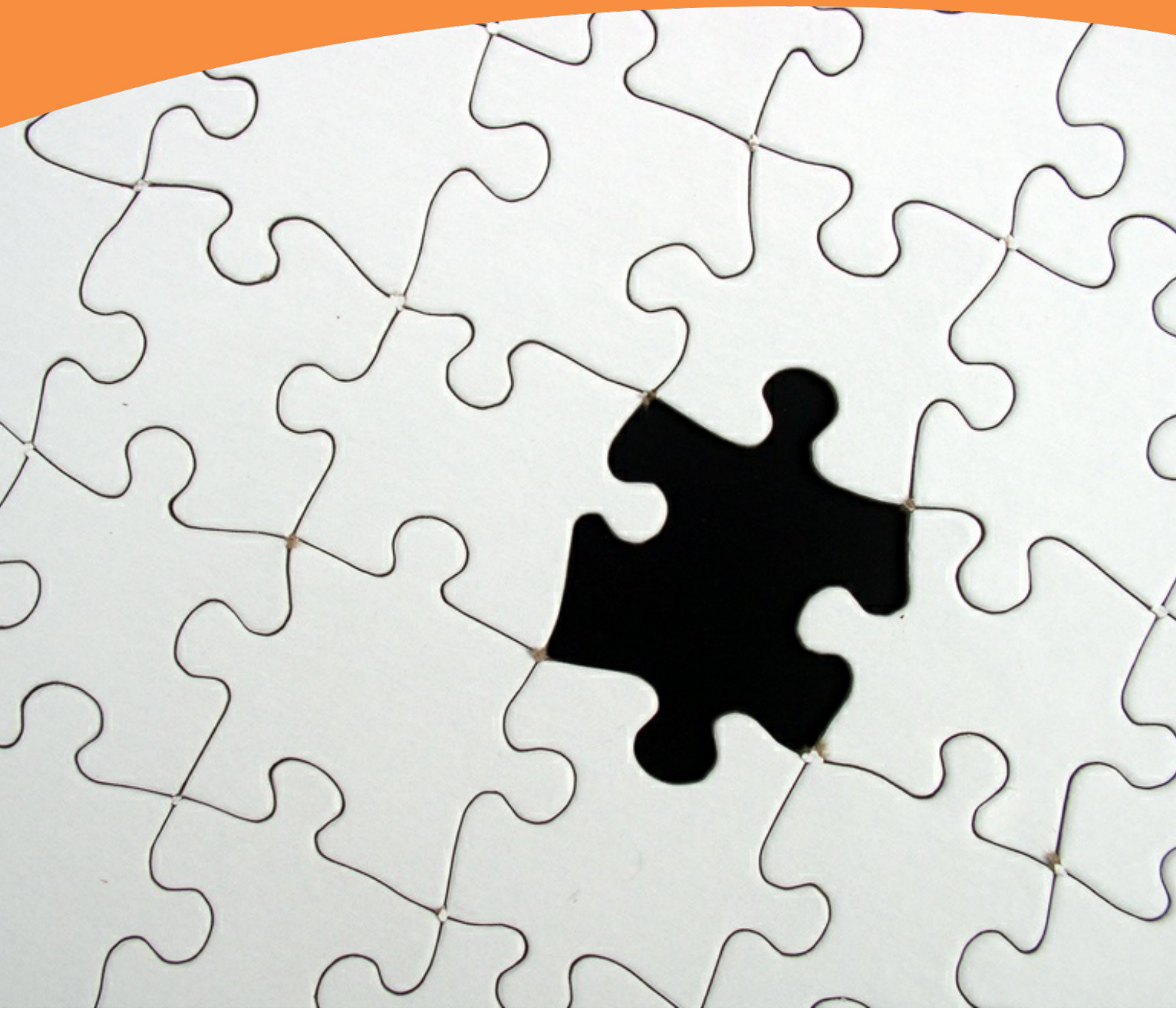
Risk Management Made Easy

Andy Osborne



bookboon
The eBook company

Andy Osborne

Risk Management Made Easy

Risk Management Made Easy

ISBN 978-87-7681-984-2

Contents

About the author

An acknowledged expert in the field of risk management and contingency planning, Andy Osborne has spent over twenty years helping businesses of all sizes, across a broad range of industry sectors, to understand and manage their risks effectively. He is a firm believer that the role of a consultant or adviser is to simplify apparently complex processes and present them in a way that is easy to understand, not the other way around.

Andy provides the following risk management consultancy services to clients, through his company, Acumen :

- Business risk assessment
- IT risk assessment
- Fire risk assessment, audit and evacuation planning
- Health and safety risk assessment and audit
- Training courses (including an introduction to risk management)
- Emergency planning
- Business continuity management

To contact Andy, call 01386 834455 or e-mail him at aosborne@acumen-bcp.co.uk

You can also follow him on Twitter (@AndyatAcumen) or link to him on LinkedIn (http://uk.linkedin.com/in/andyosborneatacumen)

Andy's first book 'Practical Business Continuity Management' (ISBN 978-1-906316-01-3, www.practicalbcm.co.uk), is a collection of hints, tips and good ideas for getting the best out of your business continuity management programme.

His second book 'Risk Management Simplified' (ISBN 978-1-906316-48-8, www.rmsimplified.co.uk) is a more comprehensive version of this e-book.

Andy's entertaining and amusing blogs, which link his day-to-day business and personal life experiences to risk and business continuity management themes can be read at www.acumen-bcp.co.uk/blog

Chapter 1

In this chapter we consider :

- *Why we should bother thinking about risks to our business*
- *The benefits of effective business risk management*
- *What we mean by risk*
- *Some of the risks that our business might face*
- *Balancing opportunities and threats*
- *Some of the possible uses for risk management*
- *A simple but effective risk management process*

1.1 Introduction

> *"To be alive at all involves some risk."*
> Harold Macmillan

Risk is unavoidable. Like the proverbial death and taxes, it's one of the few things in life that's inevitable. All businesses, whatever their size and shape, whatever markets they operate in and whatever products or services they provide, are constantly faced with a multitude of risks, large and small. Indeed, businesses can only prosper by successful risk taking.

In our own businesses we need to strike the correct balance between risk and potential reward; to maximise our upside risk and minimise our downside risk. To succeed we need to manage risk appropriately, not to try to eliminate or avoid it, as, in any case, that simply isn't possible. It's therefore essential that we understand the major risks to our business operations to enable us to manage them to our advantage.

Some risks are so minor as to be insignificant, whereas others have the potential to seriously affect our business's continued well-being. So it's important to understand the likelihood and the potential consequences of our own particular risks, and to take sensible, cost-effective mitigation measures for the more significant ones.

This book will help you to do just that; leading you through the process in a straightforward, no-nonsense way.

It will help you to identify and manage your risks in a number of areas, such as strategy, day-to-day business operations, financial control, capitalising on potential business opportunities, launching new products or services, expanding or changing the shape of your business and managing projects, to name just a few.

It will guide you through the various stages of assessing and mitigating your risks without blinding you with pseudo-science, techno-speak or jargon.

It will provide you - the business owner, director, departmental manager or project manager, who presumably doesn't have the time or inclination to be a full-time risk manager - with a simple, straightforward and effective risk management system. One that deals with the basics and avoids some of the complexity and non-essential 'padding' that comes with many risk management systems.

The end result is a very simple, but above all usable, process that can be applied to the real world that the vast majority of business managers inhabit.

> This book will help you to identify and manage the risks to your business by providing you with a simple, straightforward and effective risk management system.

1.2 The benefits of effective risk management

> *"While 'risk' is commonly regarded as negative, risk management is as much about exploiting potential opportunities as preventing potential problems."*
>
> BS31100:2008 Risk Management Code of Practice, British Standards Institution

There are many benefits to managing our risks effectively, including :

- Informed decision making
- A more resilient business
- Increased likelihood of successful risk taking (capitalising on opportunities)
- Protection of revenue, profits or market share
- Protection of reputation/goodwill
- Improved product or service quality and reliability
- Protection of valuable assets
- Increased likelihood of achieving strategic goals or objectives
- Reduced costs and/or increased profits
- Less failures and downtime
- Competitive advantage
- Fewer nasty surprises

Many risks are seen as having purely negative consequences and for this reason it's not uncommon for those involved in risk management to take a pessimistic view of risk. But we shouldn't forget that many risks also have positive consequences. Effective risk management can help us to reduce the negative and increase the positive consequences of risk, thus helping our business to grow and flourish.

Risk management has a part to play in your decision making, whether it's with regard to business start-up, strategy, exploiting opportunities, managing your various projects or in your day to day business operations.

Risk management can help you to justify your decisions - to your management team, your employees, your business partners, investors, creditors or customers. And it should mean that you go into things with your eyes open; that you make informed decisions rather than just acting on gut feel or on a hunch.

There are many benefits to managing our risks effectively. Effective risk management can help us to reduce the negative and increase the positive consequences of risk and to make informed decisions.

1.3 What is a risk?

"Whatever can go wrong will go wrong."
Murphy's Law

Look in any dictionary and you'll find a definition of risk. Here's one :

risk *n* the possibility of incurring misfortune or loss; hazard **at risk** vulnerable

What we're really talking about is a potential future problem - or, indeed, opportunity - or the potential future effect of a decision or an action that we take now. And every decision we make or action we take contains some element of risk.

