variables and common units of measure, it is practically impossible to undertake meaningful risk management at a company level.

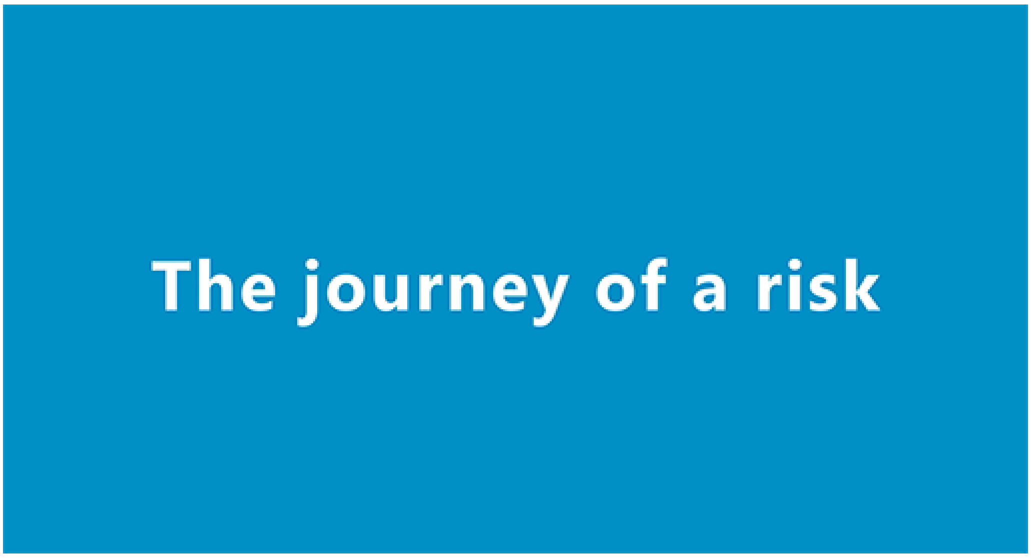
As discussed in Session 2, it is therefore a prerequisite to set out, across an organisation, a set of common scoring variables and units of measure that everyone uses. Only by doing this is it possible to compare risks from one part of an organisation with risks from another part and thus maximise the return for the effort invested in risk management. You can see an example of this under the scoring scheme in the RMP you can download from Session 2.

2 The importance of assessing all consequences

In Session 3 you saw how one risk can have more than one consequence. It is therefore important that you can understand and assess all of the consequences a risk can have. It is also important to consider how a consequence can evolve.

Risks change over time. It may seem obvious to say so, but over time the risk level faced for some risks may go up, while for other risks it may go down. Sometimes this is due to things within your control (e.g. tangible things you have done to alter the risk level); other times it may be due to a change in the external environment that change the level of risk faced. Consider the different points at which risks are normally assessed.

Video content is not available in this format.



Video 1 Dynamic movement of risk

When assessing a risk you need to consider the level of risk and how this changes over time. This part of the process is iterative, where assessment of risks and treatment of risks need to be considered together. Risk treatment will be covered in more detail in Session 5.

3 How to go about assessing a risk

As stated earlier, the impact and probability must be considered in combination – not as discrete items – and the assessment must be made in line with any organisation guidance provided around expectations. In this section you will see how to assess a risk.

Firstly, consider the impact. Using the definition from Session 1, risk is defined as an uncertain event, but what most organisations are really interested in is risks that prevent them from achieving their objectives. The first step is therefore to understand the potential consequence(s) of interest to the organisation; this must be done bearing in mind that a risk can have more than one consequence. This may also mean in practice that some risks are discounted – those, for example, where the impact does not materially affect the company's objectives.

Let us consider the risk inherent in driving a vehicle. While undesirable and something that should be avoided – both for the individual and for an organisation minor – 'non injury' accidents are of less concern than accidents that involve serious injury or fatalities. Therefore, if there are limited resources to manage the risk, as discussed in Session 5, the focus, individually and as an organisation, should be on reducing the risk associated with serious and fatal accidents. This approach, whereby a 'single version of the truth' is adopted, allows the organisation to fix the consequence(s) and focus on the root causes.

Activity 1 Road risks

Allow approximately 10 minutes

Now watch Video 2, which covers real-life examples of road risk, to explore how root causes will change our assessment.

Video content is not available in this format.

Video 2 Road risk

Once root causes have been understood the next step is to ask how likely the consequence is to occur. It is an important point to remember that the aim is to understand how likely is it that the risk will lead to the consequence defined previously, because as stated earlier the probability and impact are coupled.

3.1 How to quantify impact

There are a number of different approaches that can be used to quantify the impact of risk. This section takes a look at some of the most common approaches and discusses their limitations.

- **Models** – Financial models that calculate the impact are often used. These are particularly helpful where there is a history of information about the risk and how often it occurs. Models can then be constructed, based on historical observations, to predict the future level of risk. It is important when using models to know whether the model is being used to extrapolate (i.e. predict results beyond the data the model is based on).
- **Scenarios** – Scenarios are similar to financial models but can be used to assess risks that are new and/or are yet to happen. The scenario will define a set of assumptions about the nature of the risks; these assumptions will then be used to assess the risk's impact.
- **History** – Impact of risks can be based on actual information on risks that have occurred. For example, last time the machine cost 10% more than forecast so the risk is future machines will cost 10% more than forecast.
- **Expert opinion** – In certain circumstance there may be no historical information to fall back on. It may be that the venture or the circumstance is so novel than no comparable or relevant information exists. In such situations it is common to solicit expert opinion. It is recommended that, where possible, the assumptions made by the experts when giving their opinion are captured – these can then be revisited over time to ensure the assumptions (and therefore the assessment) are still valid.

Best practice is to be able to show how the assessment was arrived at and, in particular, what assumptions have been made.

3.2 How to deal with risks that are on a continuum

As discussed earlier, a number of risks operate on a continuum. These risks exist as a range of impacts that can simplistically be described as there being a much higher probability of a low impact and (hopefully) a much lower probability of a very large impact. One approach, already highlighted, is to ensure that the organisation adopts a 'single version of the truth' where everyone is expected to report one scenario; however, with more complex risks, where there are many root causes, this may not be appropriate.

Consider a real-life example – earthquakes – to understand the importance of examining the distribution (or pattern) of combinations of risk probability and risk impact.

Being specific about consequences is important: whilst there are thousands of small earthquakes globally, there have only been around 500 since 1900 that have exceeded 3 on the Richter scale. These are shown in Figure 3

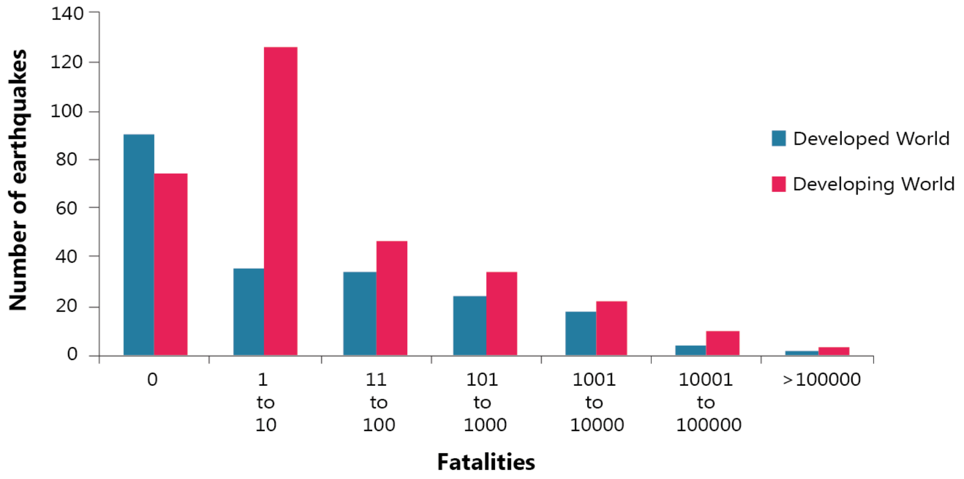


Figure 3 Number of earthquakes exceeding magnitude 3 since 1900 based on number of fatalities

Of those 500, in approximately 17% of cases there were no fatalities, and in a further 34% of cases there were fewer than 10 fatalities, meaning that in 51% of earthquakes there were few fatalities. In 15% of earthquakes there were 1000 or more fatalities. However, the view can change depending on location in the world (and the data chosen to use). Figure 4 shows just the data from 1900 to 1950.

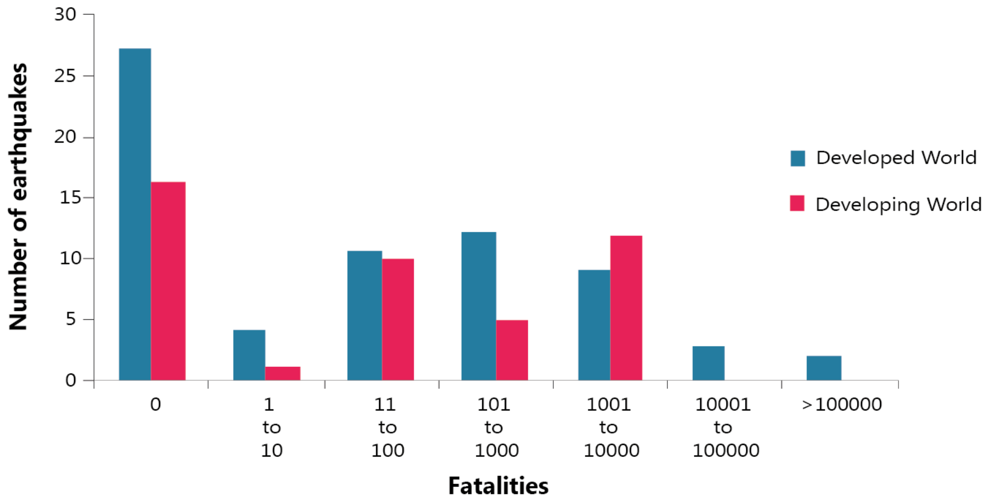


Figure 4 Number of earthquakes exceeding magnitude 3 between 1900 and 1950 based on number of fatalities

If you just look at data up to 1950, then 37% of earthquakes killed in excess of 1000 people, with people in the 'developed world' being the most impacted. Perhaps because of better recording or perhaps because of greater earthquake activity, but the picture for the second half of the twentieth century and early twenty-first century is very different, as shown in Figure 5

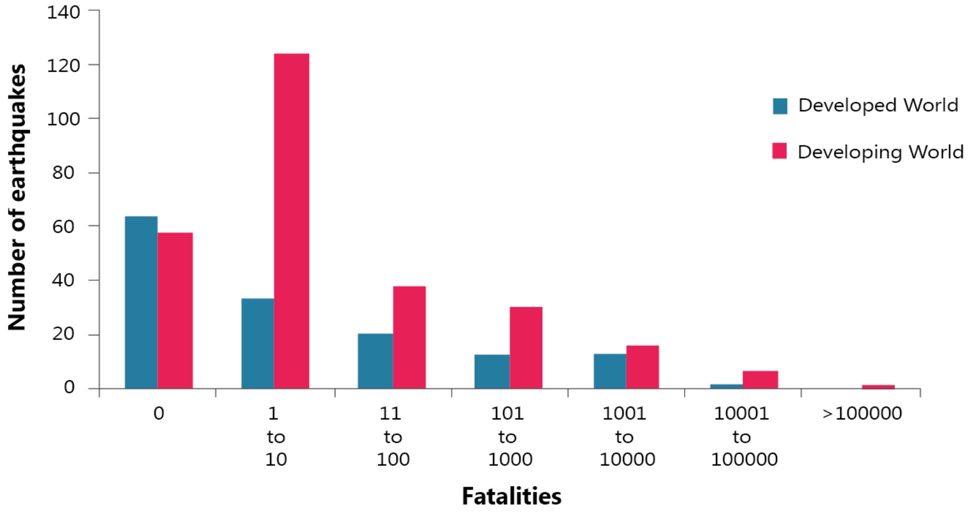


Figure 5 Number of earthquakes exceeding magnitude 3 since 1950 based on number of fatalities

Since 1950, earthquakes in the developed world where more than 1000 people die make up just 2.8% of the total. Worryingly for those in the developing world, while earthquakes that kill over a 1000 people since 1950 in these regions represent 4.2% of the total, earthquakes that kill over 10,000 people represent 2% of the total. Thus very large-impact earthquakes in the developing world are almost as prevalent as a lower-impact event in the developed world. A large portion of the difference potential is due to controls, which will be covered in treatment.

These risks and their impacts are often shown as a distribution. In such cases it can often be very important to understand the shape and nature of the distribution; in certain circumstances it may be appropriate to capture multiple pairs of probability and impact to properly describe the risk faced. This can prove to be particularly important where different treatment approaches will be required. There will be more on this in Session 5.

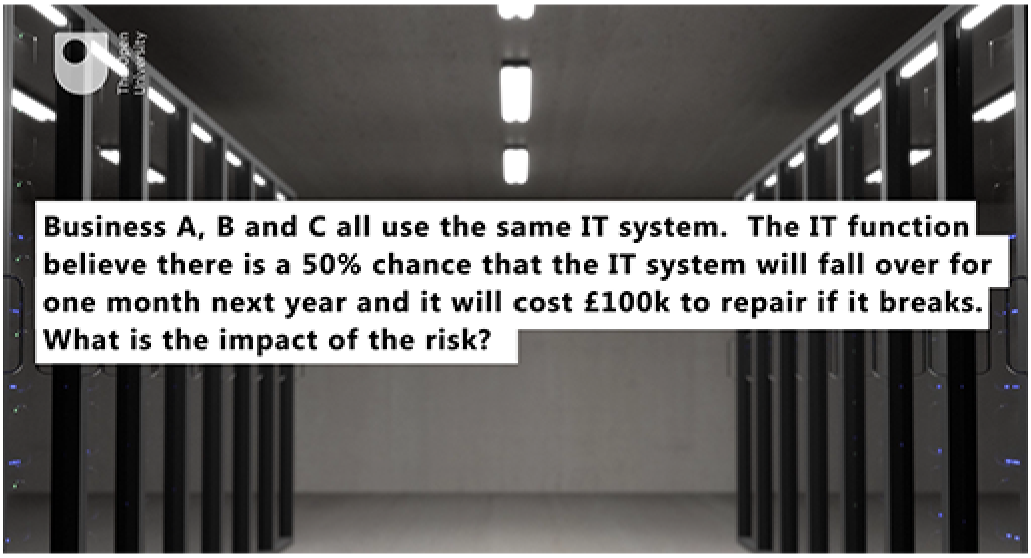
Distributions such as these are often used in the financial services industry – for example, in credit scoring. In this area, a plot of the distribution of credit scores versus loan default rates can be used to assess the risk of default based on approving loans relative to a certain credit score.

3.3 Risk aggregation

Now consider a simple example to explore what the term risk aggregation means. Take a look at the video below and see how the experts assess risk.

Video content is not available in this format.

Video 3 Risk aggregation



Business A, B and C all use the same IT system. The IT function believe there is a 50% chance that the IT system will fall over for one month next year and it will cost £100k to repair if it breaks. What is the impact of the risk?

3.4 Using mathematical models

In certain cases it may be useful to aggregate the impact from multiple risks, with unrelated root causes, each with their own impact and probability. A common reason for doing this is on large projects to look at both potential schedule and financial impacts, and ensure that sufficient funds or contingency (time and money) are put aside to deal with the risks.

The approaches used to assess these risks can be quite advanced and are beyond the scope of this course. They are usually performed by experts using specialised computer packages. The information below outlines common approaches that you may come across.

Analysis type	Description
Monte Carlo	A mathematical model (sometimes called a stochastic model) based on a repeated random sampling to obtain a numerical value. Results are numbers. ‘Simulations’ are then brought together to give a statistical probability of a particular outcome. Results are often presented as ‘p’ values, denoting how statistically likely a particular outcome is.
Strategic Review Analysis (SRA) or Programme Evaluation and Review Technique (PERT)	This is an approach to understanding the likely variance to a schedule. Like the Monte Carlo, this is a mathematical simulation. Each task is typically give three values (often called a three-point estimate) where the values relate to Shortest, Longest and Expected time to complete. Multiple ‘iterations’ are then run to present the statistical probability of a particular outcome.
Expected Monetary Value (EMV)	EMV is calculated by multiplying the impact of the risk by its likelihood. For example, if the

impact of a risk is £10m and the likelihood is 50% then the EMV is 10 × 0.5 = £5m. This can be helpful if there is a group of independent (unrelated) risks where the impacts and likelihood are similar. This approach is often used for calculating contingency funds for projects. Care should be taken, however, where there is a small number of risks, where the risks are inter-related and where there is a number of large, but unlikely risks. Like most risk modelling it is recommended that you engage an expert.