A risk is essentially a potential future problem (or opportunity). Every decision we make or action we take contains some element of risk.

Risks come about when the vulnerabilities in our systems, processes, facilities or resources are exploited by threats. Examples might include the burglar or hacker who exploits the vulnerabilities in our physical or IT security system, or a fire that starts due to an electrical fault and spreads because of weaknesses in our fire detection and suppression systems, errors made by inexperienced or insufficiently trained staff, or a whole host of other things.

The following are examples, in no particular order, of some of the possible risks to businesses. It's by no means a definitive or exhaustive list - rather it's intended to give a flavour of the types of risks that businesses may face. We only have to read or watch the news or think of our own experiences to realise that, unfortunately, these events do happen - in some cases all too frequently.

- Fire
- Flood
- Computer failure/data loss
- Failure to exploit opportunities
- Theft
- Poor sales
- Late payment/bad debts
- Supply chain failure
- Over-commitment
- Workplace accidents
- Equipment disruption/failure
- Loss/unavailability of key personnel
- Power failure
- Fraud
- Interest/exchange rate fluctuations
- Human error
- Breach of contract/contract disputes
- Increased costs
- Loss of a major customer
- Negative cash flow
- Industrial action/disputes
- Insufficient profits
- Pollution/environmental contamination
- Faulty products
- Lack of working capital
- Breach of regulation/legislation
- Litigation
- Vandalism
- Business lost to competition
- Product contamination/tampering
- Negative publicity
- Workplace violence
- Insolvency
- Hostile takeover

Risks can arise as a result of our own business's activities or as a result of external factors such as legislation, market forces, interest or exchange rate fluctuations, the activities of others or even the weather. They can be a product of the business environment, the natural environment, the political or economic climate or of human inadequacies, failings or errors.

The bottom line is that risk may impact on our ability to meet our business objectives or even threaten the business itself.

> Risks can arise as a result of our own business's activities or as a result of external factors.

1.4 It's never happened/will never happen to us

> *"It's likely that something unlikely will happen."*
> Aristotle

We might be tempted to think that risks like those listed on the previous page will never happen to us, particularly if we're one of the fortunate few who has never experienced anything particularly bad or disruptive in our business. We may feel that the likelihood of us suffering from events like these is just too low to worry about; that the odds are stacked in our favour.

It's an interesting thought, though, that many of us who take the 'it'll never happen to us' approach to risk in this context, where the odds might be hundreds or thousands to one, will nevertheless gamble on the national lottery, where, despite the fact that the odds of winning, at many millions to one, are stacked massively against us, we consider it a gamble worth taking.

Unfortunately, the past isn't necessarily that useful or reliable in helping us to predict the future. Just because a particular risk hasn't yet come to fruition doesn't necessarily mean that the risk isn't there. And on the other hand it doesn't mean that it's imminent (section 3.2 'Assessing and rating our risks' discusses likelihood and the benefits, or otherwise of relying on statistical 'evidence').

The thing about unexpected events is that, by definition, they're unexpected. The reality is that only we, as business managers, can decide whether a particular risk is acceptable to our business.

Sadly, things do go horribly wrong from time to time. And the reality is that bad things don't just happen to other people. History is littered with the casualties (large and small businesses alike) of events that they thought couldn't possibly happen to them.

In reality, almost every business is likely to suffer some sort of disruptive or damaging event or situation during its lifetime. And whilst the consequences of many of these events will, though painful, be manageable or at least survivable, for the unlucky or unprepared some of them will have the potential to seriously damage the business. These more serious events will range from the headline grabbing fires, floods and explosions, through product and environmental contamination, fraud and theft, to the less news-worthy but equally debilitating power or technology failures and supply chain or cash flow problems.

Almost every business is likely to suffer some sort of disruptive or damaging event or situation during its lifetime.

Some of the risks in the list in paragraph 1.3 are largely beyond our control, because they are due to external forces, such as nature or changes to the political or economic environment. Whilst that may be true, it's interesting to note that many of the risks listed are down to the actions of people, with very few 'natural' events and relatively few external influences over which we have absolutely no control. It's a sad fact that when we introduce people into the equation things often go wrong. Because, people being people, they sometimes do unexpected, dangerous or even stupid things; they don't follow processes; they cut corners; they make mistakes.

However, in many ways this is good news. Clearly we normally have little or no influence over natural events, the political or economic climate or the legal or regulatory environment and can only really take steps to mitigate their effects (for instance we can't prevent severe weather from happening, although we can choose not to locate our business premises in a flood plain). However, in many cases, it is possible to do something to prevent or reduce the likelihood of the man-made risks occurring in the first place.

Investing some time and effort in managing our risks is a worthwhile investment and makes good business sense. Ultimately, effective risk management could be the difference between the survival and failure of the business.

Many of the risks we face are due to the actions of people. It is often possible to prevent or reduce the likelihood of theses 'man-made' risks occurring.

1.5 Me, a risk manager?

"There is a new appreciation of the wider scope of risks facing businesses requiring them to look at risk in a more structured way...A good risk management process is an essential part of being in business."

Institute of Chartered Accountants in England and Wales

The good news is that every one of us is an intuitive risk manager!

Being in business may be risky, but life is a risky business and we're constantly faced with countless risks that we have to assess and make decisions about. Most of the time we don't even realise we're doing it - we just do it naturally. Which is just as well really, as if we had to stop and think about it we'd spend all of our time assessing risks and never actually get anything done.

For instance, every time we cross the road or drive our cars or play sport, or carry out many other day-to-day activities, we have to assess and manage risks, identifying and assessing the threats that we face and working out appropriate mitigation measures. But we do this almost subconsciously.

So, if we're all risk managers already, what's the point of this book? Well, the difference is that here we're more concerned with assessing and mitigating *business* risks. The process is pretty much the same as for our intuitive method, it's just that we probably have a bit more time to think about things. And in business we really need a slightly more structured system than the instinctive approach, to enable us to identify and quantify our risks a bit better before we make our decisions.

When we evaluate risks to our business we need to have a clear and reasoned method of doing so. We may have to justify our thinking to others. We may need to persuade others to do something as a result. Perhaps more importantly, the potential downside if we get it wrong may be extremely serious - for ourselves, for our employees, for our customers, or for our business as a whole.

When we evaluate business risks we need to have a clear and reasoned method, rather than employing a 'gut feel' approach.

1.6 The balanced view

"Who bravely dares must sometimes risk a fall."
Tom Bradley

Almost every business opportunity has a potential downside. But some of the risks that we take also have a potential upside – that's why we take them. Indeed, a business may consciously decide, as part of its strategy, to take a high level of risk because of the potential rewards.

We need to balance the opportunities (to make a profit, grow the business, move into new markets, launch new products and services, etc) against the potential downside (such as over commitment, the impact of interest or exchange rate fluctuations, inability to sell our wonderful product or service, inability to pay our staff, and so on).

It's not possible to create a completely risk-free environment. But what we can do is manage risk more effectively. We can identify risks, quantify them, and once we understand what we're up against we can make informed, considered decisions regarding what (if anything) to do about them.

In business we need to balance opportunities against the potential downside.

1.7 Risk management has its uses

"Recent research indicates over 70% of programmes are late, over budget or ineffective. Organisations employing effective risk management have reduced this failure rate significantly and gained a significant competitive advantage."

Colin Wheeler, Technical Director, Istria

Risk management has many uses. It can be used to :

- Ensure the safety and well-being of employees, visitors, customers, etc
- Make your business more resilient
- Support your decision making process
- Increase the likelihood of successfully exploiting opportunities
- Perform 'what if' assessments
- Ensure legal or regulatory compliance
- Protect your cash flow
- Increase the likelihood of success in your projects
- Support requests for action or expenditure
- Improve the strategic and day-to-day management of your business
- Improve operational processes and reduce failures and problems

Risk management has many uses.

1.8 The risk management process

> *"Only a person who risks is free. The pessimist complains about the wind; the optimist expects it to change and the realist adjusts the sails."*
>
> William Arthur Ward

The risk management process described in this section is simple but effective. More to the point, it has been proven to work in businesses of all types and sizes. There are five very straightforward stages to the suggested process, which are shown in the following diagram, outlined below, and described in more detail in subsequent chapters :

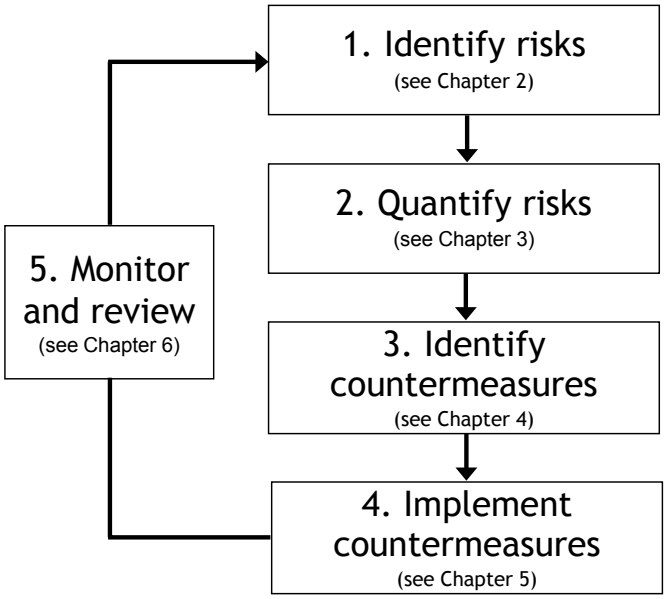


Figure 1 : The risk management process

Stage 1 :

Before we can take any meaningful action to address our risks we need to know what we're up against. So we need to identify the risks that we face (more information on risk identification can be found in Chapter 2).

Stage 2 :

Once we've identified our risks we need to quantify them. Because the risks that we're really interested in are those we consider to be significant enough to do something about. So we need a way to sort the wheat from the chaff. We do this by assessing the likelihood of the risk occurring and the impact if it does. (Chapter 3 discusses likelihood and impact in more detail).

Stage 3 :
Once we know which risks are the most serious we can start to deal with them, by identifying and implementing possible countermeasures or mitigation measures - methods of removing, reducing, controlling or recovering from adverse events (Chapter 4 contains information relating to various risk response options).

Stage 4 :
Having determined which countermeasures we feel are sensible and cost effective and decided which ones we want to invest in, we can go ahead and implement them (see Chapter 5).

Stage 5 :
To complete the process we must monitor the effectiveness, or otherwise, of the controls we put in place. (Chapter 6 suggests some considerations for this important, but often overlooked stage).

The following five chapters explore each of the above elements in turn and provide useful information to help put them into practice.

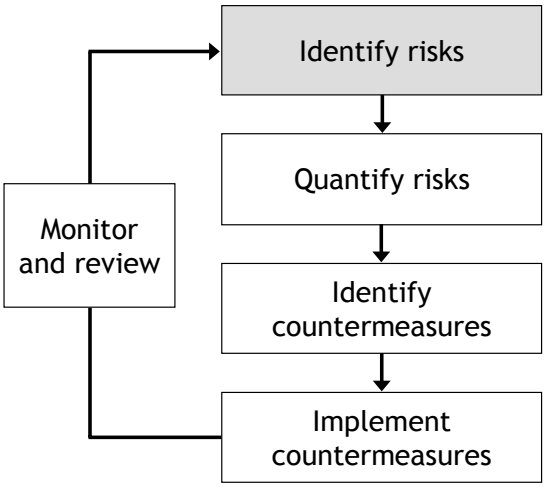
The five-stage risk management process described above is simple but effective and has been proven to work in businesses of all types and sizes.

Chapter 2 looks at the first stage in the risk management process – identifying risks...

Chapter 2

In this chapter we consider :

- *The types of risks that might apply to our business*
- *Stage 1 of the risk management process – identifying risks*
- *How to go about identifying specific risks to our business*



2.1 Identifying the risks – where do I start?

> *"We can't get much better at predicting. But we can get better at realising how bad we are at predicting."*
>
> Nassim Taleb

With all those possible risks out there, where on earth do we start? If we tried to identify every potential risk to our business we could make it a full time job. And for most of us this simply isn't an option. Therefore, we need to focus our efforts.

We need to concentrate on the risks to the most important parts of our business. These are likely to vary from business to business, but for many they might well include some of the following :

- Strategic risks, such as those associated with :
  - Business planning and future direction
  - Achievement of strategic objectives
  - Business growth
  - New markets/products/services
  - Mergers, takeovers and alliances

- Operational risks, in areas such as :
  - Supply of components or raw materials
  - Production
  - Distribution
  - Service delivery
  - Operator errors
  - Pollution/contamination/environmental damage

- Financial/commercial risks, for example to :
  - Cash flow
  - Sales
  - Customer retention
  - Contracts

- Regulatory/compliance risks, such as :
  - Breach of regulation
  - Failure to meet legal/contractual requirements
  - Loss of operating licence
  - Legal action

- Health & Safety risks, including :
  - Workplace accidents
  - Serious injury or death
  - Litigation

- Personnel risks, for example :
  - Loss or unavailability of key staff
  - Inadequate skills/skills shortage
  - Recruitment and employment
  - Workplace violence

- Technology risks, including :
  - IT failure
  - Viruses, denial of service attacks, phishing, etc
  - Plant/equipment failure
  - Data loss

- Project risks, such as :
  - Failure to meet timescales
  - Increased cost/resource requirements
  - Failure to meet business requirements
  - Project failure

The risks in the above list are shown in the various categories (strategic, operational, financial, etc) purely for illustrative purposes and you may wish to categorise your own risks differently. For example, skills shortage, shown here under 'Personnel risks' may also be categorised as an operational or project risk.

An alternative way of looking at things is to think of the business's assets. These might include :-

- Physical assets (premises, equipment, plant, tools, etc)
- Monetary assets (cash in the bank or projected income)
- People (knowledge, skills and experience)
- Intellectual property (e.g. computer programs, designs, patents, copyrighted materials, etc)
- Reputation and goodwill

Once we've listed the assets, we can determine which are the most critical. We can do this by assessing the impact to the business of the loss of any of our assets, or our inability to perform a particular function. In this way we can focus on the risks to the most critical areas of our business.

It may also be helpful to group the assets (e.g. by location or function or product/service), so we can assess the threats to each group of assets as well as individually.

In order to focus our risk management efforts we should concentrate on the risks to the most important parts of our business or to its critical assets.

2.2 Identifying the risks – how do I go about it?

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."

Charles Tremper

Having identified the most critical elements of our business, we can set about assessing the risks to them.

Whilst it's possible to do this on your own, it's generally far more effective if several people are involved. Involving others gives a more objective view and helps to avoid the 'wood for the trees' syndrome, where risks that are obvious to some people are either not noticed, or worse still, ignored by those closest to them.

Once the team has been established, all that's needed is a couple of hours without interruptions and a flipchart or other means of recording the identified risks.

During this session, it's important to focus on identifying risks. That might sound obvious - this is a risk assessment after all! However, it's easy to get sidetracked into thinking about issues rather than risks. There's a subtle but important distinction here. An issue is something that exists already, perhaps a prevailing situation that gives rise to specific risks. For instance, low morale in itself isn't a risk, but it might give rise to the risk of key staff leaving or poor quality work. To ensure we stay focussed on identifying risks, it can be useful to complete the sentence "*there is a risk that……..*" or "*there is a risk of…….*" for each of the risks put forward.

It's also important to stress that we're not looking for solutions at this stage, just the possible risks. And we don't want to get bogged down in assessing likelihood and impacts or the relative importance of each at this stage – more on that later. When everyone is 'brainstormed out' and has nothing more to add, that's the end of the first part of the process.

You should now have a list of risks that might look something like this :

#	Risk
Commercial :	
1	Risk 1
2	Risk 2
3	Risk 3
Operational :	
4	Risk 4
5	Risk 5
6	Risk 6
Financial :	
7	Risk 7
8	Risk 8
	Etc

Figure 2 : List of identified risks

When identifying risks, it can be helpful to complete the sentence *"there is a risk that……..."* .

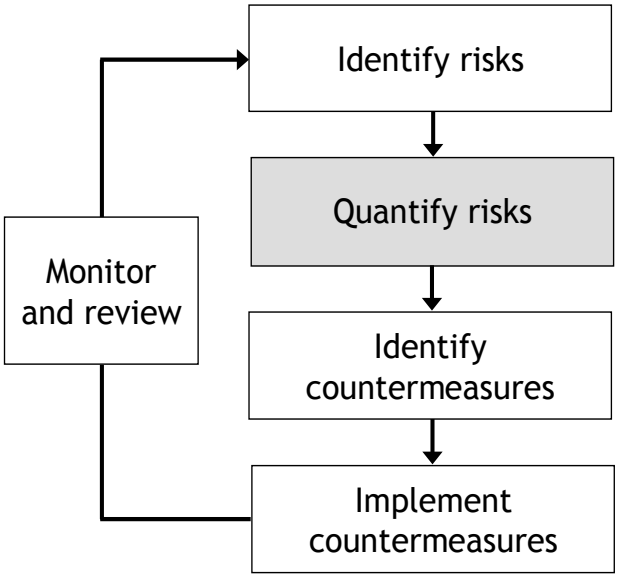
In the next chapter we'll look at quantifying the risks by thinking about *likelihood* and *impact*.

Chapter 3 looks at the second stage in the risk management process – quantifying risks...

Chapter 3

In this chapter we consider :

- *Stage 2 of the risk management process – quantifying risks*
- *Quantifying our previously identified risks by assessing likelihood and impact*
- *Possible impact types and definitions*
- *Rating our risks using a simple risk matrix*
- *Prioritising by identifying significant risks*



3.1 Quantifying our risks - likelihood and impact

> *"If there's a 50% chance of something going wrong, then 9 times out of 10 it will."*
>
> Anon

If you've completed the risk identification session outlined in the previous chapter the chances are you now have quite a long list of risks. Some of them may well be trivial, but some of them will be significant enough for you to want to do something about them. And it's those significant risks that we're most interested in. So we need to be able to quantify our risks in some way, so as to identify the significant ones. So how do we do this?

Our vulnerability to any particular risk is a combination of the ***likelihood*** of the risk materialising and the ***impact*** if it does. In other words, when assessing risks, we need to answer two simple questions :

1. How likely is it to happen?; and
2. If it does happen, how much will it hurt?

When determining likelihood, we could take a scientific or analytical approach and seek out statistics from the emergency services, the environment agency, insurance companies, salvage companies or the multitude of other sources on the internet. Indeed, your average full-time risk manager in a large organisation will often use a lot of statistical analysis and historical information in determining the likelihood of particular risks occurring. This is all very well if you have the time (and the inclination) to go to these lengths. However, there's a very real risk of over-complication and, more to the point, of spending an inordinate amount of time on it. In the vast majority of cases it's sufficient to determine whether the likelihood is high, medium or low. Alternatively we might use terms like 'unlikely', 'possible', 'probable' and 'inevitable' or a simple numerical scale, such as 1 to 3 or 1 to 4. For the purposes of outlining the process, in this book we'll use a 1 to 4 scale (see section 3.3 'The risk matrix').