It should be remembered that as with all calculations, these models are only as good as their inputs. Moreover calculations, if assumptions are not made clear, can be misleading. Often end users may not understand what a ‘p’ value is. Furthermore, the shape of the distribution may be important to understand, and, finally, people may believe that the output is more trustworthy simply because it has been put though a complicated model, irrespective of the quality of the underlying information.

3.5 Human factors in risk assessment

Risk assessment is often far from an exact science and it is important to be aware of some of the behavioural factors that can be at play. Here are a few examples:

- When assessing risks that are highly uncertain or have not happened before there is often little or no known empirical data on which to base assessment. In these cases there can be a reliance on expert judgement.
- Judgement, of course, can be subject to bias. For example, recent events may skew our perception of the probability of a risk; moreover, things that have happened to people personally (or to people they know) may be perceived as more likely to happen than they really are.
- Perceptions and attitudes to risk may also skew our perception and assessment.

Best practice is to involve multiple people and to document the basis of estimate and the key assumptions that have gone into arriving at this estimate. In this way the key assumptions can be understood and, where necessary, tested.

Take a look at the video below, which looks at dealing with undefined risk.

Video content is not available in this format.

Video 4 Dealing with undefined risk

4 This session's quiz

Now it's time to complete the Session 4 badge quiz. It is similar to previous quizzes, but this time instead of answering five questions there will be 15.

Session 4 compulsory badge quiz.

Remember, this quiz counts towards your badge. If you're not successful the first time, you can attempt the quiz again in 24 hours.

Open the quiz in a new tab or window then come back here when you've finished.

5 Summary of Session 4

Session 4 has focused on risk assessment. You have discovered that while there are many factors that can be used to assess risk, probability and impact are of greatest importance. To illustrate probability and impact you have covered the use of the PID diagram.

In discussing earthquakes and road risks you should now recognise that it is essential to understand what the risk's consequences of interest to you are and how these come about (the root causes) in order to correctly assess the risk. You should also now understand that everyone in an organisation must assess in a common way for there to be effective risk assessment across the organisation.

You were introduced to the use of mathematical models in risk management, a subject that is too large to be covered sufficiently here. If you found this an area of particular interest then you could research opportunities to find out more. Finally the session closed by considering some of the human factors involved in risk assessment.

The main learning points that have been covered in this session are:

- the process of arriving at an 'assessment value' for the risk – scores and Probability and Impact Diagrams (PIDs) (gross, current, residual)
- how to assess risk events (basic probability and impact assessment)
- 'basis of estimate' – including the Programme Evaluation and Review Technique (PERT)
- risk modelling – including Monte Carlo analysis and Schedule Risk Analysis (SRA).

You are now halfway through the course. The Open University would really appreciate your feedback and suggestions for future improvement in our optional end-of-course survey, which you will also have an opportunity to complete at the end of Week 8. Participation will be completely confidential and we will not pass on your details to others.

Session 5: Risk treatment

Introduction

In Session 5 you will build on the learning from previous sessions to consider probably the most important part of risk management, referred to in the ISO diagram as risk treatment.

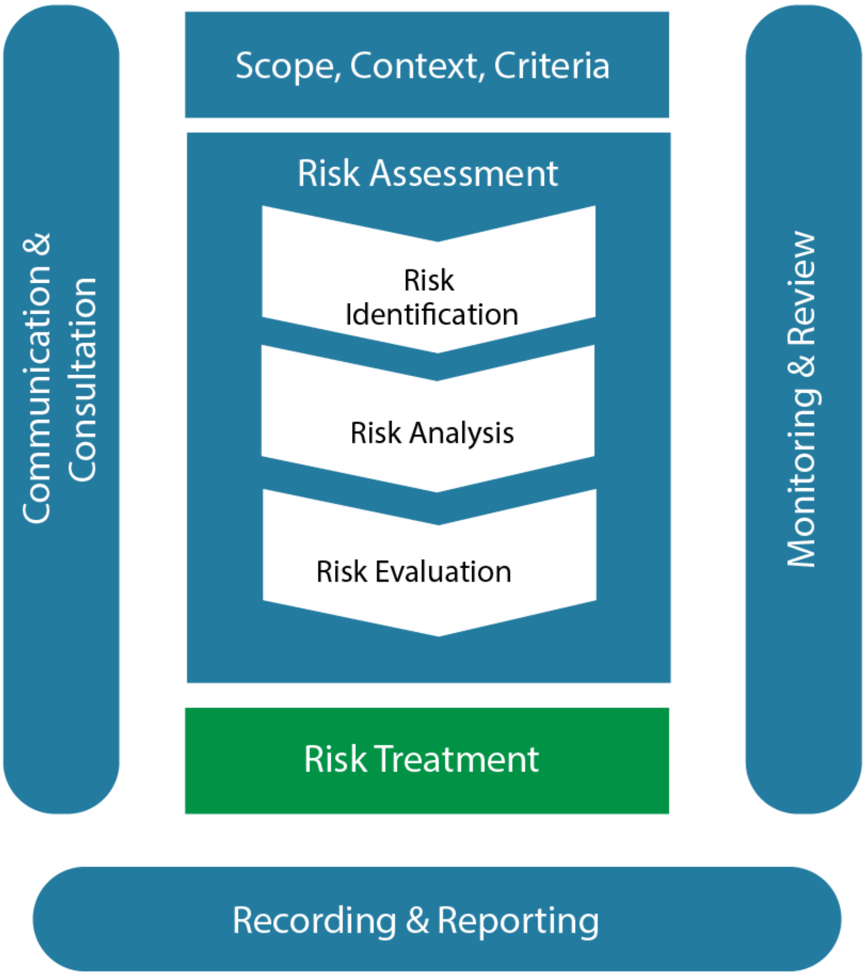


Figure 1 ISO 31000 diagram – risk treatment

You will underline some of the concepts discussed in previous sessions, in particular risk appetite and risk assessment, and you will consider the most common approaches to risk treatment, including:

- controls
- actions
- risk transfer.

By the end of this session, you should be able to:

- have an overview of treatment
- understand treatment strategies
- understand an introduction to mitigation through action
- demonstrate knowledge of an introduction to controls
- understand assessing treatment effectiveness
- produce an example of a treatment plan.

Now begin Session 5.

1 Risk treatment overview

All risk treatment should be related to risk appetite (discussed in Session 2). Risk treatment is the term applied to 'doing something' about a risk, essentially the phase of risk management that delivers value to the organisation. Without effective risk treatment, risk management has little benefit. Risk treatment is mainly about seemingly obvious business activities: identifying options, evaluating them (will they reduce the risks and are they value for money?), selecting the best option and then making sure it is implemented.

At all levels, the organisation, through its risk management processes, must decide whether there is a business case for treating certain risks, based on a number of factors:

- What level of risk are you prepared to accept (risk appetite)?
- Is the current level of risk lower than the appetite?
- What measures can be taken?
- Are these measures affordable?
- Can the risk be accepted without further action?

2 Treatment options

Options for risk treatment can be wide ranging, from changing the consequences or probability, removing the risk source, changing plans to avoid the risk altogether or accepting the risk (and making provision for it happening). Risk treatment is an iterative process, linking with other parts of the risk management process.

The figure and table that follow will recap some key definitions on the life cycle of a risk.

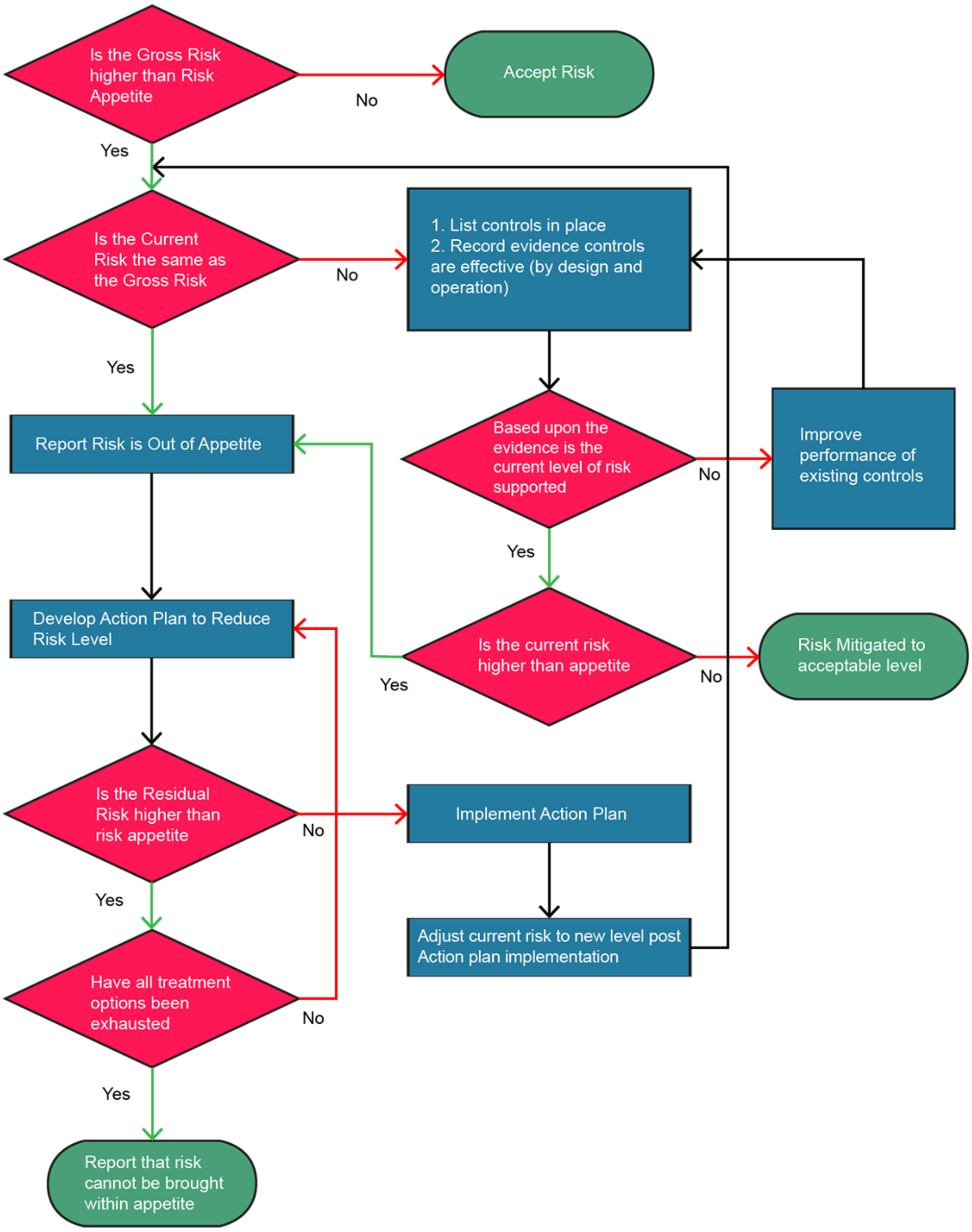

Is the Gross Risk higher than Risk Appetite
No
Accept Risk
Yes
Is the Current Risk the same as the Gross Risk
No
1. List controls in place
2. Record evidence controls are effective (by design and operation)
Yes
Report Risk is Out of Appetite
Based upon the evidence is the current level of risk supported
No
Improve performance of existing controls
Yes
Develop Action Plan to Reduce Risk Level
Is the current risk higher than appetite
Yes
No
Risk Mitigated to acceptable level
Is the Residual Risk higher than risk appetite
No
Implement Action Plan
Yes
Adjust current risk to new level post Action plan implementation
Have all treatment options been exhausted
No
Yes
Report that risk cannot be brought within appetite

Figure 2 The iterative approach to treating risk

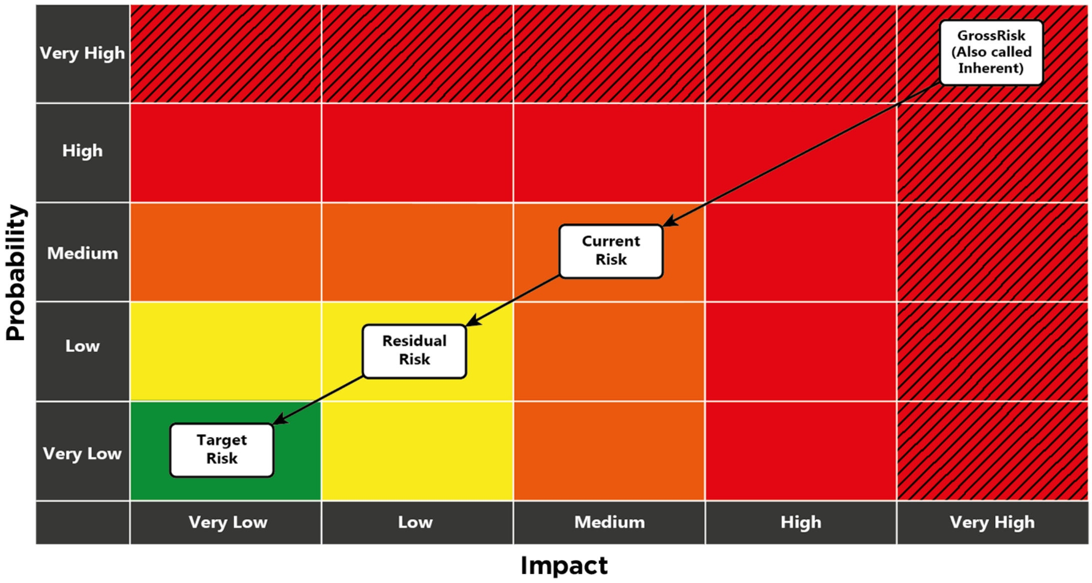


Figure 3 The life cycle of a risk

Table 1 The life cycle of a risk

Type of risk assessment	Definition
Gross (also known as Inherent)	The worst case: the level of risk assuming existing measures (e.g. controls) don't work as intended.
Current	The level of risk faced today. When assessing the current risk level you need to understand: What measures are already in place that reduce the level of risk? How do you know that these measure are working properly?
Future	The level of risk you will face in the future; this is commonly referred to as the Residual and Target risk level
Residual risk	The level of risk once all risk treatments have been completed. Good practice is to only take into account treatment activities that have been fully funded and resourced, as many companies find that without funding and resource, their best laid plans don't happen! This leads to a potential further level of risk, the target risk level. This is the level of risk you want to take and is linked to risk appetite.

So there are potentially four levels (Gross, Current, Residual, Target) of risk that you may wish to assess. Often, however, things are simpler. Consider a few examples.

- Residual risk = Target risk. On many occasions a company will fund all of the necessary treatment activities such that the level of risk faced once all treatment activities are completed will be the same as the level of risk they would wish to take, and therefore their residual risk is the same as their target risk
- Residual risk = Target risk = Current risk. Furthermore, once a company has completed all 'actions' to reduce the level of risk, they may find that their current risk level is the same as their residual risk level, which in turn is the same as their target level. Remember, it is not the case that the risk can no longer happen: rather, based on the current controls (and assuming they are working effectively), the agreed level of risk is taken.

There is one further point to highlight, which is as circumstances change so can the risk level. This could be driven by things inside an organisation, as well as factors outside the organisation, it could be that new information is found that changes our view of a risk, or that technology changes change the nature of the risk. It is for this reason that risk assessment should be regularly revisited. Many organisations ensure there are links between their risks, the audit and assurance findings and their incident management processes for precisely this reason, as this gives them clear and early notification if their risk level is changing.

3 Treatment strategies

Traditional risk management teaching suggests there are four different ways you can react to a risk:These will be explored in the following sections at the links below.

- acceptance
- rejection
- transfer
- mitigation.

3.1 Acceptance

Acceptance is when the organisation consciously (fully aware) accepts the risk and decides to do nothing. This course of action may be because the organisation, after having assessed the risk, believes the size/scale of the risk is small enough that no action is warranted (i.e. the risk is within its risk appetite). Alternatively the risk may be at the other extreme for the business, whereby the organisation can do nothing to change the risk but decides that the organisation still wants to operate with this risk. In this situation the organisation may be changing its risk appetite or would need to accept that it is operating outside of its agreed risk appetite.

It is the people accountable for the overall viability of the organisation who would have to accept the risk(s) that exceed appetite. Those decision makers should be clear about what risks they have accepted and the consequences of the decisions they make.

The decision not to mitigate a risk any further (see Section 3.4) means that you are accepting the current risk level. It does not mean the risk has gone away and can no longer happen.

Good practice is to link your current risk level to your financial forecasts so that the current level of risk is properly accounted for. You should not link your forecasts to your residual risk level, as the residual risk level has yet to be achieved.