When determining impact, we should bear in mind that impacts can be both financial and non-financial (although many of the non-financial impacts will ultimately result in some form of financial impact too), and may include :

Financial impacts :

- Loss of revenue
- Lost interest
- Cash flow problems
- Higher bank charges
- Repair/replacement costs
- Increased cost of working (overtime, additional staff, equipment, etc)
- Consequential losses
- Reduced credit rating
- Fines or compensation payments
- Regulatory penalties/fines
- Impact on share price/reduced dividends

Non-financial impacts :

- Death or serious injury
- Loss of credibility/goodwill
- Negative publicity
- Damage to reputation
- Degradation of service to customers
- Loss of production
- Backlog of work
- Pollution/contamination/environmental damage
- Legal action
- Withdrawal of operating licence
- Low morale

Whilst we need to consider which of the above types of impacts might be felt, for the purposes of the risk assessment it's probably sufficient to use a high, medium, low approach or a 1 to 3 or 1 to 4 scale, as we did with the likelihood rating. We'll use a 1 to 4 scale in this book (see section 3.3 'The risk matrix').

Our vulnerability to any particular risk is a combination of the ***likelihood*** of the risk materialising and the ***impact*** if it does.

3.2 Assessing and rating our risks

"You can measure opportunity with the same yardstick that measures the risk involved. They go together."

Earl Nightingale

For each of the risks identified earlier, we now need to assign likelihood and impact ratings. Before we can do this though, we need to decide on the scale that we're going to use to rate our risks. As discussed previously, the two most popular approaches are to use words like 'high', 'medium' and 'low' or a simple numbering system such as 1 to 3 or 1 to 4. This book uses a 1 to 4 scale (where 1 is the lowest and 4 the highest).

Whichever scale we use, and whether we prefer words or numbers, it can help us to focus our minds and be a bit more objective if we think about what we mean by the lows, mediums and highs or the 1s, 2s, 3s and 4s.

The following table gives some possible ways to quantify the various levels of impact (please note that this is only an example as ratings and definitions will differ from business to business) :

Impact ratings	Possible impact definitions	Impact examples
1 Low Insignificant Minimal	Inconvenience but no significant business impact.	Minor, short-term staff disruption; minor customer dissatisfaction; negligible financial impact.
2 Medium Moderate Unsustainable	Operational difficulty requiring significant time and/or resource to manage.	Minor injury; several customer complaints; significant staff disruption; non-trivial financial impact.
3 Significant High Major	High visibility, significant and/or sustained business issues.	Serious injury; significant customer dissatisfaction; damage to reputation; regulatory issues; serious staff disruption (e.g. effective operation of dept/project compromised); significant financial impact.
4 Severe Catastrophic	Threat to viability or survival of the business unit or the business.	Death; unacceptable customer impacts; serious damage to reputation; brand affected; operating licence revoked; high financial impact.

Table 1 : Examples of impact ratings and definitions

When thinking about likelihood, again we can use 'low', 'medium" and 'high' or, if we prefer, numbers or even terms like 'unlikely, 'possible', 'probable' or 'inevitable'. As with the impact ratings, in this example we'll use a 1 to 4 scale. The following table gives some possible ways to quantify the various levels of likelihood :

Likelihood ratings	Possible likelihood definitions
1 Low Unlikely	Not expected to occur within or has not occurred in the past 20 years. Almost inconceivable, but cannot be ruled out entirely. Single figure percentage probability.
2 Medium Moderate Possible	Expected to occur within or has occurred once in the past 10 years. Conceivable, but more likely not to happen than to happen. Less than 50:50 chance of occurring.
3 High Likely Probable	Expected to occur or has occurred several times in the past 10 years. More likely to happen than not to happen. Greater than 50:50 chance of occurring.
4 Almost certain Inevitable	Expected to occur or has occurred at least once a year. Difficult to conceive of it not happening. High (80+) percentage probability.

Table 2 : Examples of likelihood ratings and definitions

Quantifying our likelihood and impact ratings can help provide focus for those involved in risk assessment.

When considering likelihood, we might do some statistical analysis or even think in terms of percentages. A word of caution here though – statistically, a risk that occurs once or twice a year every year without fail can be shown to have an extremely low percentage probability, even though there's a cast iron certainty that it's going to happen again if we don't do something about it. So it's not always helpful to try to be too logical or pseudo-scientific about assessing risk - common sense has an important role to play too.

Moreover, taking at face value statistical 'evidence' that a particular risk is a 20, 50 or 100 year event (as seen in some insurance-related statistics) can be somewhat misleading. Just because a '20-year' event (such as a fire) hasn't happened for 19 years, it doesn't mean that one's imminent. And just because we experienced a '100-year' event (such as a major flood) last year, it doesn't mean that we're safe for another 99 years.

Whilst statistics can sometimes be helpful, they can also be misleading – common sense has an important role to play too.

So whilst it's important to think about likelihood when assessing our risks, and whether we do so with or without the 'benefit' of huge amounts of statistical or historical information, it's really just a guess, albeit an educated one. Indeed, for certain types of risk - in particular the low likelihood, high impact risks - a sensible approach may be to focus more on the impact than the likelihood (see also 'Contingency planning' in section 4.2 'Risk response options'). This approach is borne out by the fact that many of the high profile, disastrous events of recent times had never happened before and were therefore inconceivable to many before the event - but it didn't stop them happening.

Using whatever scale we've decided to use – in this case 1 to 4 - we can now start to rate our risks. This is simply a matter of revisiting each identified risk and making a judgement as to the likelihood and impact ratings for each.

Once this has been completed we can use the risk matrix (see next section) to assign a risk rating for each risk, based on the combination of the likelihood and impact. When using a numbering system such as we are here, a common approach, as you will see from the risk matrix, is to simply multiply the two together (e.g. a risk with a likelihood of 3 and an impact of 2 results in a risk rating of 6).

However, this approach comes with a health warning - it's important to realise that the numbers are really only there for convenience, and a level 4 likelihood isn't necessarily (in fact it almost certainly isn't) four times as likely as a level 1 or twice as likely as a level 2. Similarly, a level 4 impact isn't four times as bad as a level 1 or twice as bad as a level 2. Indeed, the increase in likelihood or impact between level 1 and level 4 could well be 20 or 50 or 100-fold or more (exponential).

The important thing here is where the risk falls on the risk matrix (see next section), as this will help us to consider which risks are significant enough to do something about and what we ought to do about them.

> The risk rating gives an indication of the significance of a particular risk.
>
> The numbers aren't as important as where the risk falls on the risk matrix.

3.3 The risk matrix

> *"Always look for the calculations that go with the calculated risks."*
>
> Unknown (maxim for politicians from the US Congressional Record)

The risk matrix helps us to rate the significance of our identified risks based on the likelihood of the risk materialising and the impact if it does.

There are various sizes and types of risk matrix, depending on the rating scale chosen. The simplest form uses a 3 x 3 grid, but you could use a 4 x 4, a 5 x 5 or a 6 x 6 grid, depending on how complicated or simple you want to make things. As described in the previous section, you can use a low, medium, high or a simple numbered scale, whichever you feel most comfortable with.

In reality, it doesn't really matter. Because when we look at likelihood and impact, we're really trying to determine the *most significant* risks. In other words, the ones that are most likely to happen and the ones with the most serious consequences. The important thing here is that the risks we're most interested in, and that we really ought to do something about, are those that fall in the top right-hand corner and the ones that we're least bothered about fall in the bottom left.

For the purposes of the risk assessment in this book, we're using the 4 x 4 matrix shown below, with a simple numbering system of 1 to 4 for the likelihood and impact axes.

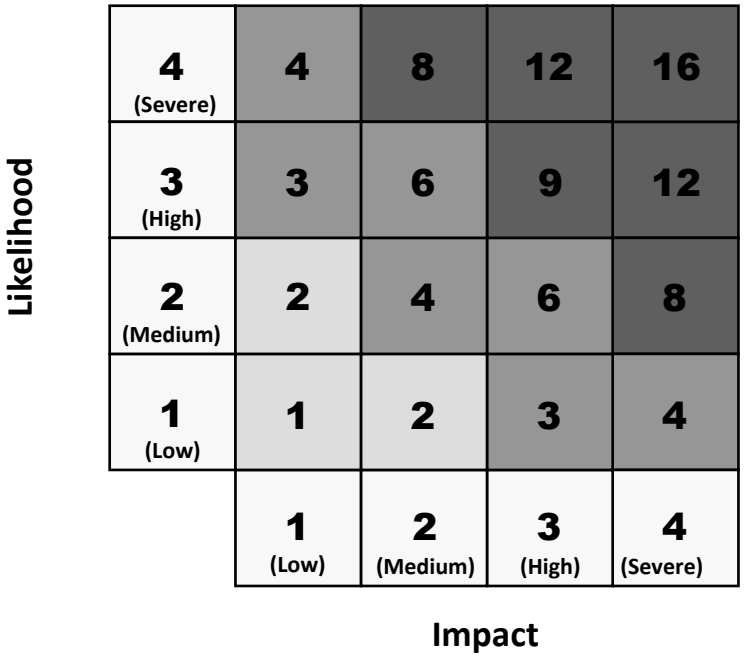


Figure 3 : Example risk matrix

It can be helpful to colour code the squares in the matrix green, amber and red, to indicate the seriousness and priority for action for any given risk, and to carry this colour coding through to our risk register (see section 5.3).

Using the risk matrix (or, in this case, by simply multiplying the likelihood and impact values), we can now assign a risk rating for each of our identified risks. Our risk assessment summary might now look something like this :

#	Risk	Likelihood	Impact	Rating
Commercial :				
1	Risk 1	1	2	2
2	Risk 2	3	3	9
3	Risk 3	4	1	4
Operational :				
4	Risk 4	3	4	12
5	Risk 5	3	1	3
6	Risk 6	4	2	8
Financial :				
7	Risk 7	1	1	1
8	Risk 8	2	3	6
	Etc			

Figure 4 : List of identified risks with assessed likelihood, impact and risk ratings

It's common practice – in fact it's common sense – that a 'rule' is implemented whereby any risk over a certain rating (in this case we'll say 8 or more), or falling in a red square if we've colour coded them, cannot be ignored and *must* be dealt with in some way.

In chapters 4 and 5 we'll look in more detail at some of the countermeasures that we might consider implementing to mitigate the risks that we consider to be significant.

Colour coding (red, amber, green) can be helpful in highlighting seriousness and priorities for action.

3.4 Significant risks

> *"Where there is much to risk, there is much to consider."*
>
> Platen

The risk rating (a combination of the likelihood and impact) is effectively a rating of the significance of each identified risk. And, as discussed previously, it's the most significant risks – those towards the top right-hand corner of our risk matrix (see section 3.3) - that we should be most interested in and that we now need to focus our attention on mitigating.

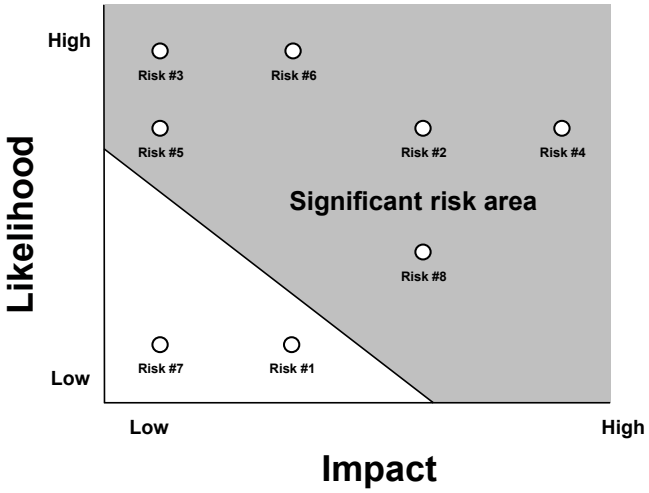


Figure 5 : Significant risks

In reality, the boundary separating what we consider to be significant and insignificant risks is more likely to be a wobbly line than a straight one and its position will largely depend on the organization's risk appetite (see also section 6.3 'Risk appetite').

The possible measures that we can take to mitigate our significant risks are many and varied, and will depend on such factors as the type of risk, its rating and the level of investment that we're willing to make versus the potential downside.

The identification and implementation of risk mitigation measures, also known as countermeasures, are discussed in more detail in the next two chapters.

The risk rating (a combination of the likelihood and impact) is effectively a rating of the significance of each identified risk.

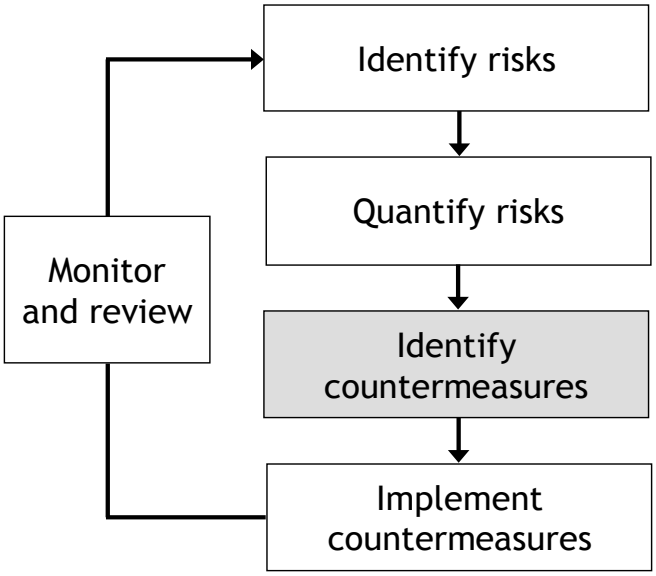
The nearer a risk is to the top right-hand corner of the risk matrix, the more significant it is.

Chapter 4 looks at the third stage in the risk management process – identifying countermeasures...

Chapter 4

In this chapter we consider :

- *The types of risk response options that apply to the various categories of risk*
- *Stage 3 of the risk management process – identifying countermeasures*
- *Some of the countermeasures that you might employ to mitigate your particular risks*



4.1 Addressing our risks

> *"You don't need a parachute to sky-dive – you only need a parachute to sky-dive twice!"*
>
> Anon

Once we've assessed the various risks to our business, we can decide what we want to do about them, prioritising our actions based on the risk rating. Clearly we'll want to concentrate first on those significant risks that fall in the top right hand corner of our risk matrix. We may also choose to address some of the less significant risks, particularly if it's easy or inexpensive to do so. As we move towards the bottom left hand corner there may well be risks that we choose to accept.

Another way of looking at it is illustrated below.

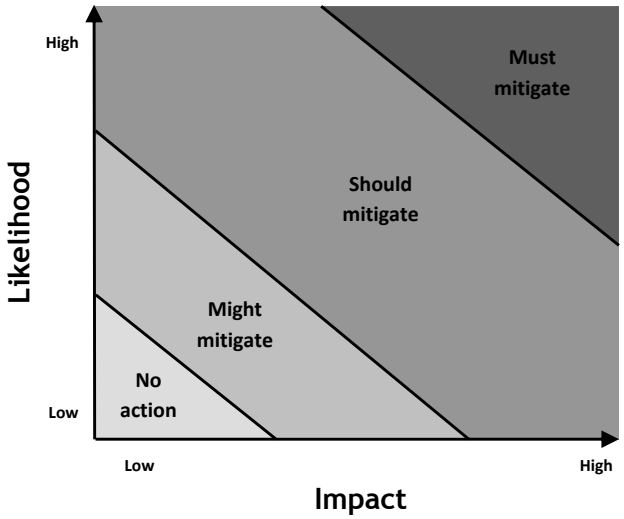


Figure 6 : Risk responses based on significance

So that we can decide what actions to take, we first need to consider some of the possible mitigation measures, otherwise known as countermeasures.

> Once we've assessed the various risks to our business, we can decide what we want to do about them, prioritising our actions based on the risk rating.

4.2 Risk response options

> *"It is impossible to make anything foolproof because fools are so ingenious."*
>
> Unknown

In general terms, the responses to our various risks can largely be divided into four categories, depending on the likelihood of the risk materialising and the impact if it does. It should be noted, however, that there may be some overlap or blurring of the edges because, as with so many things in life, it's not always possible to divide things up into neat little boxes. For instance, transferring risks or insuring against them might apply to risks in either of the two right-most quadrants in the diagram below.

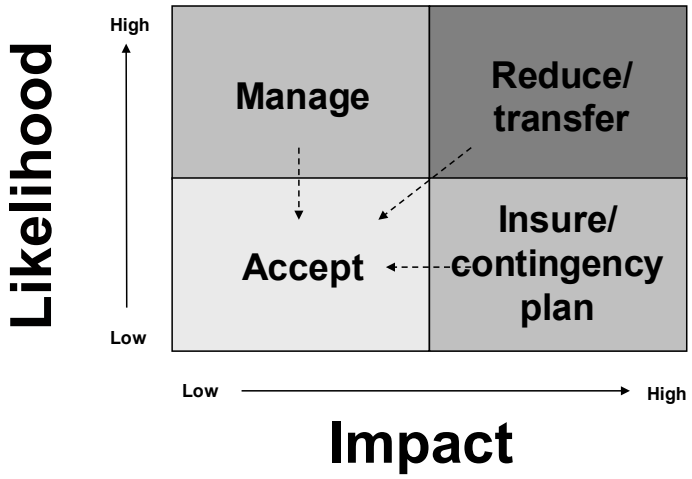


Figure 7 : Risk response categories

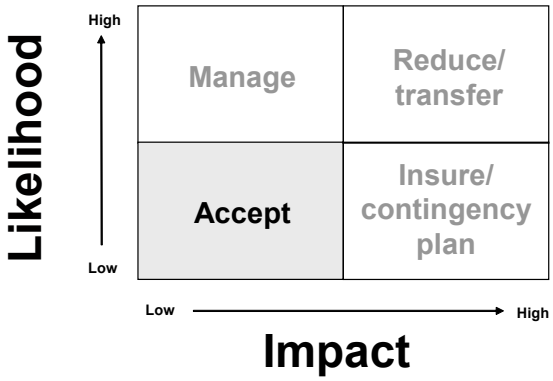
Whichever category a particular risk falls into, the ultimate aim is to select and implement measures that reduce the likelihood or impact (or both) to a level that we are prepared to accept.