3.2 Rejection

Rejection is when the organisation decides that continuing to take the risk is untenable so rejects the risk. In this situation the organisation may need to take steps beyond just formally rejecting the risk, which may mean ceasing projects, stopping work or withdrawing from business segments. The decision to reject a risk must be carefully weighed up against continuing to take the risk, balancing the opportunity against the threat. An organisation’s risk appetite will play a part in whether it rejects a risk.

Rejecting (or avoiding) a risk may be the best strategy if the consequence of the risk is too severe for the organisation to bear or the costs of avoiding the risk are unacceptable, either in terms of the mitigation costs or the lost opportunity to the business. If the consequence of the risk is greater than the organisation’s risk capacity then rejecting (avoiding) the risk may be the only viable course of action.

In practice, rejecting a risk may involve not bidding for a new contract (e.g. companies wishing to avoid corruption risks may choose not to do business in countries with a high risk on the corruption perceptions index). Certain companies may exit entire countries or industries in a bid to avoid certain types of risks.

In certain industries risks are avoided in their design, either through removal of dangerous materials or through designing equipment to be 'inherently safe' (i.e. being able to withstand conditions in excess of those permissible).

3.3 Transfer

Transfer is a specific type of mitigation (see Section 3.4) whereby the organisation transfers the entirety or an element of the risk, usually through a financial instrument, to provide some level of protection to the organisation.

There are several common forms of risk transfer, the most common of which are:

- insurance
- hedging
- contractual terms and conditions.

In the first two instances the costs of a significant (but usually low probability) risk are taken by a third party, usually in return for a fee.

In the case of contractual terms the organisation may, knowingly or unknowingly, pay a higher price for the goods or services because of the level of risk assumed. In each of the three cases outlined above, the transfer of risk is normally done by experts, and as such this will not be covered further.

There are, however, some considerations to be aware of when practising risk transfer. In the case of insurance, while it can mitigate financial risks it cannot, in most instances, mitigate reputational risks; moreover, payment of insurance may be delayed, not paid in full (if the organisation is partly at fault) or, in extreme circumstances, the insurance company many not have the resources to fulfil its obligations.

The same risks are true of contractual terms and outsourcing. Passing on all liabilities to suppliers may give the illusion that risk has been fully transferred, but if the supplier is unable to honour their financial liabilities in full it may file for bankruptcy, and the impact would then fall back on the original organisation. Furthermore, assuming that risks relating to poor quality or poor HR practices can be transferred to suppliers can be difficult to manage in practice and require a high degree of oversight.

Video content is not available in this format.

Video 1 Risk treatment

3.4 Mitigation

Mitigation is when the organisation takes steps to actively manage the risk (do something about it). This can be in the form of actions, controls or plans put in place to take action in the event of the risk actually taking place (known as fall-back or contingency plans). Mitigation may be put in place to retain a risk at its current level of assessment, especially if the organisation is satisfied that the risk is currently at an acceptable level, or alternatively actions may be implemented to reduce the level of risk to a level that the organisation finds acceptable. Mitigations are things that change the impact and/or probability of a risk.

Risk assessment (covered in Session 4) will determine the priority for treatment, with higher-impact and higher-probability risks being prioritised for treatment. The organisation may decide to classify its risks in order to draw attention to the highest-priority risks and consider how risk information is disseminated throughout the organisation using risk escalation.

Risk mitigations will usually be collectively referred to as a risk treatment plan. Consider in more detail the two most common types of risk mitigations:

- actions
- controls.

You have now looked individually at how ‘actions’ and ‘controls’ treat, or mitigate, risk. However, this is not the complete picture. To effectively mitigate risk, both ‘actions’ and ‘controls’ must be used together systematically to achieve the best outcome for an organisation.

Here is an example from risk management that uses risks and controls: UK National Risk Register.

4 Mitigation through action

If the current level of a risk is higher than your risk appetite then an action plan should be developed to reduce the level of the risk. Good action plans possess certain characteristics; these characteristics can best be described by the acronym SMART.

The definition provided uses ‘assignable’ for the A of SMART; this is relevant in the context of risk treatment because risk treatments generally need to be owned to be operating and effective. However, other examples have the ‘A’ representing ‘agreed’, meaning everyone agrees to the action being undertaken. In the sense of risk management this is misleading because there may be actions that an organisation wishes to take that people don’t agree with but none the less will be undertaken.

Here is another OpenLearn course that covers SMART in more detail. (Note that this example uses ‘achievable’ rather than ‘assignable’.)

Actions can either reduce the probability or the impact (or both) of a risk. Because many risks have more than one root cause it is important to understand which root causes and which consequences are being treated by the action plan and which are not. It is also important to consider the length of time it takes to complete the actions.

Activity 1 Managing risk through actions

Allow approximately 15 minutes

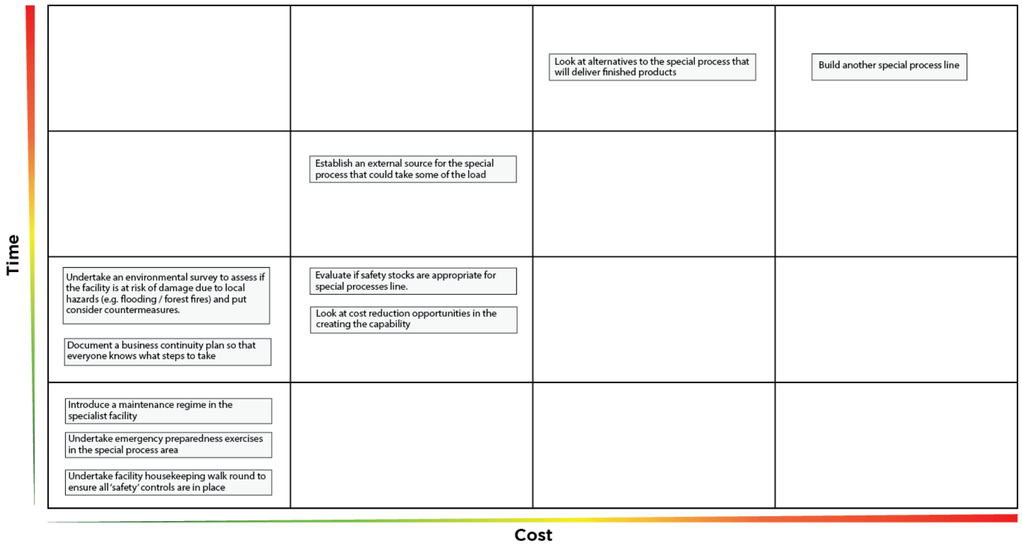
In this activity imagine you are in the role of an organisation that makes their own product and has a factory within their operations that produces these products. The factory contains a single special process line that is essential to the production of the finished product. The original introduction of the special process was a significant capital expenditure for the organisation. The organisation has already identified that the loss of the special process line is a significant business continuity risk and has identified some actions that could be undertaken to mitigate the risk. The organisation now needs to consider each of these actions in terms of risk reduction (probability and impact), the cost of implementation and the time it will take to implement.

Consider the actions associated to managing this risk. First, place the actions on a grid evaluating time (to implement) and cost to deliver the action.

Interactive content is not available in this format.

Time
Undertake an environmental survey to assess if the facility is at risk of damage due to local hazards (e.g. flooding / forest fires) and put consider countermeasures.
Cost

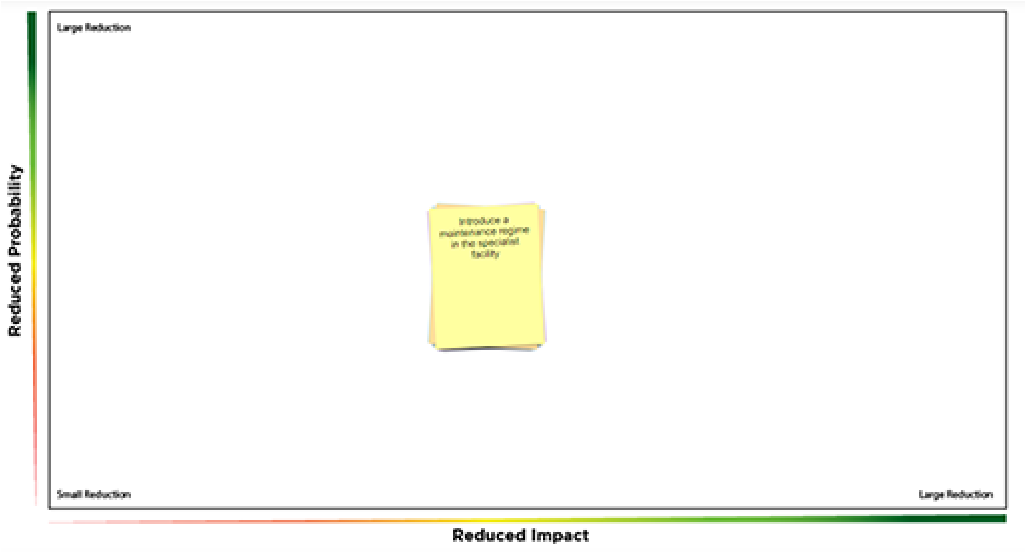
Discussion



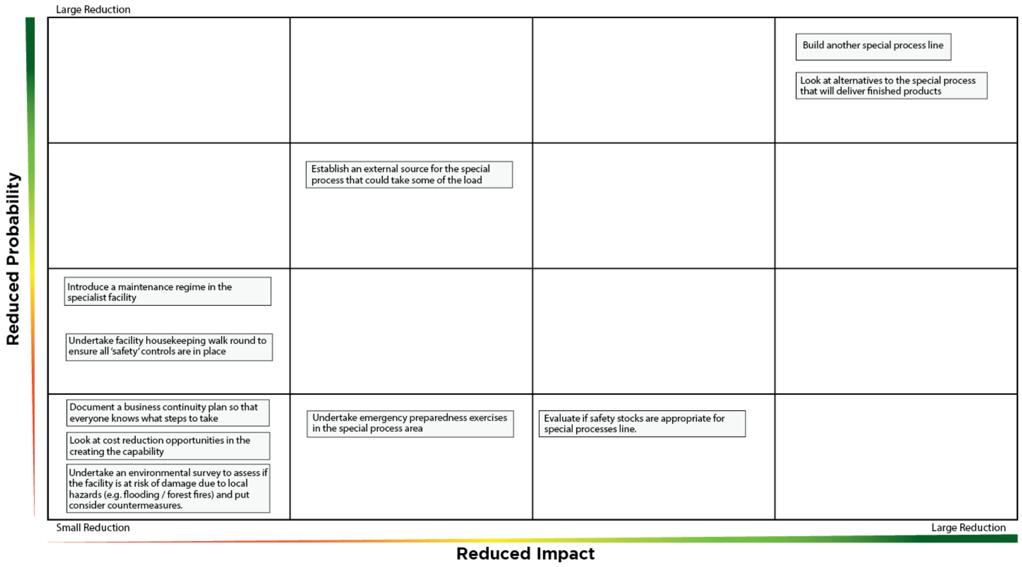
		Look at alternatives to the special process that will deliver finished products	Build another special process line
	Establish an external source for the special process that could take some of the load		
Undertake an environmental survey to assess if the facility is at risk of damage due to local hazards (e.g. flooding / forest fires) and put consider countermeasures. Document a business continuity plan so that everyone knows what steps to take	Evaluate if safety stocks are appropriate for special processes line. Look at cost reduction opportunities in the creating the capability		
Introduce a maintenance regime in the specialist facility Undertake emergency preparedness exercises in the special process area Undertake facility housekeeping walk round to ensure all 'safety' controls are in place			

Now consider how each action reduces the probability and impact of the risk.

Interactive content is not available in this format.



Discussion



			Build another special process line Look at alternatives to the special process that will deliver finished products
	Establish an external source for the special process that could take some of the load		
Introduce a maintenance regime in the specialist facility Undertake facility housekeeping walk round to ensure all 'safety' controls are in place			
Document a business continuity plan so that everyone knows what steps to take Look at cost reduction opportunities in the creating the capability Undertake an environmental survey to assess if the facility is at risk of damage due to local hazards (e.g. flooding / forest fires) and put consider countermeasures.	Undertake emergency preparedness exercises in the special process area	Evaluate if safety stocks are appropriate for special processes line.	

Much of what has been covered in the previous activity can be summarised in something often referred to as a risk burn down or waterfall chart, named after the waterfall shape the chart normally depicts. This chart, in its most often used form, has time on its *x*-axis and either financial risk measures or organisation risk scores on its *y*-axis. The chart then shows the current risk and all actions represented as steps down the waterfall as each action reduces the risk until the residual level of risk is reached. The chart can also show the target level of risk (as a gap to the residual) and potentially be adapted to show previously implemented controls, (something covered later in this session) to demonstrate the gross risk.

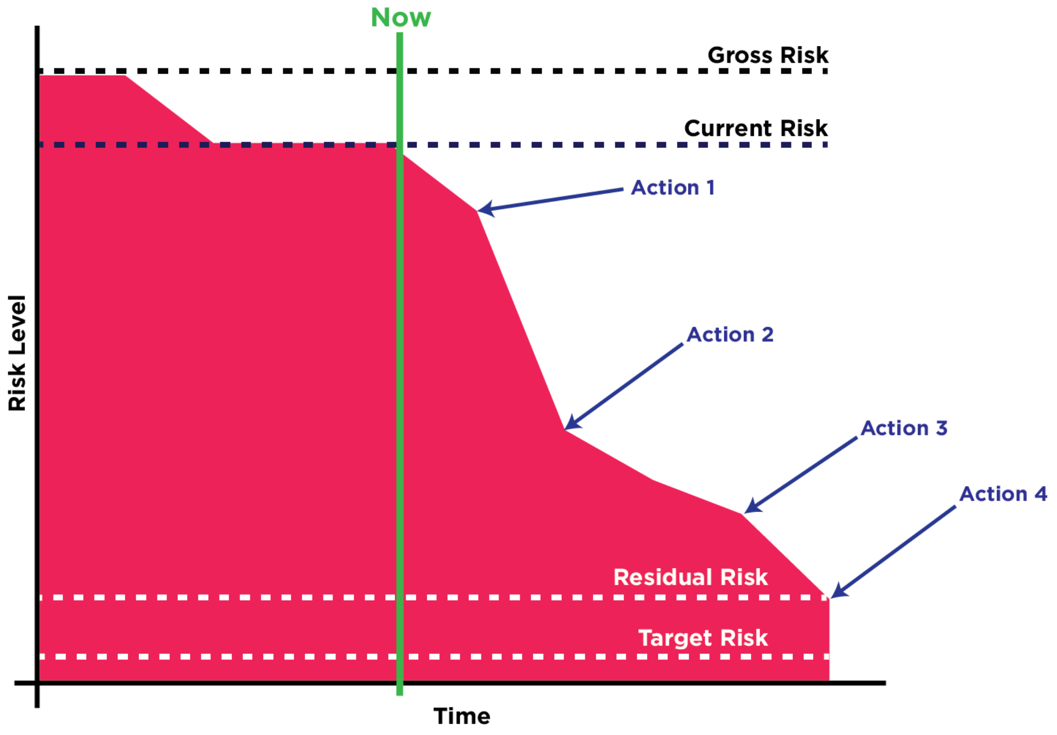


Figure 4 Risk burn down

It also needs to be considered what confidence you have that the actions will be done and will achieve their desired result, and you should adjust your plans accordingly.

Building risk treatment actions into other work plans and budgets is a powerful way to make sure that they don't get overlooked. In many organisations risk treatment actions that are not planned and funded don't happen. If treatment actions are not funded or resourced it is unlikely that they will happen.

Your residual risk level potentially tells you nothing about when this level of risk will be achieved or how confident you are about achieving it – without these two key pieces of information it should be treated with caution. In particular it should not be used in isolation for risk reporting, which is considered in Session 7, or for financial planning.

Managing actions is an integral part of any risk review process and should be aligned with the SMART objectives outlined above.

4.1 Assessing action effectiveness

Actions are an important tool to reduce the risk level being faced. Where actions are used it is important that they are effective.

An effective action will generally have the following characteristics:

- It will be targeted at one (or more) root cause(s) (or consequence(s)) and will reduce the likelihood and/or the impact of the risk by a quantifiable amount.
- There will be evidence to show how this reduction has been achieved, ideally supported by performance measures.
- The action will also have been delivered in full and will have been delivered on time.

Actions that fail to deliver the promised reduction in risk level or take longer than promised would be deemed to be ineffective.

In certain cases the action may result in new controls being introduced. In these cases the effectiveness of the new controls should also be assessed (see Section 6 in this session on control effectiveness).