The four categories, along with some of the specific risk response options for each, are described in more detail below.

The ultimate aim is to implement measures that reduce the likelihood and/or impact to a level that we are prepared to accept.

Risk acceptance

If the likelihood is low and the impact is low, it may be a perfectly reasonable decision to do nothing and to accept certain risks.

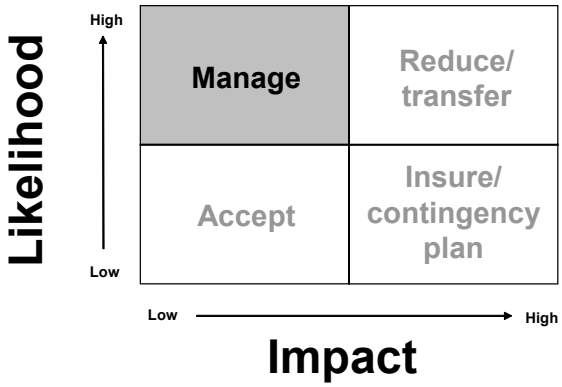


There may also be occasions when, although there is a higher likelihood or impact, it is either uneconomic or even impossible to implement countermeasures, for instance where the cost of addressing the risk outweighs the potential loss. In this event, the only viable option may be to accept the risk. As long as this is an informed decision, it is a perfectly valid decision.

The fact that many risks can't be completely eliminated means that there is likely to be a level of residual risk remaining, even after implementing our mitigation measures (see section 5.2 'Residual risk'). The ultimate aim of an effective risk management programme is to reduce all of our risks to a level that we are willing to accept.

If the likelihood is low and the impact is low, it may be a perfectly reasonable decision to do nothing and to accept certain risks.

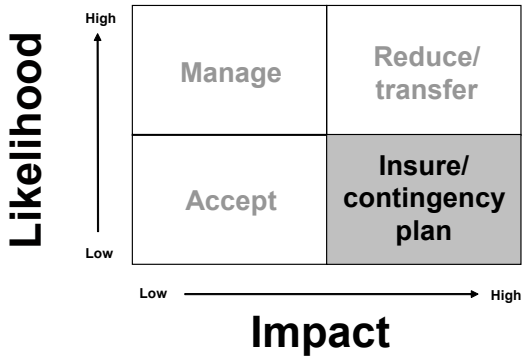
Management



For risks with a higher likelihood but a low impact (such as pilfering of low value items, minor operator errors or other 'glitches' which cause inconvenience as opposed to significant problems), a sensible approach might be to manage and control them, for instance by improving and documenting processes, by providing adequate training and education and by implementing controls and procedures to regularly monitor and review the situation.

> Risks with a higher likelihood but a low impact may be managed by improving processes, documentation, training, education and monitoring.

Contingency planning



If the likelihood is low but the impact is high (such as loss of operational capability, serious damage to our reputation, large financial losses or even failure of the business), contingency plans should be developed.

Often referred to as business continuity (or, in some cases, disaster recovery) plans, the purpose of contingency plans is to ensure that our business-critical functions or processes can continue to an acceptable, perhaps emergency level in the (hopefully unlikely) event of some sort of catastrophic disruption.

Whilst we all hope that this type of event will never happen, spending a little time and effort considering what's important to the business and thinking through alternative means of providing them will pay dividends if the worst does happen.

Some obvious examples of the types of risk mitigated by contingency planning include fire, flood or explosion, but it may also be prudent to consider risks such as the loss of a major customer, changes to the business environment, our marketplace, or in consumer behaviour, product contamination, bad publicity, failure of critical equipment, loss of key staff and a whole host of other potential 'disasters'.

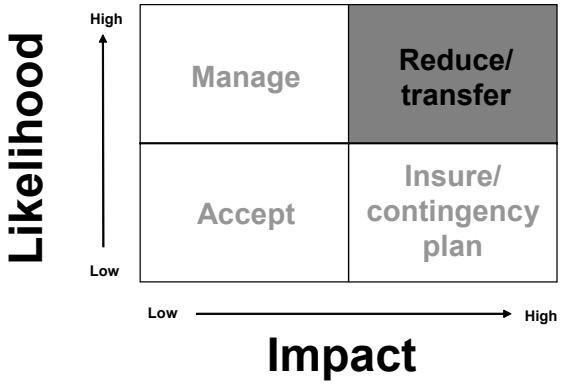
Contingency plans may include such things as :

- Evacuation;
- Crisis or incident management;
- Communication with customers and other stakeholders (including the media);
- Sourcing alternative premises, plant or equipment;
- Relocation and recovery of critical business functions and their supporting infrastructure or services;
- Alternative means of supply and/or distribution.

However, whilst contingency plans are a very good idea, it's always worth remembering that the old adage 'prevention is better than cure' holds good if prevention is at all possible – after all, it's far better not to have a disaster in the first place if it can be avoided!

> For risks with a low likelihood but a high impact, contingency plans should be developed (often referred to as business continuity or disaster recovery plans).

Risk reduction



For risks with a high likelihood and a high impact, risk reduction measures are absolutely essential.

For instance, hazardous or dangerous procedures should be modified, stringently controlled and monitored or outsourced to someone more qualified or better equipped to carry them out safely (see 'Transferring risk' in section 4.3 'Identifying countermeasures').

In extreme cases, if the potential downsides far outweigh the potential benefits, a decision to discontinue the activity altogether may be considered.

> For risks with a high likelihood and a high impact, risk reduction measures are absolutely essential. This type of risk cannot be ignored.

More information on specific countermeasures within the various categories can be found in the next section.

4.3 Identifying countermeasures

> *"Chance favours the prepared mind."*
> Louis Pasteur

For risks that we're unwilling or unable to accept, there are numerous possible countermeasures, or mitigation measures, that we may consider, within the categories of reduction, management and contingency planning described in the previous section.

The specific countermeasures we select to address each risk will vary depending upon the type of risk, its rating, our appetite for risk and our budget, but may involve steps to transfer, reduce or control the risk. Some of the possible countermeasures are shown below.

Transferring risk

Transferring the risk to someone else can be achieved by taking out insurance or perhaps by outsourcing certain high risk or 'non-core' activities or processes.

Remember though, that outsourcing carries its own risks, which also need to be assessed before making a decision. You need to be fully aware of what's being provided by the outsourcing arrangement (and what's not) and where the risks lie, as you may still need to put in place some mitigation measures. You might also want to satisfy yourself that the outsourcer takes their risk management seriously and that they have a contingency (business continuity) plan in place. And remember too, that as far as your customers and other stakeholders are concerned, the buck stops with you, not the outsourced supplier.

> Outsourcing can be an effective risk management strategy. However, outsourcing carries its own risks and these need to be properly understood.
>
> As far as customers and other stakeholders are concerned, the buck stops with you, not the outsourced supplier

Insurance

Insurance is a common, and extremely important, form of risk management. Depending on the specifics of your particular business and your personal circumstances, certain types of insurance will be necessary or desirable. There are many types of insurance, some of which are listed below. Insurance is, however, a complex area and professional advice should be sought as to the specific types and levels of insurance that you should consider for your business.

- Buildings and contents
- Goods in transit
- Business interruption
- Consequential loss
- Directors' and officers' (D&O) insurance
- Increased cost of working
- Employers', public and product liability
- Professional indemnity
- Loss of profits
- Warranty insurance
- Legal expenses
- Life and health
- Motor vehicles
- Electrical or mechanical breakdown
- Money (cash, cheques, etc on the premises, at employees homes and in transit)
- Credit risk
- 'Key person' insurance
- Income protection
- Travel insurance
- Personal accident and sickness
- Private medical insurance

Insurance may provide a safety net for your business if things go horribly wrong. But do bear in mind that insurance only addresses (some of) the financial impacts of some of your risks. It merely provides a pre-defined sum of money in the event that certain pre-defined risks occur. It almost certainly won't pay out immediately - in fact, experience has shown that insurance can take months, or even years, to pay out and that the claims process is often fraught with difficulties (strangely enough, paying out on claims isn't the favourite activity for most insurance companies!).

In the meantime, what it won't do is keep your business operating or protect your cash flow in the short term. It won't stop your customers going elsewhere or protect your market share. It won't protect your reputation or replace the goodwill you've painstakingly built up, possibly over a period of many years. And it's a sobering thought that the sums paid out are often less than anticipated, and often don't actually cover the full value of the losses incurred.

It's vital that you clearly understand what your various insurance policies cover and, as importantly, what they don't, so that you can supplement your risk management strategy with other appropriate mitigation measures. In any case, insurance shouldn't be seen as a substitute for other mitigation measures.

Often insurers will, quite reasonably, require you to have other measures in place to reduce the likelihood and/or impact of the insured risk(s) occurring - in other words, to reduce your, and their, risk of a claim arising.

The appropriate use of insurance is an important weapon in your risk management armoury, but it's a big mistake to view it as the only weapon. And it should be seen as the last line of defence, rather than the first.

> Insurance is an important weapon in your risk management armoury, but it should be seen as the last line of defence, rather than the first or the only one.