5 Mitigation through controls

Unlike actions, controls are a repeatable activity that, when designed and working correctly, maintain the level of the risk at its current level. However, when a control is not designed or operated correctly the level of risk will increase.

Controls and actions are therefore used in tandem: actions are used to reduce the risk level and controls are used to keep the risk at the new, lower level. Many risks never go away so the only way to keep the risk level within appetite is by using controls.

Not all controls are equal: they have different ‘strengths’ and operate on different parts of the risk. Some controls prevent the root causes from happening, whereas others reduce the consequence(s) once the event has occurred.

5.1 Elements that make a control

A control has the following characteristics:

- It understands what is the standard is and ‘**detects**’ it.
- It measures performance, what it is actually happening, and can **interpret** compared to the standard.
- It takes **action** or feeds back to stop differences to the standard occurring or corrects the situation back to the standard.

Therefore, for a control to operate it must have the following phases:

Table 2 Phases

Phase	Description	Day-to-day example	Operational control	Financial control
Detection	There must be a method for the control to detect that a root cause is emerging or an event has occurred.	A fire alarm system needs call points, smoke detectors and/or heat detectors.	Customers report problems with a product.	Employee submits a claim for expenses and accompanying receipts.
Interpretation	There must be a method for the control to interpret the information received during the detection.	A sensor will inform the fire alarm system, which will sound a siren as a result of a ‘detection’.	An organisation subject matter expert investigates, gathers further information and reaches a decision.	Initially employee’s manager approves the employee’s expenses. Periodically expenses are reviewed for anomalies by the finance manager.
Action	There must be an action, one that is repeatable, arising from the interpretation.	The resultant siren should trigger a fire procedure that will include an	The organisation acts, which may result in a product recall, communications	The finance manager is independent of the manager and employee. She

	evacuation of employees/ visitors and summoning of the emergency services.	to notify customers and modification of the production process to prevent re-occurrence.	may detect anomalies in submissions that could indicate fraudulent activity and collusion between the two employees.

When documenting a control you should capture six key pieces of information:

Table 3 Key pieces of information

Information	Definition
Why is it there?	What is the control there to do, in the most simplistic terms.
Who owns the control?	In organisations (particularly large organisations) it is important to understand who owns (or is accountable for) a control, to be able to recognise the source of expertise in relation to the control. The person is responsible for the design of the control and, to some extent, supporting the successful operation of the control.
What, When and How?	Explain the control in terms of detection, interpretation and action. Explain when the control operates: if it is continuously 'on', does it only operate at a set time frequency? Explain how it does what it does.
What happens if errors or omissions are identified?	If the control detects a problem or issue, how does it respond? This is a specific focus on the action phase in the event of a failure being found and confirms whether the control will act against the failure.
Levels of tolerance	What level of imperfection is allowed? e.g. if a machine was counting pennies, how many can it miss in £1,000,000?
How is a control evidenced?	The information (evidence) that the organisation retains to demonstrate that the control has been operated. In some regulated industries there may be a legal requirement to retain certain documents to demonstrate that a control has been operated.

Activity 2 Elements of a control

Allow approximately 15 minutes

Look at the information about a control and highlight where the six key pieces of information can be found.

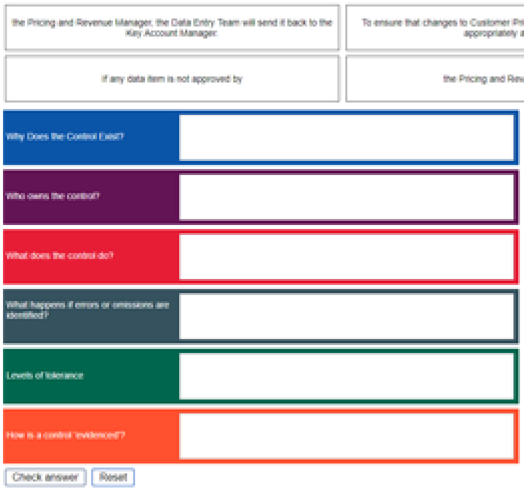
Here is a model control statement; identify the six elements of a control in this statement.

> To ensure that changes to Customer Pricing Master Data are accurate and appropriately authorised the Pricing and Revenue Manager will receive XYZ document, and approve its suitability against the prices included for the customer against the forecast and supporting information before approving by signing the document and forwarding this onto the Data Entry Team. If the Pricing and Revenue Manager does not approve any data item, the Data Entry Team will send it back to the Key Account Manager. Evidence of the control being performed is the signature on the data entry sheet held by the

Data Entry Team. Try constructing the sequence of the control yourself by dragging each part of the sequence into the correct box.

Remember to open the interactive version in a new window or tab, and it is recommended that you complete this activity using a laptop or PC, rather than a mobile device.

Interactive content is not available in this format.



the Pricing and Revenue Manager, the Data Entry Team will send it back to the Key Account Manager.

To ensure that changes to Customer Pricing Master Data are accurate and appropriately authorised

will receive XYZ document, and approve its suitability against the prices included for the customer against the forecast and supporting information before approving by signing against each data item in the document and forwarding this onto the Data Entry Team.

If any data item is not approved by

the Pricing and Revenue Manager

Evidence of the control being performed is the signature against each data item on the data entry sheet held by the data entry team.

Why Does the Control Exist?

Who owns the control?

What does the control do?

What happens if errors or omissions are identified?

Levels of tolerance

How is a control 'evidenced'?

5.2 Different types of control

Let’s look at the different types of controls that can be used for risk treatment.

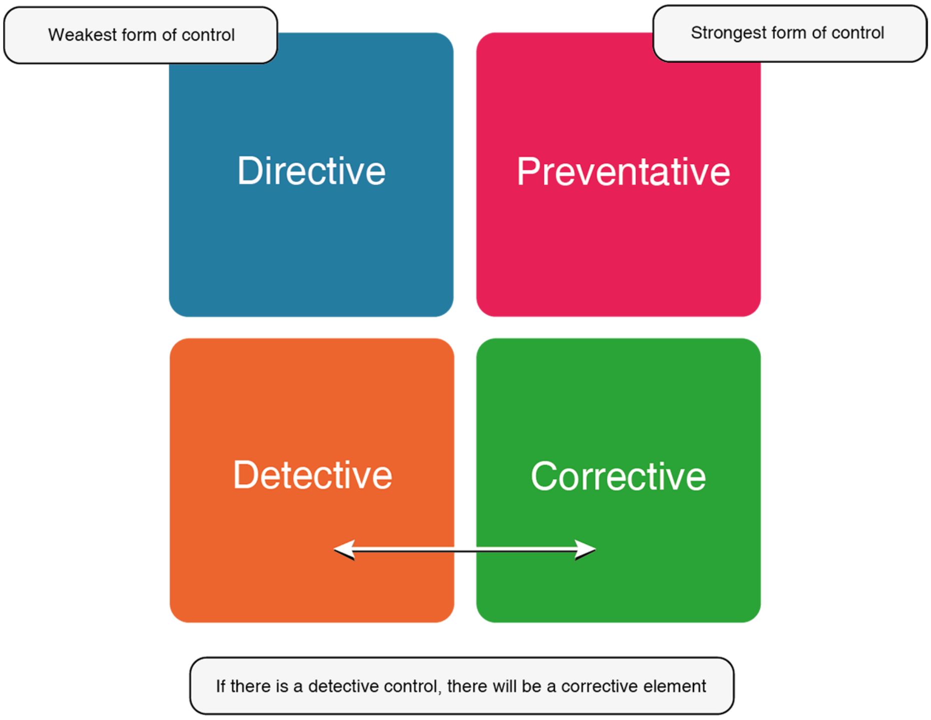

Weakest form of control
Strongest form of control
Directive
Preventative
Detective
Corrective
If there is a detective control, there will be a corrective element

Figure 5 Types of control

Directive controls give direction. These are the weakest controls. Things like policies are directive controls; they state the practice to be followed but do not stop bad practice from occurring. The Highway Code is an example of a directive control.

Detective controls aim to identify a breach after the event, an example being a financial review or audit after activity has taken place. They will often lead to **corrective** action being taken.

Preventative controls act to nullify the root cause and thus prevent the event. These are often the strongest controls. Common preventative controls include segregation of duties and IT passwords.

6 Control effectiveness

Control effectiveness must be tested in two dimensions:

- Is the control designed effectively?
- Is the control operating effectively?

It is important to make sure that the control is still working in the way that was originally intended. Because of this it is good practice to have assurance over controls. This is where people check that the control is designed and is operating as intended. It is also good practice to periodically review incidents (risks that have occurred) to see whether there are any other root causes that have occurred or haven't previously been identified, and whether the controls really are operating as intended. If control weaknesses are found then a higher level of risk than expected is being taken. This activity can be seen as testing control effectiveness.

A control must firstly be designed to be effective, in that its phases should act as intended on the root cause, the event or the consequence. If the control is not designed correctly then even if operated effectively it cannot effectively manage the risk. For example, if a fire alarm only has smoke detectors fitted on one side of a building, it will fail to detect a fire on the other side of a building as a result of control design.

If designed correctly then the control must be operated effectively. The control in its operation in the organisation, deployed as per the design, provides the required action on the root cause, the event or the consequence to be effective in operation. In the case of the fire alarm, if smoke detectors were fitted but were disconnected from the electricity supply or had their batteries removed then they would fail to operate in the event of a fire.

To test effectiveness the organisation must seek to answer two questions: have the controls been designed effectively, and is the organisation operating these controls effectively?

More mature organisations will understand the cost of running and assuring a control and be able to compare it to the reduction in risk and incidents. They are then able to perform a cost–benefit analysis for their controls.

6.1 Testing control effectiveness

Testing design effectiveness usually requires a systematic review of controls to decide whether there is an issue. Typical tests would include: reviewing the design documentation to look for potential gaps or errors; inquiry of management or subject matter experts; and observation of the process or control environment.

Testing operational effectiveness involves reviewing the activity within the organisation at its point of use. Typical tests would include: re-performance of the control; review of documented evidence of the control operating at a specific time point; or inquiry of management or subject matter experts.

7 Human factors as a controls weakness

When designing a control it is often important to think about the factors that could affect it working correctly or how the control could be bypassed or circumvented.

As with other areas of risk management mentioned previously, human factors can impact control operation. Controls that require people can often be less effective if people are:

- not trained correctly
- tired
- under the influence of drugs or alcohol
- over-worked
- distracted.

For this reason there is an increasing trend to automate controls. In fact, in many high-hazard industries there is a control hierarchy, where automated and human controls combine. In such industries mathematical models and calculations are often performed (and required by regulators) to demonstrate that the controls reduce the probability of the risk down to a level that is 'as low as reasonably practicable' (ALARP).

Activity 3 Managing risk

Allow approximately 10 minutes

Consider how manage risks are managed through controls.

Recall the special process organisation example. The action plan is complete but how is the risk maintained? You have already completed the six control items for:

- machine health monitoring
- quarterly emergency response exercise
- shop-floor IT audit.

Now it is your opportunity to complete this for operator maintenance training.

Table 4 Operator maintenance training

Information	Machine monitors	Exercises	IT audit	Training
Why does the control exist?	To provide monitoring of the maintenance status of all shop floor machines.	To provide the organisation management assurance that the organisation can respond in an emergency.	To ensure all devices within the shop floor meet the current IT security standards.	*Provide your answer...*
Who owns the control?	Head of maintenance	Head of health and safety	Head of IT	*Provide your answer...*
What does the control do?	For connected machines it provides a	Exercise the organisation emergency response plans to	Audit undertaken by members of the IT	*Provide your answer...*

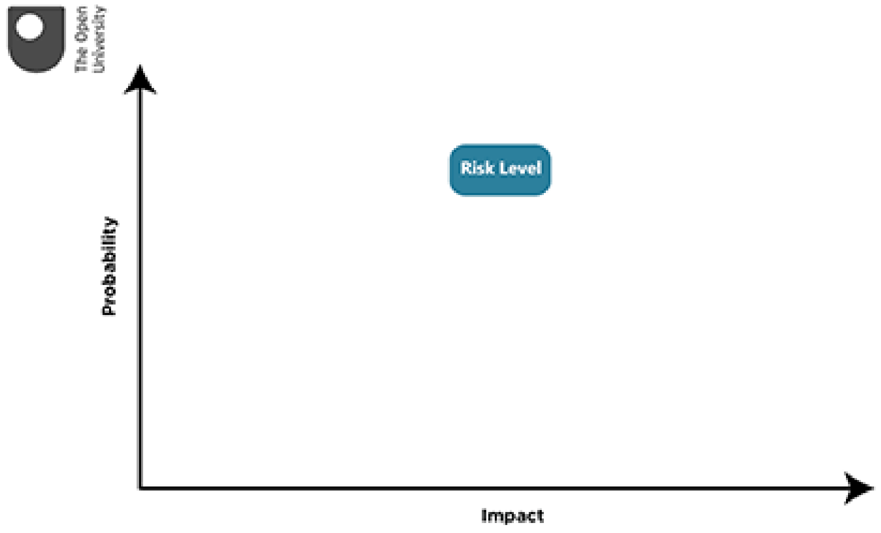
	warning indicator in the maintenance office of any machine that is outside its specified maintenance parameters. Operatives in this area must then attend this machine and resolve the issue highlighted in line with the maintenance policy and instructions for that machine.	ensure that employees and processes act as expected. Any issues found should lead to a rectification plan to fix the issues.	team to understand what devices are within the shop floor and whether they are currently up to date with IT security standards. Non-compliant items are either rectified or quarantined.	
When?	Continuous monitoring	One exercise per quarter, each in a different part of the organisation.	Normally annual but may be on an ad hoc in response to an incident.	*Provide your answer...*
How?	The machines' alerts are either hard-wired or connect via Wi-Fi to terminals in the maintenance office. When an issue is detected it sounds an alarm and sends an alert to team members.	A member of the H&S team launches the exercise and records how the organisation responds against what is planned.	Normally done remotely by the IT department, however for some older hardware this may require a physical audit.	*Provide your answer...*
What happens if errors or omissions are identified?	Operatives from the maintenance team should rectify issues.	The H&S department provide a report to the organisation management team highlighting any issues encountered. This provides recommendations that the organisation management	Non-compliant items are either 'fixed', quarantined to decide next steps or removed depending on the item, its business criticality and severity of	*Provide your answer...*

		ensure are implemented.	the issue found.	
Levels of tolerance	Machines are classified by their criticality to the process. Each level of criticality has an associated level of response and maintenance, for example some low-criticality machines do not require an immediate response.	Recommendations are classified as major and minor. It may be acceptable for some minor recommendations to be left open.	All hardware in use must meet the required standard, there is no allowance for non-compliant hardware.	*Provide your answer...*
How is a control evidenced?	The system is documented within the IT department's manual. Work carried out in response to alerts is shown in the Maintenance department's job log.	All exercises are documented with the H&S department.	IT documents the audit and their findings. The business area document follow up remediation with IT.	*Provide your answer...*

Now take a look at the following videos, looking at controls and actions working in tandem, and mitigating controls.

Video content is not available in this format.

Video 2 Controls and actions working in tandem



Video content is not available in this format.

Video 3 Mitigating controls

8 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 5 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

9 Summary of Session 5

Session 5 covered the area of risk management that is considered to provide the greatest benefit to the business: risk treatment. This session initially covered the treatment strategies available: accept, reject, transfer and mitigate. You then focused on mitigation and looked at the main areas of activity: implementing actions and operating controls.

The remainder of the session looked at how to review and assess the effectiveness of the actions and controls – a process that is essential for providing confirmation to organisations that its risk management systems are robust.

The main learning points that have been covered in this session are:

- an overview of treatment
- treatment strategies
- an introduction to mitigation through action
- knowledge of an introduction to controls
- assessing treatment effectiveness
- an example of a treatment plan.

Session 6: Monitoring and review

Introduction

So you've identified your risks, assessed them and developed a treatment plan with actions and controls. But if that is where you leave it then you have only really covered the basics.

As discussed in Session 5, risk management is all about taking action. The actions may be specific one-off activities that reduce a risk (its impact and or probability) or they may be performing a control that keeps a risk at an agreed level.

But risk, like life, is continually changing. New root causes emerge for existing risks, new risks emerge and old risks become less material or disappear completely. Sometimes best-laid plans don't deliver the expected results. Sometimes things that weren't anticipated do happen.

Your approach to risk needs to respond to these changes. Regular risk reviews act as a feedback loop to all of the other parts of the risk process, making sure that you learn and continually improve. Reviews make sure action is taken to treat risks and ensure the treatments are effective. Risk reviews are the fundamental way in which risk changes are responded to.