Risk reduction and control

Risk reduction and control measures may include (though are not limited to) the following. Please note that the risk reduction and control measures shown here are grouped under the various categories (strategic, operational, financial, etc) for illustrative purposes. Some measures may, in reality, apply to more than one category or may fall under a different category in your particular environment.

Strategic :

- Multiple locations (e.g. production, warehousing, offices)
- Market intelligence/research
- Joint ventures/partnerships
- Divestment (e.g. unprofitable/non-core business)
- Diversification
- Cessation of high risk activities

Operational :

- Fire detection and suppression
- Physical security measures (e.g. security guards, intruder detection, access control, etc)
- Duplication of, or built-in redundancy in critical equipment or functions

- Regular maintenance
- Policies and procedures - ensuring things are done in a certain way, every time
- Buffer stocks
- Automation
- Stock control and regular stock checks
- Alternative/multiple suppliers
- Quality assurance
- Documentation

Financial/commercial :

- Customer relationship management
- Authorisation levels/purchasing limits
- Contractual terms and conditions
- Financial controls
- Cash flow management
- Credit limits and credit references
- Overdraft facilities
- Hedging
- Cost control
- Futures/options
- Factoring/invoice discounting
- Segregation of duties/processes (e.g. authorisation from payment)

Regulatory/compliance :

- Due diligence
- Monitoring and reporting

Health and safety :

- Evacuation procedures
- Personal protective equipment
- Safety devices/guards on equipment/machinery
- Health and safety reviews and targeted risk assessments
- Safe systems of working
- Good housekeeping

Personnel :

- Employing suitably skilled/experienced staff and contractors
- Background checks on new employees
- Supervision
- Training (including cross-training)

- Good working conditions
- Management reviews
- Job rotation and succession planning
- Good employee relations

Technology :

- Information security measures (e.g. secure passwords, restricted access, virus checking, firewalls, etc)
- IT backups
- Uninterruptible power supplies or standby generators

Project :

- Project management methodology
- Experienced/skilled project manager(s)

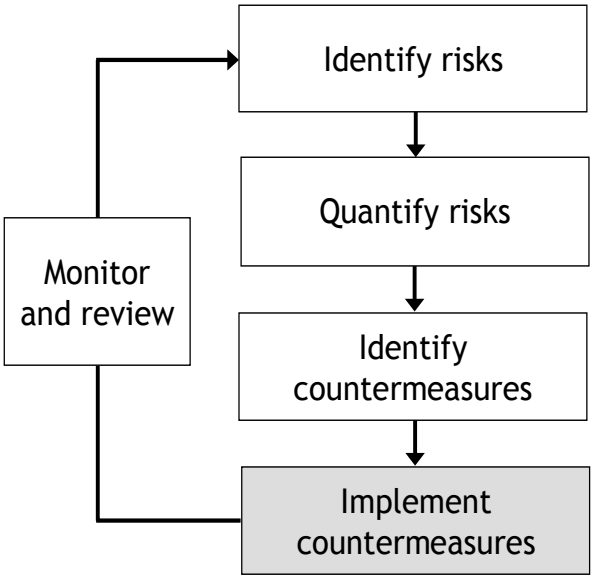
The above list is by no means an exhaustive one and you may well come up with additional countermeasures that address your own particular risks.

Chapter 5 looks at the fourth stage in the risk management process – implementing countermeasures...

Chapter 5

In this chapter we consider :

- *Stage 4 of the risk management process – implementing countermeasures*
- *Residual risk – the level of risk remaining after implementing our selected countermeasures*
- *Risk registers*



5.1 Implementing countermeasures

> *"We are ready for any unforeseen event that may or may not occur."*
>
> George W. Bush

There's little point spending time and effort identifying and quantifying our risks and thinking about the countermeasures that we can implement to address them if we then do nothing else. We can assess risks until the cows come home, but it's what we then do about them that really matters, otherwise it's all been a bit of a waste of time.

In order to make our business more resilient we now have to make some decisions and take some action. It may seem blindingly obvious, but it's an often overlooked fact that merely writing down our risks in a risk register (see section 5.3) won't actually protect our business or make it any more robust.

> Merely writing down our risks in a risk register then filing it away doesn't actually make our business any more resilient - it's what we then do about them that really matters

So we now have to turn our attention to implementing some of those countermeasures and deciding how much time, effort and money we want to invest in mitigating our more significant risks.

No business, no matter what its size, has limitless resources to invest in risk management. In any case, there's little benefit and little sense in spending a fortune addressing a risk which is unlikely to happen and which would have minimal or no impact even if it did. On the other hand, if a risk that has the potential to cause significant harm or to put you out of business is likely to occur, a substantial investment (in money, time or other resources) may be needed to reduce the likelihood and/or the impact to an acceptable level, or serious consideration should be given to whether it's a risk that's worth taking at all. The countermeasures that we choose must therefore be appropriate, pragmatic and cost-effective.

Once we've selected the countermeasures to be implemented, it's important that the implementation process is properly managed. It may be that some countermeasures are fairly quick and easy to implement, whereas others may require significant effort, cost or time. The latter type will probably need to be managed as a formal project, with all that that entails. Either way, it's important to allocate responsibility for implementing specific countermeasures, whether to a particular director or manager, a project manager or a member of staff. Often, risks are not properly mitigated because it was wrongly assumed that the proverbial 'someone else' had dealt with it.

> It's important to allocate responsibility for implementing specific countermeasures to ensure implementation actually takes place.

5.2 Residual risk

It's impossible to totally eliminate risk and there will almost always be some level of risk remaining after we've implemented our countermeasures. This is often referred to as residual, or net, risk (gross risk being that which exists before mitigation). As discussed previously, the aim is to end up with a level of residual risk that we're willing to accept.

It's also possible that reducing risk in one area might actually have the effect of increasing the level of risk elsewhere. Examples might include :

- A business employs a factoring company to aid cash flow, but customers are upset by the factoring company's methods of chasing payments, resulting in customer dissatisfaction and a negative impact on reputation;

- Consolidation of premises and facilities to reduce costs and improve efficiency reduces resilience and results in a single point of failure;
- Moving the production of products or components overseas to increase competiveness results in a reduction in quality and an increase in failure rates;
- Training staff to enhance skills, increase productivity and reduce operational errors makes them more marketable and increases the risk of losing staff to competitors.

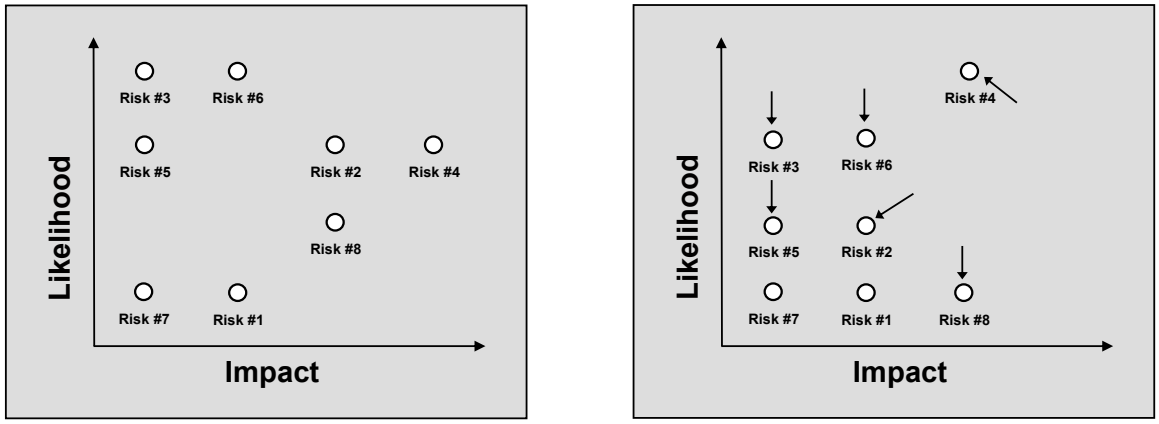


Figure 8 : Residual risk

Whilst it's important to give individual risks the focus they deserve, we also need to ensure that we keep an eye on the bigger picture to ensure that our overall risk levels are acceptable (see also Chapter 6, which discusses the need for ongoing monitoring and review).

This brings into play the concept of enterprise risk management. Whether yours is a huge multinational corporation, a five-person business or somewhere in between, a co-ordinated approach to risk management is desirable, if not essential, if the entire portfolio of risks is to be effectively managed.

> There will almost always be some level of residual risk remaining after we've implemented our countermeasures.
>
> The aim is to end up with a level of residual risk that we're willing to accept.

5.3 The risk register

The risk register is a very simple but very useful tool, which will help you to manage your risks. It's a document that summarises the risks (and opportunities) identified, along with the likelihood, impact and the resulting risk rating and the appropriate countermeasures for each, plus the actions that you've decided to take and the current status of them.

Once you've been through the process of identifying risks, assessing their likelihood and impact and identifying countermeasures, you will have much of the information you need to create your risk register(s). All that's required is to create a table or spreadsheet similar to the example below, populate it with the information gathered from your risk assessment workshop(s), then assign specific actions, with associated responsibilities and timescales.

#	Risk/Opportunity	Likelihood	Impact	Rating	Countermeasures	In place?	Actions/Status/ Comments	Person responsible	Due date/ Complete
1	Risk 1	1	2	2	Countermeasure1 Countermeasure 2	Y N			
2	Risk 2	3	3	9	Etc				
3	Risk 3	4	1	4					
4	Risk 4	3	4	12					
	Etc								

Figure 9 : Example risk register

The key point here is that the risk register should be a working document, that's reviewed and updated regularly, not something that's produced once and then filed away, never to be seen again.