Monitoring and reviewing look to answer the following key questions:

- Is the organisation taking the right risks?
- Is its risk management effective?
- Is it delivering the desired results?
- It is providing useful, timely information that helps improve the organisation's decisions?

Video content is not available in this format.

Video 1 What does good risk management look like?

By the end of this session, you should be able to:

- understand the value of monitoring and reviewing risks
- understand what a risk review is
- understand what takes place during a risk review
- understand the basics of risk assurance (including the three lines of defence concept).

Now begin Session 6.

1 Are the right risks being taken?

It is essential for organisations to review their risk management practices periodically – and certainly at least annually. This allows those responsible for risk management to check that the methodologies and policies adopted remain appropriate. It also enables consideration of whether the right risks are being taken in the business – while other risks which do not need to be taken are controlled or mitigated. The business and economic climate within which organisations operate change over time and, if only for this reason, regular reviews of risk strategy are an integral part of good management.

The next three sections examine different approaches that can be taken when reviewing an organisation's risk strategy.

1.1 Risk reviews

Risk reviews look for new risks and new root causes; they look to share learning, best practice and incidents to inform the other parts of the process.

Risk reviews follow the same basic pattern as other meetings. They should have an agenda and a terms of reference. Participants should be engaged in the subject matter and not continually distracted.

Like many other meetings, most of the real value happens before and after the meeting. Before the meeting risk owners should be clear on their risks, their assessment, what treatments are in place and whether these treatments are effective.

A good meeting is also clear on *why* the information is being provided – is it to inform or is it so a decision can be made? If so what decision is required, why and why now?

Risk owners should make sure that the treatments are working, that assurance is taking place and that they are learning lessons from incidents.

The paradox of risk management, which is particularly apparent in reviewing risk, is that if done well it is rarely visible, but if done poorly this becomes all too apparent to the wider organisation.

Activity 1 Examples of good and bad risk reviews

Allow approximately 10 minutes

Look at the statements relating to risk reviews and decide which are 'good' and which are 'bad' for risk review quality. Select from the drop-down lists.

Interactive content is not available in this format.

1.2 Risk key performance indicators (KPIs)

Good risk review meetings often look to key performance indicators (KPIs) to help inform the debates and discussions.

There are many risk KPIs: some measure the process, some measure the result, some measure the amount (or value) at risk. Others look to be leading indicators predicting the direction of travel that a risk is likely to take. The key thing is to have a range of metrics that cover the breadth and depth of activity. Here are a few of the common areas to measure:

Table 1 KPIs

The amount of risk being taken	Value at risk (see Session 4) Risk profile and details of any risks out of appetite
Change of risk level	Key risk indicators (KRIs)
Risk treatment compared with plan	Amount of risk reduction achieved (compared to plan) Performance of controls (e.g. internal audit and other assurance findings) Timely completion of mitigation actions
Compliance metrics	Completion of risk training Compliance with risk management policy and other directives
Coverage metrics	Areas of the organisation performing or not performing risk management
Measure of incidents	Incidents (and re-occurring incidents) Health and safety performance (e.g. HPI (or fatality rates) per million working hours)
Maturity	Is the approach to risk management comprehensive and effective?

1.3 Deep dives

Some companies perform a ‘deep dive’ into selected risks. A deep dive is an opportunity for the attendees to understand the risk in more detail, to get a more in-depth view of the causes and consequence, and to add their perspective, providing an opportunity to highlight any areas that may have been missed and test the thinking and assumptions. It can be a good way to avoid blind spots.

The risk(s) chosen do not need to be highlighted by the exception report (i.e. the risk has failing controls or overdue mitigation actions). Instead a deep dive is an opportunity for the panel to review treatment activities (actions and controls) and make sure that they are confident the risk is being appropriately managed. It is also a good opportunity to reinforce the tone from the top that risk management is important and valued.

Some companies focus their deep dives into areas with a known problem or where incidents have occurred. These deep dives primarily focus on helping the area to improve.

Take a look at seven key questions to ask in a deep dive.

2 Is the risk management effective?

A further aspect of the periodic reviews of risk management within organisations needs to focus on the effectiveness of the controls in place which aim to ensure that risk policies are adhered to. Without good controls even the most sophisticated risk management policies risk being impaired.

2.1 The role of risk assurance

A key question that needs to be asked of any system, not least a risk management system, is, 'How do you know it works?'

A variety of different approaches can be taken. For example, you could ask:

- Is the risk level reducing?
- Are the internal controls being audited and attested to?
- Is risk training being completed?

Some people go further by measuring maturity while others measure the nature and impact of incidents that have occurred.

There is no right or wrong answer as long as you know your risk management system works and you can prove it. One way that organisations offer this proof is via a three lines of defence approach.

2.2 Risk and assurance – three lines of defence

To ensure the effectiveness of an organisation's risk management framework, the board and senior management need to be able to rely on adequate line functions – including monitoring and assurance functions within the organisation. The Institute of Internal Auditors (IIA) and the Institute of Directors (IoD) endorse the 'three lines of defence' model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided. This model is broken down as follows.

- **The first line of defence** – functions that own and manage risk. Under the first line of defence, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.
- **The second line of defence** – functions that oversee or specialise in risk management and compliance. The second line of defence consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk-related information up and down the organisation.
- **The third line of defence** – functions that provide independent assurance. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's board of directors and senior management. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of

defence. It encompasses the entire framework, the operation of the framework and the coverage and all categories of organisational objectives.

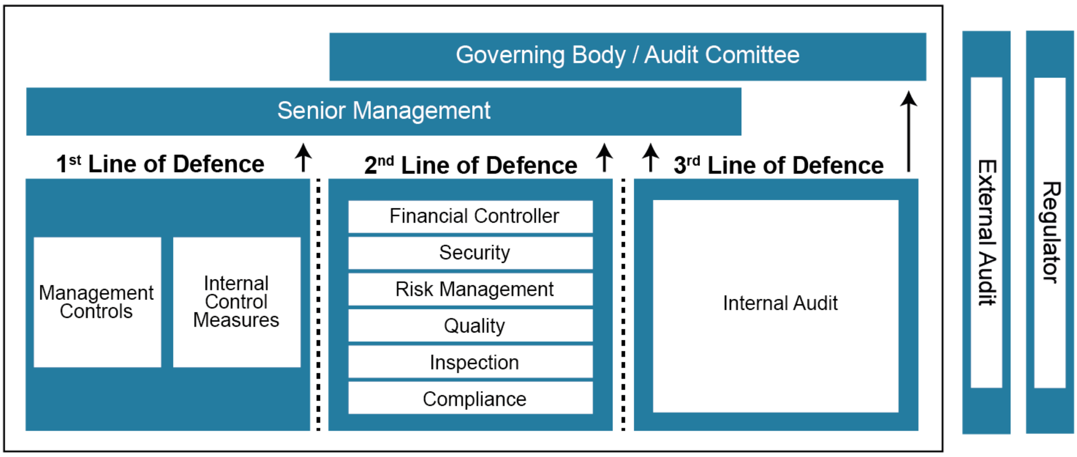


Figure 1 Three lines of defence model

3 Risk-based assurance

The term ‘assurance’ refers to checking and testing, that the oversight that should be happening is happening. People who conduct assurance can often go under the generic title of ‘auditors’. Auditors generally look for evidence that such activities are taking place.

Best practice is to have assurance activities focused on your risks – but what does this mean in practice? In the following sections you will look at how the facets of the control framework should be audited. This audit has certainly got to extend to reviewing the potential impact of behavioural weaknesses amongst employees and ensuring that these do not impair effective risk management.

You can recap the purpose of actions and controls in Session 5, Video 1.

3.1 Controls

The more important each control is (i.e. the bigger the level of risk reduction it achieves) the more important it is to have assurance. Assurance of controls should look at both the design (does the control, as designed, reduce the probability or impact of the risk?) and also the operation (is the control operating in the way the design intended?), to confirm that both are effective.

There is a ‘many to many’ relationship between risks and controls. This means that each risk could have several controls related to that risk, but also one control may mitigate several risks. Controls are often embedded in processes. Organisations often get assurance over their controls by auditing their processes. When identifying their key controls, organisation should also consider situations where they are reliant on a single control.

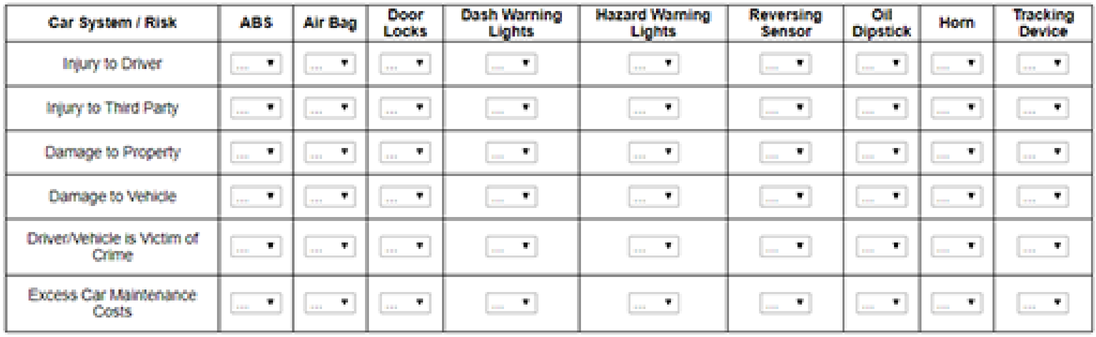
Activity 2 Risk/control matrix

Allow approximately 10 minutes

One way to manage the ‘many to many’ relationship is by using a risk/control matrix.

Click on the interactive to start selecting your answers from the drop-down options.

Interactive content is not available in this format.



Car System / Risk	ABS	Air Bag	Door Locks	Dash Warning Lights	Hazard Warning Lights	Reversing Sensor	Oil Dipstick	Horn	Tracking Device
Injury to Driver	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾
Injury to Third Party	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾
Damage to Property	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾
Damage to Vehicle	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾
Driver/Vehicle is Victim of Crime	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾
Excess Car Maintenance Costs	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾	... ▾

3.2 Mitigation actions

The more important each action is (i.e. the bigger the level of risk reduction it achieves) the more important it is to have assurance. Assurance of actions should look at:

- the effectiveness of the action in delivering the promised risk level
- the ability of the organisation to fund and deliver the action
- the timeliness of the action in respect to the risk (i.e. there is no value delivering an action after the risk is likely to have impacted)
- the level of risk reduction achieved for the amount spent on delivering the action (i.e. if the action costs more than the impact of the risk then it is unlikely to be a suitable course of action).

3.3 Risk framework

Assurance here takes the form of coverage – whether the risk framework covers the entire organisation, whether it addresses all of the areas of risk and whether all the elements of risk framework are present (see the diagram in Video 5, Session 2).

Assurance over the risk framework can often be overlooked but is very important. Assurance is often conducted by the third line of defence and looks at both the design of the framework as well as its implementation.

3.4 Human factors and internal controls

Internal controls are a widely used component of most risk management systems. But controls that rely on people can sometimes fail.

Of a more sinister nature, deliberate deception or fraud can cause an otherwise high-performing risk management system to fail. Failing to identify risks or to properly assess them, or deliberate subversion of controls for fraudulent purposes, can lead to a risk system failing to operate correctly – fraud effects all organisations, to a greater or lesser extent, and it is something that should be guarded against.

To guard against an individual committing fraud it is common to have ‘segregation of duties’ – this simply means that more than one person is involved in carrying out a task. An example is paying a supplier. Segregating duties would involve one person raising the invoice and another person paying the invoice. Segregation of duties can be subverted (got around) when people collude. For this reason an independent oversight (e.g. by internal audit) is necessary, even when, at face value, appropriate controls are in place.

3.5 Antidotes to behavioural issues

To conclude this review of the matters that need examining in an audit of risk management systems have a look at this list of recommendations for controlling (and hopefully containing) the potential adverse impact of behavioural issues.

- Learning from history.
- Reporting incidents.

- Incentives – for example, personal objectives regarding ethics and compliance, or rewards to whistle-blowers who identify frauds. These are common in the US with the whistle-blower receiving a proportion of any fine subsequently handed down.
- Incentive system designed to remove conflicts (e.g. production rate v. quality rate, sales targets v. bribery).
- Not doing risk reviews in a group but in independent one-to-one sessions.
- Reviews and assurance conducted by third parties (and without notice).
- UK government approach to horizon scanning and risk assessment (futures toolkit).

4 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 6 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

5 Summary of Session 6

Session 6 has looked at monitoring and risk reviews. You have considered why you need to monitor and review risk activity, and you were introduced to the three lines of defence model as best practice to structure the monitoring and review activity.

You then looked at some tools to support monitoring activity for risk management, discussing the use of risk KPIs and the concept of a deep dive to ensure the right information is reviewed for risks and that those risks are ‘brought to life’ for those involved in their management.

Finally in Session 6, you looked at risk-based assurance and considered an overview of what would be expected from any risk-based assurance activity undertaken in an organisation as part of risk monitoring and review.

The main learning points that have been covered in this session are:

- the value of monitoring and reviewing risks
- what a risk review is
- what takes place during a risk review
- the basics of risk assurance (including the three lines of defence concept).

Session 7: Managing risks: communicating and reporting

Introduction

In response to a number of high-profile corporate failures (Enron, WorldCom, etc.) regulators have introduced standards that apply to large listed companies. References to risk management are commonly contained in listing rules or agreements (India, UK and US), company laws (Austria, Germany, Turkey and Japan), or stock exchange laws (Mexico).

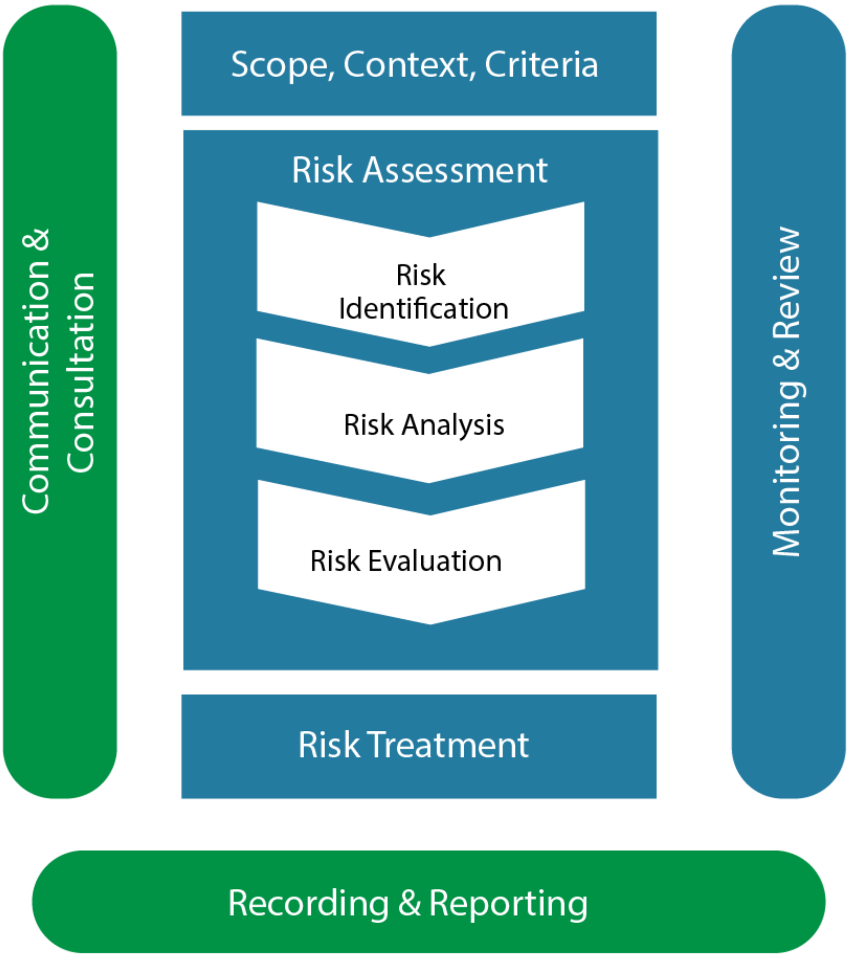


Figure 1 ISO 31000 diagram – communication & consultation and recording & reporting

Video content is not available in this format.

Video 1 Good risk management

Additional guidance that is sometimes provided, such as the UK's 'Turnbull Guidance', mainly refers to audit and internal controls. One exception is Singapore's Corporate

Governance Council, which in May 2012 issued guidance specifically on the governance of risk management ('Risk Governance Guidance for Listed Boards').

Video content is not available in this format.

Video 2 History of the UK Corporate Governance Code

History of the
UK Corporate Governance Code

In 2014, the OECD produced a review of Risk Management and Corporate Governance.

As the OECD report highlights, all of these codes have a similar theme. Whether it is Sarbanes Oxley (or SOX) in the USA, the Code Tabaksblat in the Netherlands or the Corporate Governance Code issued by the Financial Reporting Council in the UK, the requirement is to manage opportunities and risks and if companies choose not to comply to be able to explain why they have chosen not to do so.

All of the main risk management standards place a large importance in having top-down support for risk management (see ISO 31000 and COSO).

Increasingly there is a consensus on the need for an organisation's board to play a leading role in the management of risk. All of the codes make clear the importance of the board in setting the right 'tone from the top'. This is why good corporate governance, underpinned by codes and requirements, places a clear onus on boards to actively engage in risk management.

By the end of this session, you should be able to:

- evaluate the roles of key stakeholders and their communication needs
- understand the relationship between programme, business and functional risks, and how to communicate and consult between them all
- understand further the impact of human factors on risk management.

Now begin Session 7.

1 How are the requirements implemented at Rolls-Royce?

The Rolls-Royce board members are clear on their role in managing risk and it forms part of their accountabilities. The board owns the principal risks and oversight of these is carried out by the full board or delegated to one of the board subcommittees. They will perform a deep dive into each of the group principal risks at least once a year (deep dive was covered in Session 6). You can see in the Annual Report that the code is referred to and committees describe how they oversee the principal risks.

Risk is also considered as part of the board's decision-making process. One way in which this is done is by requiring that every paper that is presented to the board is clear on the risks that it raises and addresses.

2 Working with stakeholders

Effective risk management is about delivering reliable, timely and useful information that helps improve decisions. A prerequisite is therefore to understand who the decision makers are and what information they need.

The board is one group that plays an important role in setting the tone for how risk is managed but other stakeholders may play an equally important role and this will to a large extent depend on the business in question. The tone for risk may be set by regulators, such as the US Food and Drug Administration (FDA) in pharmaceuticals, the Federal Reserve (the US central bank), the UK Financial Conduct Authority (FCA) or European Central Bank (ECB) for banks, or by governments, non-governmental organisations (NGOs) or simply by industry norm.

A stakeholder map is a useful tool that can be applied to identify stakeholders and understand the most appropriate way to engage with them. This is typically done using a two-by-two matrix with ‘Influence’ on one axis and ‘Power’ on the other, both ranging from ‘high’ to ‘low’. These are sometimes undertaken alongside a communication strategy known as a ‘RACI’ (responsible, accountable, consulted and informed) and with richer forms of communication (such as one-to-one and face-to-face) used with groups who have ‘high’ Power and Influence, whilst more generic forms of communication (such as newsletters or web pages) used with groups with lower levels of Power and Influence.

Activity 1 Communication routes

Allow approximately 10 minutes

Consider different communication routes for the different ‘risk audiences’.

- **Safety risk**: There is a risk around cut hands from handling sharp metal chips.
- **Finance risk**: There is a risk around ABC within some sales activity.
- **Legal risk**: There is a risk personal data could be stolen (cyber attack).
- **Business continuity**: There is a risk to production if the factory is lost due to a fire.

Interactive content is not available in this format.

Interactive content is not available in this format.

Interactive content is not available in this format.

Interactive content is not available in this format.

3 Risk ownership in a matrix business

As discussed previously, many businesses today operate a matrix structure. Put simply, this means that the typical employee has two reporting lines: one to the business unit in which they work and another into the function to which they belong.

Video content is not available in this format.

Video 3 Matrix structure

Risk in a Matrix Business

Businesses that operate in such a fashion need to design their risk systems carefully to avoid duplication of effort or, potentially worse, a situation where no one feels accountable for managing a risk because it is always someone else’s job.

The typical approach to avoid these issues is as follows:

> Risks are owned by the part of the organisation that suffers the consequences (or gets the benefit) from the risk. This will typically be a business unit.
>
> This does, however, leave one remaining issue: how to deal with risks that occur from the same root cause (e.g. failure of a common IT system) that impacts more than one business unit?
>
> Here functions can play a key role. By aggregating the impact of the common root cause across multiple business units, risks can be properly assessed and prioritised accordingly.
>
> Functions have a role in breaking down silos. As discussed earlier the company management team often see across multiple business units and as such are well placed to identify hidden risks (often risks identified by one business unit but not by another), setting standards for managing certain types of risks (e.g. safety and compliance risks) and sharing best practice.

4 Communication and consultation

Risk management, done well, is an excellent way of breaking down silos, sharing information across an organisation and allowing different parts of the organisation to learn from one another.

At its most basic this could involve learning from incidents in one part of the business to prevent them occurring in another part.

In some industries or for certain types of risk this information is shared across the industry; examples include fraud risk in the financial services industry and health and safety risks in the chemicals industry.

Communication is important in each of the different steps of the risk process and can be broken down as follows:

Identification: A broad span of skills and experience is important to make sure that all risks have been identified and that no risks have been missed. Learning from past incidents is important as is learning from other parts of your own organisation or learning from other companies.

Assessment: Quantification of risks often requires the support of finance teams (who can fully model the financial impact of risks). Understanding of past incidents and the actual performance of existing controls (and assurance findings) also help to inform assessment of risk. Risk assessment and treatment are closely related. As the situation changes the risk assessment should be updated.

Treatment: Treatment of risk is often done by many different parties; some risks can have many different people accountable for treatment actions or controls. The risk owner needs regular conversations with action and control owners to make sure that their treatments are effective and deliver the required level of risk mitigation. Treatment owners may be treating many different risks so communication and consultation is very important.

Reporting and review: Most organisations have scarce resources and cannot afford to grasp all the opportunities that are presented or treat all of the risks they face. It is important that decisions are made about which risks will be treated and which will not, and to communicate these decisions in a way where people are clear which risks will be treated and which will be accepted. In this way the organisation can then plan accordingly to account for the decisions that have been made.

5 Recording and reporting

This section considers what is involved in the recording of risks and in the reporting about them to senior management within organisations.

5.1 Risk recording

As discussed in Session 3, it is common for risks to be recorded in a risk register. A risk register can be captured in a variety of ways ranging from a piece of paper to a purpose-built IT system. Irrespective of the tool used the information captured is the same.

In large organisations there may be many risk registers. Risks from higher-level registers may be flowed down to lower-level registers and risks from lower-level registers may flow up to higher-level registers (normally due to their level of impact). This can mean that certain risks can 'appear' on more than one risk register, either in their own right (because of their potential impact) or as broader 'aggregated risk'.

5.2 Risk reporting

It is common for large organisations to set thresholds for risks (typically based on their impact and probability) above which they need to be shared (or reported) with certain groups of people; these are commonly called 'escalation criteria' and are often linked to 'delegated authority' levels. Very large organisations may set several such levels (e.g. a level for the project manager, a separate level for the managing director and a separate level again for the board).

Risk reporting provides information to help decision making, enables risks to be communicated across the organisation and also drives improvements to the way in which risk is managed.

There is no right or wrong answer to how to do this and different organisations have different ways of approaching it, but the fundamental requirement is accurate, complete, unbiased, timely information about risk.

Reporting to the board

In most organisations it is the Board of Directors who are ultimately responsible for the management of risks and they will commonly look to:

1. ensure there is an effective system of risk management in place
2. ensure that treatment activities are appropriate and effective
3. ensure that the right risks are being taken and that the organisation is operating within its risk appetite.

Reporting can be done to the board as a whole but certain activities are often delegated to specific committees of the board. In general there are two approaches:

- An audit committee looks at the effectiveness of risk systems while a separate risk committee focuses on the content of the risks and the effectiveness of the treatment activities.

- An audit committee looks at both the effectiveness of risk systems and the content of the risks and the effectiveness of the treatment activities.

Video content is not available in this format.
Video 4 What do the Board want?

5.3 Reporting considerations

Larger organisations should give thought to how risk reporting and reviews flow down the organisation. Again there is no right way to do this, but it is typical for smaller units to have their own local reviews. The only difference between these and higher-level reviews tends to be the size (impact) of the risks being discussed.

The cadence (timing and frequency) of risk reviews should be based on the business in question and the pace with which risks can emerge, change and be mitigated. There is, therefore, a broad spectrum of review frequencies ranging from daily to annually.

In cases where there is a lower frequency, thought should be given to how exceptions will be reported and key decisions made. This is often done by linking risk to the organisation's delegated authorities and incident reporting processes. A standard risk review is described below:

Risk committee terms of reference

Download the read-only or the read + write version.

A good risk review will often conduct a review by exception and a deep dive.

The review by exception looks at things that are not as they should be, which would include:

- incidents (risks that have happened)
- control weaknesses (based on near misses or assurance findings)
- mitigation actions that have not worked or are off track
- risks that are greater than appetite (and, in particular, those that will remain so for a long period of time)
- changes to the risk profile, particularly new risks (or new root causes) and risks that are to be closed.

A deep dive will be undertaken as described in Session 6. This should be an opportunity for the panel to review treatment activities (actions and controls) and make sure that they are confident the risk is being appropriately managed.

Take a look at the Reporting Toolkit (read-only).

6 Risk systems and tools

There are a variety of risk tools on the market that help support communication; these range in price from pennies to many millions of pounds. Organisations like Gartner offer a summary of 'the best' tools available, but these will often focus on 'GRC system'. GRC, or Governance, Risk and Compliance, are tools that look to bring together, under one umbrella, all risks, controls, assurance and incident information. The choice of tool will depend on the size and complexity of your organisation and the number of users.

The common requirements vary from a simple database in which to store risk, to more integrated systems where risk, controls and assurance activities are linked. Some of the more advanced tools even link to operating and Enterprise Resource Planning (ERP) systems and thereby provide 'real time' control monitoring.

That said the basic requirements for any of these tools are common and should include:

- ease of data entry
- ease of data extraction and reporting
- ability to link one risk to many root causes, many controls and many mitigation actions
- ability to link one consequence, root cause and one control to many risks
- ability to present visually (including charts and graphs).

Many organisations find that one tool cannot meet all of their needs and therefore use separate software specifically designed for a particular solution. This section only gives a brief overview into system tools and anyone interested in this area should undertake their own research before deciding on a particular approach to risk systems and tools.

7 Human factors associated with risk reporting

Risk reporting and communication can be made more difficult due to ‘human factors’. Some common factors are:

Table 1 Human factors

Human factor	Description
Optimism bias	People believe that negative events are less likely and positive events more likely than is the case.
Burying bad news	Where bad news is not shared and even hidden. The case of Nick Leeson at Barings Bank is a classic case of burying bad news. The large losses he sustained were only found when they became too large to hide.
Hero culture (that loves firefighting)	A hero culture is one where hard working and highly talented people, through ‘sheer strength’ and ‘will power’, fix seemly insurmountable problems. The problem is that if these people get praised and highly rewarded for their efforts, whereas people who prevent the seemingly insurmountable problems from arising in the first place are ignored, poorly rewarded and overlooked for promotion, the organisation will tend to be one which moves from crisis to crisis without an effective approach to risk management that secures long-term growth
Organisation silos	Different departments, locations or groups do not share information, goals or processes with one another. This impacts operations, efficiency and morale.
Loss aversion	Is the psychological tendency to prefer to avoid a loss rather than acquire a similar gain?
Group think	Does the organisation favour internal harmony and consensus over getting the right decision? Group think is often associated with irrational or dysfunctional decision making.
Poor estimate of risk	The assessment of risk can be flawed if the activity is new or novel or if the risk rarely happens. Estimates can also be effected by behavioural factors and incentives. For example, the incentives may be to downplay or underestimate threats, in an attempt to make a situation look better than it really is. Common examples include large capital programmes and acquisitions, where underestimates of risk lead to large overruns in cost and time or destruction of shareholder value.
Halo effect	Recent or more memorable events are more highly thought of, and the impression created in one area (e.g. a previous activity) influences opinion of competence in another, unrelated, area.

Activity 2 Controls and human factors

Allow approximately 15 minutes

Look at the controls below and consider how human factors might influence their effectiveness.

Control 1

Which human factor might be present?

- A company decides to outsource some work and in doing so releases some control of the standards by which its products are produced.
- After successfully tendering the work and after a number of months of high-quality production, the customer services team begin to receive some complaints. Looking into this the company finds a number of small flaws in the outsourced components.
- Company representatives visit the outsourcing provider and find that the local entry criteria is lower and the induction process is far shorter than they would have expected.

○ Competence (person not properly trained)

○ Fatigue (person is tired)

○ Impaired performance (under the influence of drugs or alcohol)

○ Distracted (other things catching their attention)

○ Over worked (too much work to properly operate the control)

○ Pressure

○ Deliberate action

Control 2

Which human factor might be present?

- A company provides customer support through a team of field services representatives. These representatives travel to customer sites within a geographic region and provide service and maintenance to customer products. Representatives must adhere to strict processes to ensure that they remain safe whilst in the field and that they maintain a customer's product in a safe manner.
- Recently a service representative has had to go on long-term sick leave. To cover the resource gap, colleagues from neighbouring regions are filling in. However, it is peak season for product use and late one evening a representative receives a call to attend to a malfunctioning product at the furthest point from her base location.

○ Competence (person not properly trained)

○ Pressure

○ Fatigue (person is tired)

○ Impaired performance (under the influence of drugs or alcohol)

○ Distracted (other things catching their attention)

○ Over worked (too much work to properly operate the control)

○ Deliberate action

Control 3

Which human factor might be present?

- An employee is invited to attend a week-long conference and training event overseas representing the company. At the end of the week there is a function in the evening and a number of the delegates stay on late into the evening.
- The employee was booked onto an early flight, but had taken the precaution to book a taxi to the airport. However, the employee is called by the airline very early in the morning to advise that due to a security alert at the airport early outbound flights have been cancelled and that the only way for the employee to get to his destination would be to fly from another airport around 100 km away and at an earlier time. To do this the employee would have to drive after having drunk the previous night.

○ Competence (person not properly trained)
○ Pressure
○ Fatigue (person is tired)
○ Over worked (too much work to properly operate the control)
○ Impaired performance (under the influence of drugs or alcohol)
○ Distracted (other things catching their attention)
○ Deliberate action

Control 4

Which human factor might be present?

- An company has a relaxed approach to personal use of the internet at work: employees are permitted to use the company internet for personal use as long as it does not interfere with employees hitting their objectives.
- At the end of the year one of the sales managers reviews his team's performance. The employees have hit their targets, but errors have been alarmingly high. The errors have cost the company in terms of re-work, delays and in some cases refunds.
- The manager reviews internet traffic for the team and finds that it is considerably higher than other teams in the company. The manager also notices that internet usage goes up around major sporting events and errors also increase at the same time.

○ Pressure
○ Competence (person not properly trained)
○ Fatigue (person is tired)
○ Impaired performance (under the influence of drugs or alcohol)
○ Over worked (too much work to properly operate the control)
○ Distracted (other things catching their attention)
○ Deliberate action

Control 5

Which human factor might be present?

- A production line produces high-volume products (thousands of items per hour). To ensure that products meet the required standard, a quality control department undertakes a series of tests on a product sample. The sample of products is taken for every 10,000 products produced.

- The company acquires a competitor's production line of a similar scale and, to cut costs, closes its quality control department transferring all quality control work to one department. The original department remains unchanged.

○ Pressure
○ Competence (person not properly trained)
○ Fatigue (person is tired)
○ Deliberate action
○ Impaired performance (under the influence of drugs or alcohol)
○ Distracted (other things catching their attention)
○ Over worked (too much work to properly operate the control)

Control 6

Which human factor might be present?

- A despatch manager is preparing a product for despatch/ Partway through the preparation she realised that certain paperwork is missing and contacts the customer services team requesting clarification and further paperwork in line with the company process.
- Shortly afterwards the despatch manager receives a call from the director of the customer services team demanding she despatches the product ASAP because a customer needs the part to keep them operational.
- To ensure customer satisfaction the despatch manager finds a way to get the part despatched.

○ Competence (person not properly trained)
○ Over worked (too much work to properly operate the control)
○ Deliberate action
○ Distracted (other things catching their attention)
○ Pressure
○ Impaired performance (under the influence of drugs or alcohol)
○ Fatigue (person is tired)

Control 7

Which human factor might be present?

- A company is sourcing a major supplier to undertake work for a major government programme and must follow a set of sourcing guidelines provided by the government.
- To gain experience the process of initial supplier selection is given to a relatively junior member of the team. It is their role to create a shortlist of suppliers that will then go thorough a formal tender process.
- A relative of the team member works at one of the potential suppliers and invites the team member to a corporate hospitality box at a major sporting event.
- At the event they begin to discuss the shortlist.

- Competence (person not properly trained)
- Over worked (too much work to properly operate the control)
- Pressure
- Distracted (other things catching their attention)
- Deliberate action
- Impaired performance (under the influence of drugs or alcohol)
- Fatigue (person is tired)

8 This session’s quiz

Check what you’ve learned this session by taking the end-of-session quiz.

Session 7 practice quiz

Open the quiz in a new window or tab then come back here when you’ve finished.

9 Summary of Session 7

You were introduced to Session 7 by looking at the worldwide approach to legislation around reporting on corporate risk management. You will have recognised that much of the legislation was similar and, having evolved from large corporate failures, placed an emphasis on recording and reporting to ensure managers were aware of what was happening in the organisation. You were shown how this happened in Rolls-Royce as an example.

You then looked at communication within an organisation, in relation to risk management, considered some of the challenges, such as large matrix organisations, and looked at some of the solutions (e.g. RACI matrices).

You then considered risk reporting and looked at some best practice opportunities as well as some of the considerations to be taken into account when developing an approach to risk reporting. The session concluded by considering how systems can assist risk reporting and the human factors that are present in reporting activity.

The main learning points that have been covered in this session are:

- the roles of key stakeholders and their communication needs
- the relationship between programme, business and functional risks and how to communicate and consult between them all
- the impact of human factors on risk management.

Session 8: Risk specialisms

Introduction

In this, the final session of the course, you will look at specialisms in risk management. The need for risk management is expanding as the business environment changes and companies realise the significance of needing to manage risk properly (and the impact of not managing risk) as well as the benefits that good risk management delivers to their bottom line. For those aspiring to a career in risk management there are many routes to a role in risk and the background to those working in the field is as diverse and varied as the variety of risks that an organisation may face.

Risk managers are present in almost all industries and fields, although in some industries it may not be as explicit as in others; a short search of the internet for risk vacancies will reveal the potential of hundreds of different roles available involving risk management. To provide some insight into a career in risk management you will now focus on just five risk specialisms in more detail:

- business continuity and crisis management
- internal control management
- project risk management
- emerging risk management and horizon scanning
- safety risk management.

By the end of this session, you should be able to:

- understand the variety of risk management specialisms
- appreciate which of these specialisms may be appropriate for you currently or in your future career.

Now begin Session 8.

1 Business continuity and crisis management

Business continuity (BC) is a systematic way of managing potential or actual disruption in order to promote the long-term health, viability and reputation of the business. Business continuity and crisis management professionals support businesses in ensuring business continuity plans are in place, ensuring the plans are robust and well thought through and testing or exercising those plans to ensure that they will work. Some business continuity managers are also involved in supporting the business in responding to incidents.

Video content is not available in this format.
Video 1 A BC expert on what BC is

In its simplest form, business continuity is about:

- understanding how your business works and what is required for it to operate (e.g. how it is structured, who its customers are, etc.)
- being aware of the internal and external risks that your business faces and understanding whether these can be reduced (e.g. through contingency arrangements, etc.)
- being aware of what the main processes within your business are, what would happen if you lost any of them and which ones would be absolutely critical to making your business operate effectively (e.g. without your delivery vehicle for a day, you won’t be able to ship to your customers)
- having plans to recover your critical process in the event of disruption or complete loss
- having a response plan in place so that your business can respond quickly and consistently to any incident (including out of normal working hours).

Business continuity is important to a business because, if done well, it can add value by:

- building a better understanding of your business – in undertaking business continuity planning and exercises you will often be surprised by what you don’t know or assumed you knew
- building customer trust and confidence in you
- promoting teamwork amongst your employees and external parties on whom you are dependent.

Video content is not available in this format.
Video 2 Using business continuity in business

An important part of business continuity is ensuring that plans will work. Thankfully extreme real-life incidents are often few and far between so it is not often that a business continuity manager can assess their plans against real-life information. To overcome this difficulty, business continuity managers rely upon exercises to come as close as possible to real-world testing without an incident occurring. Undertaking business continuity exercises are a great way of bringing business continuity to life. The benefits of a business continuity exercise are:

- it raises awareness of your business continuity plan
- it raises awareness of key roles in your business continuity plan
- it builds confidence in tackling incidents
- it promotes close team-working
- it allows you to test approaches and make mistakes in a safe learning environment
- it allows you to learn lessons and make changes to your business continuity plans so that they are up to date
- it can be tailored to suit your required level of complexity and time available to run it (a simple business continuity exercise can be run in less than an hour).

Activity 1 Putting business continuity management into practice

Allow approximately 20 minutes

Lion Down is a textiles machining company based in Birmingham in the West Midlands region of the UK. Imagine you're the business continuity manager at Lion Down. Read the information below and consider the questions asked.

Key company information is as follows:

- 100 employees (70 of whom are skilled sewing machine operators or product finishers; 20 are supervisors, managers or back-office support; 10 are in the sales and purchasing function).
- The site runs a 6-day week, 8am – 6pm.
- Contracts are mainly full-time and salaried. Twenty of the skilled sewing machine operators are contract staff who are brought in based on demand.
- The sales and purchasing team are located remotely and travel to Asia and sub-Saharan Africa is common for them.
- Production is centred on a single site in Birmingham, close to the M42 and M6 motorways and Birmingham International Airport. The site was constructed in 1928 and has undergone a number of additional upgrades. There are a number of industrial manufacturers located in the vicinity and the site's immediate neighbour is Board Stiff, a cardboard and plastic recycling plant.
- Trade union membership is common across the workforce with the General Workers Union being the main representative body.

- Lion Down's main customers are suppliers of fine bed linen to major UK high-street retailers. A plan to market finished product directly via an online retail partner was shelved before the start of the current trading year.
- Finished goods are shipped by an outsourced logistics provider, Hev-E-Lift. This is the third logistics provider that the company has used in the last five years.
- The company has a web page and its own presence on Facebook and Twitter. Each of these are maintained by Lee Valone, who looks after all the company's IT systems (including the accounts management and shipping systems). Lee has only been at the company for six months and this is the fifth place he's worked in the last three years.

What are the biggest risks that your business faces and how does it manage them?

Figure 1

Provide your answer...

Discussion

For Lion Down:

- **Facility/equipment**. The age of the building at our main site gives us some concern. At a recent management meeting, our Health & Safety lead raised a number of concerns regarding risk to the integrity of the roof, the electrical supply and the possible presence of asbestos in some areas. We plan to commission an external provider to carry out a full property survey in order to indicate the necessary works required to keep the site operating. Having a single site causes us some concern, so we are looking at entering a mutual agreement with Rag Trade Limited to move production in the short term in the event of catastrophic loss.
- **People**. We need to guarantee a minimum staffing level to meet demand and this varies considerably. To meet demand, we need to communicate effectively with our agency staff provider to ensure that we have the right people with the right skills to do the job. We also need to build and maintain a good working relationship with our trade union rep to ensure that salaried staff do not feel undermined by agency staff (time lost through industrial disputes is currently at an all-time low). Our risk register tells us that our biggest people risk is a pandemic and we have to think about not only how we manage staff absence at our main site, but we also need to think about how our sales and purchasing team's ability to travel may be affected.
- **Systems/documents**. We are concerned that we only have one person as out IT expert. This has been flagged as a single point of failure and we are looking to bring in a part-time contractor to work with Lee Valone. Our back-office team keeps a risk register and from this carries out a simple Business Impact Analysis to look at the 'what-if' scenarios that might affect us.
- **Logistics**. We are monitoring our logistics contract, given the fact that we have had a number of providers in a short space of time. Our Operations Director has been tasked with scoping whether we can move to a multi-provider contract to spread the risk.

Where is your Business Continuity Plan located and how does it work?

Figure 2

Provide your answer...

Discussion

For Lion Down:

- **Facility/equipment**. In addition to a map of the site, the BCP contains a full inventory of key machinery and resources (along with 24 hour contacts for relevant providers) that are required to restore business operations. Restoration of business operations is covered by a separate and distinct 'Recovery' checklist in the BCP and any recovery operation is led by a designated member of the Incident Management Team.
- **People**. The HR Director leads on all people-related issues once the BCP is activated. To support this activity, the HR Director can access the online employee database and payroll records (each is backed up automatically every 12 hours and access can also be gained via the cloud). The HR Director meets with the General Workers Union rep every quarter, part of which includes a discussion on BCP activation and access to employee data.
- **Systems/documents**. The BCP is a simple document that contains:

  a. A crisis response checklist.

  b. the composition of the Incident Management Team (IMT) – including deputies for each role and a template IMT meeting agenda

  c. a role map for each IMT role, outlining key crisis responsibilities

  d. a list of key contacts (staff, agencies, utility providers)

  e. a map of the site

  f. a copy of the BIA with key actions and considerations listed against our main risks

  g. a recovery checklist.

  Our BCP is located in a fire-proof cabinet in the main office, with a duplicate in the Operations Director's office. There is an electronic copy on the company's shared drive and on three encrypted memory sticks that are held with senior management. We are also about to move to a new cloud-based IT operating system that allows anyone with a role in the BCP to be able to access the plan via any work or personal device with internet access.

- **Logistics**. Contact with Hev-E-Lift is part of the immediate Crisis Response checklist and it is part of the agreed logistics contract for contact to be made at any time, 24/7, to Hev-E-Lift's Regional Operations Centre in Dudley, West Midlands. If required, Hev-E-Lift's duty Operations Manager can dial into the IMT. During partial or total loss of the facility, any stock in transit can be held at a Hev-E-Lift depot initially for up to 72 hours at no additional cost to Lion Down.

When was your Business Continuity Plan last exercised and what were the main lessons that were learned from this?

Figure 3

Provide your answer...

Discussion

For Lion Down:

The recycling plant is recognised as a potentially significant fire risk and an incident on their site would probably limit or cease access to our main site and bring production to a standstill. For this reason, three months ago we conducted a joint exercise with Board Stiff; this followed a genuine incident at the recycling plant, where a small fire took hold in its packing plant.

The exercise consisted of a no-notice activation of the IMT, with representation from Board Stiff and Hev-E-Lift, both of which agreed to have their respective Operations Managers dial-in to the meeting. Key lessons identified from the exercise were:

- **Facility/equipment**. A question was raised about whether the dye process line should be shut down completely in the event of a full evacuation. A concern was raised about the possible overheating of a key component if left unattended for a protracted period (which could then lead to a further fire risk). The Director of Operations took an action to liaise with the Fire Engineer and the local Fire & Rescue Service to determine whether a ‘double-knock’ capability should be built in to the fire alarm to allow confirmation of a genuine incident before evacuating and shutting down the dye process line. The Health & Safety Officer also added that a capital investment scheme to retrofit sprinklers to the main site should now be re-visited.
- **People**. The IMT was mobilised successfully within 15 minutes of initial notification and the meeting was chaired by the Chief Executive, Ed Spread. There was some discussion about whether the main site should have been evacuated by activation of the fire alarm if this incident had happened for real. The general view was that the Fire Marshal should be alerted as soon as possible in the event of a fire at Board Stiff and a decision should then be taken whether to

keep all staff indoors or evacuate them. It was noted that depending on wind direction, the advice from the emergency services may well be to stay indoors, close all windows and monitor local radio and/or social media for regular updates from the emergency services.

- **Systems/documents**. All IMT members gained access to the BCP the shared drive. As part of the exercise, anyone in possession of an encrypted memory stick containing a back-up copy of the BCP was required to print it out. This highlighted that the BCPs on the stick were an earlier version (Version 2.0), whereas the current and up-to-date version is Version 3.0. A lesson was identified for all BCPs to be at Version 3.0 with immediate effect and for version control to be checked and confirmed every quarter by the Operations Director.
- **Logistics**. In accordance with the crisis response checklist, the IMT attempted to make contact with Hev-E-Lift’s Duty Operations Manager at the Regional Operations Centre. Two calls were made and on each occasion the number was unobtainable. Contact was then made using a mobile number provided by the Exercise Director. An urgent action was agreed to confirm the correct emergency contact number with Hev-E-Lift and to ensure that this number was checked as part of the quarterly BCP version control check by the Operations Director.

2 Internal controls

In Session 5 the importance of controls as a form of mitigation was discussed; the activities of an internal control professional takes these concepts and builds on them. Internal controls are a fundamental part of good risk management, so much so that many of the governance codes (discussed in Session 7) require boards to take an active role in reviewing the effectiveness of the internal control environment. To remind you, look at this extract from the 2018 FRC Corporate Governance Code:

> Internal controls are a central component of a good risk management system as Video 3 shows.
>
> The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.
>
> FRC Corporate Governance Code (Clause 29, p. 12, 2018)

Video content is not available in this format.

Video 3 The importance of internal controls

A bow tie is a great way of displaying this risk/control picture graphically, as shown in Session 3 during risk identification. Now watch Video 4 which covers the key elements of a bow tie and the internal controls.

Video content is not available in this format.

Video 4 The key elements of a bow tie

Activity 2 Key elements of a bow tie

Allow approximately 10 minutes

Take a look at the image below and match up the correct answers to the numbered labels.

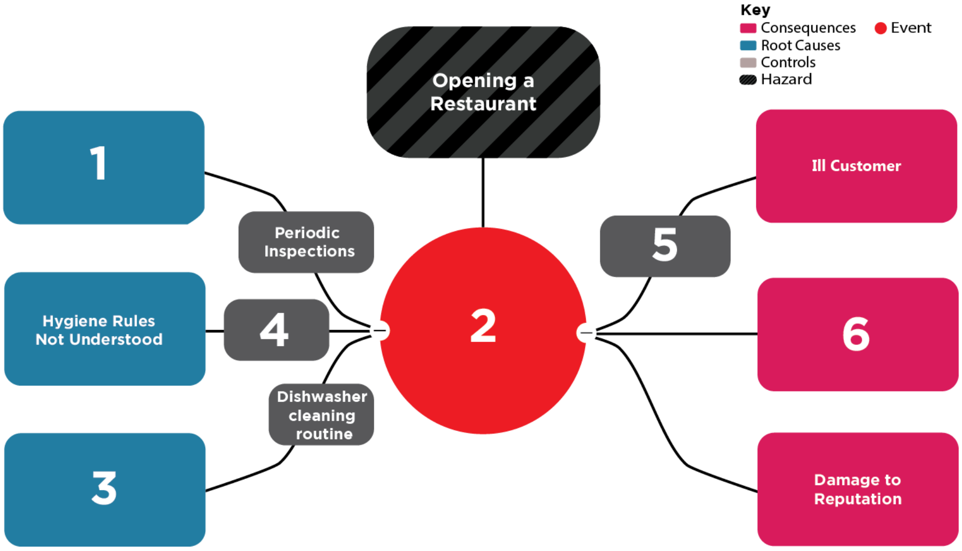


Figure 4 BowTie diagram (without labels)

inadequate hand washing

unsafe food produced

plates not clean

induction training

temperature check of food

loss of trade/legal action

Match each of the items above to an item below.

1

2

3

4

5

6

Answer

Take a look at the image below to see the whole BowTie diagram and how your answers compared.

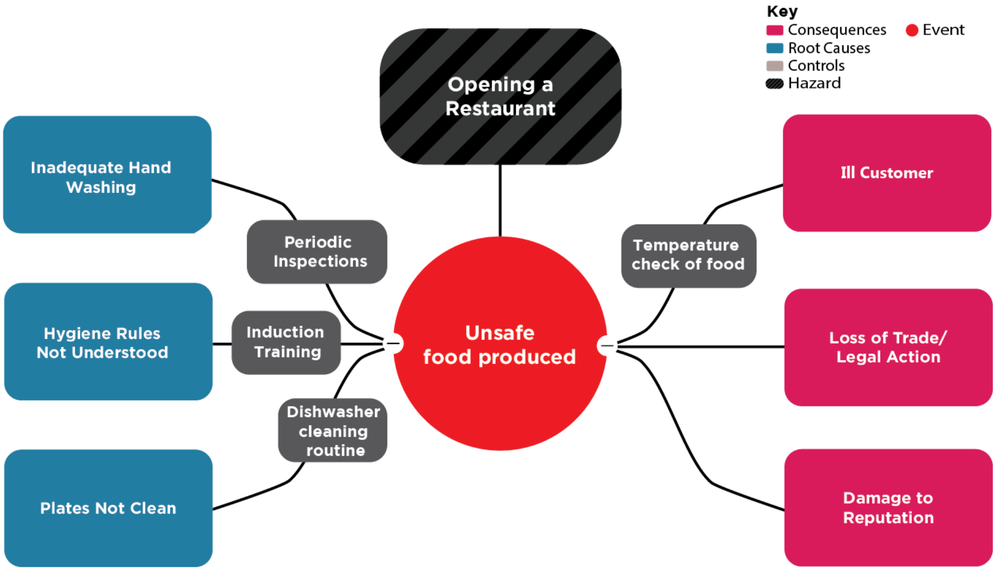


Figure 4 BowTie diagram (with labels)

More advanced risk management may start to apply quantitative assessments to these types of assessments. Techniques such as ‘HAZANs’ (hazard analysis) are commonly applied in high-hazard process industries. This technique builds on the bow tie thinking of identifying root causes and controls. It then asks how likely it is that a certain root cause will occur and how likely it is that a certain control will fail. This can then be brought together to give a mathematical model of how likely a certain risk is, based on the controls in place and their effectiveness. This modelling is often quite complex and is performed by trained engineers.

However, it is worth sharing some of the common observations that flow from this thinking:

- high-hazard systems normally have several controls and care is taken to make sure these controls cannot be circumvented by a ‘common mode of failure’
- controls that rely on people are normally the least effective
- controls that are directive should not be the sole prevention for high-impact risks.

3 Project risk management

Much is made of risk management in projects but in essence good risk management is the same whether performed in projects, operations, compliance or strategy. At its most basic it is all about understanding what risks you face and then doing something about them.

Where projects differ is that projects (and therefore some of their risks) have an end date whereas other business risks do not.

In general there are three types of risk that need to be considered for any project:

- the risks to delivering the project (on time and in full) and the benefits promised
- the risks to the business during the project – particularly pertinent for change and transformation projects, where the transformation may cause uncertainty in the business
- risks that are introduced post project – new systems, products, ways of working and locations can all introduce new risks that were not present at the start of the project.

Video content is not available in this format.

Video 5 Project risk management

There are standard assessment models available for assessing the state of risk management in projects, one such being P3M3, which is recommended by the UK government.

This is a project maturity model that defines 'what good looks like' for various aspects of a project, from financial planning, to estimating through to risk. A maturity model such as P3M3 can be a useful tool for understanding your current level of maturity and providing a road map for improvement.

Activity 3 Short risk exercise

Allow approximately 10 minutes

Consider this project and run a short risk exercise.

Consider the following scenario:

A small family owned manufacturing business has been expanding rapidly, selling to new customers in different countries as well as introducing new products.

But this expansion has not been without growing pains. They have received an increasing number of customer complaints because of late deliveries, some of which have been caused by customs-related delays of shipping products to new countries and poor product quality.

In addition they are seeing high levels of staff turnover. At their exit interviews people leaving the company commonly highlight old IT systems and excessive workload as their reason for leaving. Many of the people who helped to build the original IT systems have now left the company.

The owners have decided to invest in a new IT system to handle order taking and production scheduling. The system is relatively new and no one in the company has any experience of using it. The provider of the IT system has said that it can be installed and up and running in less than six months, providing that all of the necessary information is available and of good quality and that the company's best people are available. They have said that the customs module is not in their current quote. The sales team believe that they will recoup the cost of the IT system if it reduces the late deliveries by 50%.

The company management team have asked you to give them some advice. They would like to know the following:

1. Which of their existing threat risks the project will reduce and which it will not.

Select all of the risks that will be reduced:

- □ Late delivery to customers
- □ Quality problems
- □ Customs-related problems
- □ Business continuity: Lack of support for existing IT tools
- □ Staff turnover

2. What risks you foresee to delivering the project on time (and its benefits).

- □ Availability to release the 'best' people to support the project
- □ Quality of data (and time to clean up)
- □ Capacity at manufacturing plant
- □ Quality problems
- □ The amount of the benefits caused by customs issues

3. What risks to normal operations you think they should be aware of during the project.

- □ Higher levels of staff turnover (due to higher workload)
- □ Higher levels of customer complaints (due to higher workload)
- □ Higher levels of product quality issues

4. The new risks they should consider once the new IT tool is installed.

- □ Opportunity: lower staff turnover
- □ Opportunity: additional benefits from installing customs module
- □ Higher levels of product quality issues
- □ Business continuity for new IT tool

Answer

Good project managers deliver projects on time, to costs and to the customer specification. They do this, in large part, by effectively managing risks.

Good business managers need to understand not only the risks to delivering a project but also the risks to running their business whilst the project is running and the risks that will be created once the project has finished.

4 Emerging risk management and horizon scanning

Risks are continually changing, either due to changes within or outside an organisation. An organisation needs to keep on top of these changes to make sure they don't get caught out. Organisations will try to look into the future to anticipate the potential changes on the horizon and give them as much time as possible to plan and respond to these changes; this is often know as horizon scanning.

To help with their horizon scanning activities some organisations add an additional dimension to their risk assessments, that of risk velocity. They use the term 'velocity' to refer to the speed at which the risk could impact – the quicker the impact the less time the organisation has to react, and the more important business continuity (BC) and crisis management plans become.

Organisations may also attempt to differentiate risks between those which are likely to become longer-term trends, and thus create a material shift in the business or industry, against those which are likely to be a more short-term 'event' that may be temporarily disruptive but could act as a trigger to a new norm.

The timings of either trends or events are extremely difficult to predict with any degree of accuracy so instead risk managers will rely on scenario (what if) analysis, described in Session 3, to bring together multiple visions of different realities that may exist given certain circumstances. Risk managers can then look at what risks might exist in these scenarios and how resilient the business is currently or how it might need to change to respond to these scenarios. The business can take a view of how plausible the scenarios are and consider this in deciding if it needs to respond to a particular scenario.

The plausibility of a particular scenario can be driven by a number of factors, including, but not limited to, industry dynamics, wider political and economic indicators and technological advances. However, an approach often used in scenario development is to consider what key milestones and changes would need to happen before a particular situation could come to pass. The more of those milestones that have happened or seem likely to happen, it follows that the more likely the scenario is to come to pass and thus the more likely that the company will face the risks present. Those milestones can often be categorised to make identification easier using a PESTLE analysis as described in Session 3. Consider a historical example to demonstrate this, the Demise of Ocean Liners.

The benefit of considering emerging risk can be seen in the ocean liners case study. Within 15 years these vast ships that had originally been huge investments for their owners became redundant in providing Atlantic passage and had to find a new market catering for newly wealthy holidaymakers seeking cruises. Looking back to Session 1, Kodak failed to see the significance of digital photography, despite designing it, and Rolls-Royce did not move fast enough to capture the widebody engine market.

Take a look at the following articles, which look at the adoption of electric vehicles and their emerging risks:

- *UK wants fully autonomous cars on road*
- *The five major challenges facing electric vehicles*

Now that you've looked at some emerging risks, consider some emerging risks in your own industry and develop some scenarios using a blank version of the toolkit.

Table 1 gives an example of some factors to consider.

Table 1 Emerging risks for the adoption of electric vehicles

Area	Scenario
Political	• Taxation would have to become less reliant on fossil fuels • Regulators respond to increasing pressure to respond to environmental crisis by ○ increasing the cost to run older technology ○ incentivising electric technology ○ prohibiting use of activity (e.g. cannot drive diesel cars in cities)
Economic	• Access to vehicles would need to be affordable, whether through total ownership or through alternative use methods
Social	• Society would need to accept: ○ the alternative power sources (and changes in use this may require – e.g. overnight charging) ○ autonomous control taking over from humans • There would be a shift in the labour market as 'driving' jobs disappear • Ethical considerations around automation would need to be resolved (e.g. in the event of an accident scenario how should automation respond)
Technological	• Autonomous technology would need to reach a point where it was reliable to the extent where failure would be so remote that society could accept the residual level • Power technology would need to reach a point where it is comparable to 'current' alternatives • Infrastructure to support technology would need to be in place (e.g. power charging points, 'traffic signals' that can communicate with vehicles)
Legal	• Legislation would need to be changed to allow for automation within the driving environment • Industry changes would need to consider how liability is apportioned in the event of a failure • The insurance industry would need to shift to consider automation
Environmental	• Environmental pressure increases to the point where burning fossil fuels is unacceptable

5 Safety risk management

Probably one of the earliest and most familiar forms of risk management is that of safety risk management. You probably have some degree of awareness of the efforts undertaken to improve health and safety in the workplace that, in the UK, has continually evolved since the 1960s. There are many areas and specialisms involved in safety management that allow industry to operate in a manner that minimises harm to employees and the wider public.

Now look at these videos created by Network Rail that provide an example of the importance employers place on putting safety high on their risk management priorities and set the same expectation for all their workforce.

- Lifesaving rules series - safe behaviour
- Lifesaving rules series - working with electricity
- Lifesaving rules series - driving
- Lifesaving rules series - working with moving equipment
- Lifesaving rules series - working at height
- Lifesaving rules series - taking responsibility

Aside from the obvious benefits of safety risk management, which aims to prevent harm to employees and the public, there are also a number of less obvious benefits to managing safety risk, including, but not limited to:

- greater employee satisfaction and recruitment/retention (safe workers are happier workers)
- identification of other risks that need addressing (e.g. spotting a fire risk may identify a single point of failure that needs addressing)
- enhanced reputation, which can help in winning work and improving relationships with stakeholders
- reduced interruptions/delays and managed costs (accidents have a cost and cause delay).

Activity 4 Safety initiatives

Allow approximately 10 minutes

Consider your own work environment. What safety initiatives have been implemented or could be implemented that should have additional benefits?

Below are some examples of safety risk treatments with the additional wider business benefits.

Consider your own work environment and safety initiatives that have or could be implanted and the wider business benefits these can bring.

Table 2 Safety initiatives

Safety initiative	Additional benefit
Life Saving Rules	Encouraging a positive culture towards each other which can improve team work and

	enhance mental health well-being in the workplace
Site Safety Case	Should also identify priorities for maintenance that will reduce down time of equipment/facilities which will improve output
Contractor Induction	Opportunity to improve site security through knowledge of who has access to site and when they are on site
1	*Provide your answer...*
2	*Provide your answer...*
3	*Provide your answer...*
4	*Provide your answer...*
5	*Provide your answer...*

6 This session’s quiz

Now it’s time to complete the Session 8 badged quiz. It is similar to the quiz that you took at the end of Session 4, with 15 questions in total.

Session 8 compulsory badge quiz

Open the quiz in a new tab or window and come back here when you’re finished.

7 Summary of Session 8

The next video covers good practice in risk management.

Video content is not available in this format.

Video 6 Good practice in risk management

Now look at how good risk management can add value.

Video content is not available in this format.

Video 7 How good risk management can add value

The main learning points that have been covered in this session are:

- the variety of risk management specialisms

- appreciating which of these specialisms may be appropriate for you currently or in your future career.

Video content is not available in this format.
Video 8 Risk management inspiration

Well done for completing the course! Now look at what you have learned overall from this badged course on risk management.

Risk management is important. It protects assets and adds value by making sure risk is taken in a conscious, competent way and in places where risk taking is rewarded – in other words it helps people make better decisions.

In procedural terms risk management is simple: we set targets (risk appetite), we identify risks, treat them and then review the outputs – then repeat. But risk is more than a process. We know this because incidents happen frequently at big firms who are excellent at following processes.

So why is this? Firstly it is because risk management is not just a process. Organisations are designed by, run by and governed by people. So for risk management to succeed it needs to involve people and help them to manage the risks they face.

Secondly risk management, even when done well, rarely means that the risk can no longer happen. Instead it means that the risk is less likely to happen or will have a lower impact – it improves the chances of things going right (or reduces the chances of things going wrong) but it rarely removes the risk completely. It is for this reason that managing risk is an ongoing activity, not a one-off event.

Finally risk management is a verb – a doing thing. Risk management delivers no value if no action is taken. These actions may be specific one off activities; they may be ongoing controls to reduce risk (providing they work!); it may be checking actions and controls are effective or using incident information to learn from risks that have happened. In all cases it is about doing something.

Video content is not available in this format.
Video 19 Last words

We hope that you have found this course useful and that it will help you take action to manage risks, to make better decisions and to achieve your objectives.

Where next?

If you've enjoyed this course you can find more free resources on OpenLearn.

New to University study? You may be interested in our access courses or courses related to Business and Management.

Making the decision to study can be a big step and The Open University has over 40 years of experience supporting its students through their chosen learning paths. You can find out more about studying with us by visiting our online prospectus.

Tell us what you think

Now you've come to the end of the course, we would appreciate a few minutes of your time to complete this short end-of-course survey (you may have already completed this survey at the end of Session 4). We'd like to find out a bit about your experience of studying the course and what you plan to do next. We will use this information to provide better online experiences for all our learners and to share our findings with others. Participation will be completely confidential and we will not pass on your details to others.

Glossary

BC

business continuity

COSO

The Committee of Sponsoring Organizations (of the Treadway Commission)

ERP

The acronym for Enterprise Resource Planning

FCA

The UK Financial Conduct Authority (responsible for the regulation of financial firms)

FDA

The US Food and Drug Administration

Five Whys

An interrogative technique where the question 'why?' is repeatedly asked to help identify the root of a problem or an issue

ISO

The International Organization for Standardization

NGO

The acronym for non-governmental organisation

PERT

The acronym for Programme Evaluation and Review Technique

PESTLE

The acronym for a management brainstorming technique (i.e. what are the Political, Economic, Social, Technological, Legal, Environmental matters relating to an organisation?)

RACI

The acronym for Responsible, Accountable, Consulted and Informed communications processes

SRA

The acronym for Strategic Review Analysis

SWOT

The acronym for a management brainstorming technique (i.e. what are the Strengths, Weaknesses, Opportunities, Threats of, or relating to, an organisation?)

Acknowledgements

This course was written by Peter Ralph and Michael Lawrence of Rolls-Royce in collaboration with Martin Upton of the Open University Business School. The course was first published in November 2019.

The Open University would like to thank the Rolls-Royce team for their support in the production of the course.

Grateful acknowledgement goes to Sharpcloud, CGE Risk Management Solutions and AIM Commercial services for their contributions to the course.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this free course:

Course image: Artyom_Anikeev / iStockphoto.com

Session 1

Activity 1: *Skydiving*: Pixabay; Pexels; *Horse riding*: Anna Jokiranta; Pexels; *Reading a book*; Burst; Pexels; *Saving money*: rawpixel.com; Pexels; *Gambling*: Pixabay; Pexels; *Stock trading*: Negative Space; Pexels; *Water skiing*: Pixabay; Pexels; *Donkey ride*: csfotoimages; iStockphoto.com; *Rock climbing*: photo by Jonathan Ouimet on Unsplash

Piper Alpha Timeline: Day of explosion: Trinity Mirror/Mirrorpix/Alamy Stock Photo;

Kodak Timeline: Little Visuals; Pexels

1884: GL Archive; Alamy Stock Photo; 1888: courtesy of George Eastman Museum; Denise Jans on Unsplash; 1891: Robert Cutts; https://creativecommons.org/licenses/by-sa/2.0/**;** 1900: Cquoi; https://creativecommons.org/licenses/by-sa/4.0/deed.en; 1922: Denise Jans on Unsplash; 1925: taken from: https://www.findagrave.com/memorial/38307810/william-g_-stuber; 1969: photographer: Eric Long; (c) Smithsonian Institute; https://airandspace.si.edu; 1975: eileen wang; https://creativecommons.org/licenses/by-nc-sa/2.0/; 1976: Thistle33; https://creativecommons.org/licenses/by-sa/4.0/deed.en; 1984: Math; Pexels; 1994: Jared C. Benedict; https://creativecommons.org/licenses/by-sa/3.0/deed.en; 2004: Jared C. Benedict; https://creativecommons.org/licenses/by-sa/3.0/deed.ent; 2005: Metoc; https://creativecommons.org/licenses/by-sa/2.5/deed.en; 2012: Guy Solimano / Stringer

Video 3 / Rolls Royce Timeline: Music: Philip Guyler; Audio Network

1960: Douglas McFadd/Stringer; courtesy of The Boeing Company; Valeriy A. Vladimirov; 1965: courtesy of The Boeing Company; 1966: Pratt & Whitney; Jelson25; courtesy of The Boeing Company; Dirk Grothe; AirTeamImages Limited; 1967: Arnold Newman, White House Press Office (WHPO); taken from: https://commons.wikimedia.org/wiki/File:37_Lyndon_Johnson_3x4.jpg; taken from: https://commons.wikimedia.org/wiki/File:Rolls_Royce_RB.211_vl.jpg; 1971: Copyright ©

2008, EBSCO; 1974: taken from: https://edition.cnn.com/travel/article/airbus-a300-history/index.html

Session 3

Figure 2: William Ely Hill

Session 7

Risk Committee Terms of Reference and Reporting Toolkit; courtesy of Rolls Royce

Session 8

Figure 1: Sammie Vasquez on Unsplash

Figure 2: Startup Stock Photos; Pexels

Figure 3: Helloquence on Unsplash

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.