Ideally (and depending on the size and structure of the business), each department or business function should create and maintain its own risk register, for the risks that apply to them and that they are able to do something about, with a central risk register for the business-wide or 'bigger picture' risks. However, it's very much 'horses for courses', and, at the end of the day, a single risk register is much better than none at all. Whether you plump for one or several, it's important that each risk register is owned by someone, who is given responsibility for its upkeep.

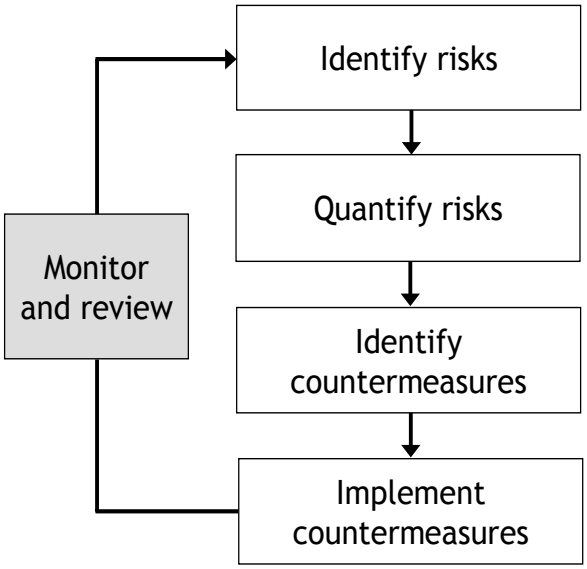
> The risk register should be a working document, that's regularly reviewed, acted upon and updated.

Chapter 6 looks at the final stage of the risk management process – ongoing monitoring and reviewing...

Chapter 6

In this chapter we consider :

- *Stage 5 of the risk management process – ongoing monitoring and reviewing*
- *Assessing the effectiveness of our selected countermeasures*
- *The appointment of a risk group to monitor risks and associated actions across the business as a whole*
- *The organisation's risk appetite*
- *The benefits of a risk-aware culture and the roles of key groups of people in embedding one*



6.1 Monitoring and reviewing

> *"It is clear that risk management is now a core business process and should be planned accordingly and on a continuing basis so as to reduce risk and volatility and improve returns."*
>
> Institute of Chartered Accountants in England and Wales

The final stage in the risk management process is to monitor and evaluate the results of our risk mitigation measures.

For each countermeasure put in place we should consider whether :

• It does the job it's intended to do.	To what extent does it address the risk? If it doesn't do the job fully, can we do anything to improve things?
• It reduces our overall exposure to risk.	In some cases, too much focus on reducing one risk can actually increase other risks. We need to be aware of this, avoid being too blinkered and consider the bigger picture too.
• It improves efficiency.	In addition to mitigating specific risks, modifying and improving processes, procedures and working practices can often have a positive effect on the day to day running of the business by reducing operational errors, failures or outages and increasing efficiency.
• It continues to be cost effective.	Do we reach a point where the cost outweighs the benefit? If so, is there anything we can do to improve the situation? Or should we drop it and consider other mitigation measures instead?
• The level of residual risk is acceptable.	This is not a decision to be taken lightly. Bear in mind that accepting a risk also means acceptance of the consequences if it does occur.
• It's being adhered to.	If the countermeasure requires a process or procedure to be followed or some other form of manual intervention, is it being carried out correctly and consistently? Merely assuming that it is could be risky – you need to regularly check and monitor the situation.

There's an old adage that 'what gets measured gets done', so it's important that we review and assess the effectiveness of our risk mitigation measures. There are a number of ways in which this can be done. For instance, we might look at the following metrics :

- Financial measurements, e.g. :
  - Cash flow
  - Revenue
  - Costs
  - Profit margins

- Operational measurements, e.g. :
  - Service delivery
  - Productivity
  - Quality control
  - Equipment/IT failure
  - Operator errors
  - Accidents
  - Downtime

- Commercial measurements, e.g. :
  - Increased sales
  - Lost sales
  - Contractual issues

- Customer feedback, e.g. :
  - Customer service ratings
  - Complaints
  - Accolades
  - Repeat business

It's important that we review and assess the effectiveness of our risk mitigation measures.

As well as keeping an eye on the effectiveness of our risk control measures and identifying changes or improvements to existing countermeasures, regular monitoring and review will ensure that new and emerging risks, changes to existing risks and new opportunities are captured and addressed appropriately.

The frequency will vary depending on a number of factors, including the type of business you're in, the rate of change (both within the business and within the environment or marketplace in which it operates), the type of risks and the specific controls implemented and any regulatory requirements (for instance, health and safety legislation requires certain risks to be periodically reviewed or re-assessed when certain changes occur).

The main point is that this should be an iterative process, rather than a one-off exercise if risks are to be effectively managed.

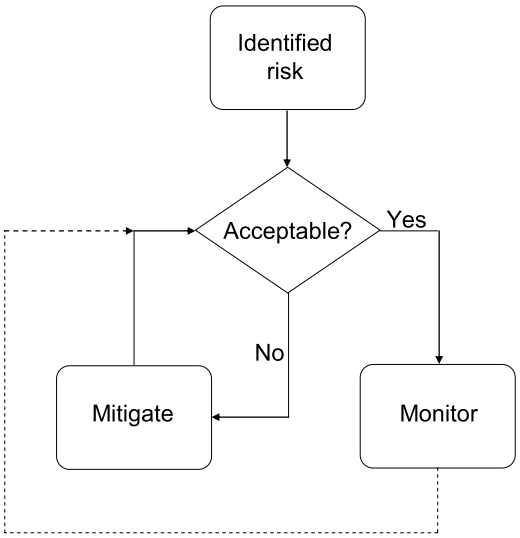


Figure 10 : Ongoing monitoring and review

Most reviews are carried out internally, and regular internal reviews or audits have a key part to play in the risk assessment process. It may, however, also be beneficial to obtain an independent assessment from external experts from time to time. Indeed, in some cases external audit of the effectiveness of controls may be a regulatory or statutory requirement.

> Risk management needs to be an iterative process, rather than a one-off exercise if risks are to be effectively managed.

6.2 Joining it all up

> *"Efforts and courage are not enough without purpose and direction."*
>
> John F. Kennedy

In order to ensure that risks are managed in a consistent way across the business, rather than in isolated pockets, it can be beneficial to appoint some form of risk management steering group. Indeed, many organisations employ this approach very successfully as part of their risk management structure.

The size and composition of the group and the frequency with which it meets are likely to vary from business to business, but it usually comprises management representatives from each key area and reports directly to the Board or senior management team. This reporting usually includes identification of the key risks (often the top ten) facing the business and updates on the status of these risks.

The role of the risk management steering group is to monitor risks and associated actions across the business as a whole, ensuring that key risks affecting more than one area or those that can't be addressed by a single department or function are escalated and treated appropriately. The advantages include :

- A consistent, co-ordinated, business-wide approach to risk management;
- Consideration of 'the bigger picture' and monitoring of the overall level of risk;
- A strategic, as well as tactical, view of risk;
- Key risks being given the focus and attention that they deserve, including awareness at the highest level of management.

A risk management steering group, management representatives from each key area, can help ensure that risks are managed in a consistent way across the business.

6.3 Risk appetite

> *"The early bird catches the worm, but the second mouse gets the cheese."*
> Unknown

People are individuals and we all have our own particular appetite for risk. Some people are extreme risk takers who think nothing of taking huge risks, both in their business and personal lives, which the mere mortals among us would cringe at the very thought of. Others are far more reserved, to the point of being almost totally risk averse, avoiding almost any situation in which there is even the slightest hint of risk. The vast majority of us fall somewhere in between.

Similarly, all organisations have a 'corporate' risk appetite, which dictates the types and levels of risk that the organisation, or at least the Board or senior management team that directs it, are willing to take or to accept. One of the key roles of the Board or senior management team is to decide on the level of risk that the business is willing to take in seeking to exploit opportunities.

The problem is that it can be very difficult to pin them down and get them to define the corporate risk appetite, partly because it's quite difficult to put into words and partly because it's actually quite subjective and can change depending on factors such as the prevailing business environment, the timing or even the personalities, personal experiences or professional (or emotional) judgement of the decision makers. So few organisations bother to do so, and fewer still actually document and publish a formal statement of risk appetite to their managers and staff, which can make life a bit difficult for them in terms of their own risk management efforts.

> A key role of the Board or senior management team is to decide on the level of downside risk that the business is willing to take in seeking to exploit opportunities.

Whilst it's not always possible to come up with a clearly defined and agreed statement of the corporate risk appetite before embarking on your risk management programme, it's a good idea for the Board or senior management team to give some direction on the levels of risk that they're willing to accept and those which they aren't - for instance the level of financial, customer service, reputation, and other types of impact that they're comfortable with.

One way of doing this is to agree with them what the risk matrix should look like; to at least help define the boundaries for the green, amber and red segments. And, once the significant risks (particularly the 'bigger picture' ones) have been identified and quantified, they should be asked for confirmation (ideally in writing as this always helps to focus the mind!) of which specific risks they are willing to accept and which they want to address in some way.

It's entirely possible that the acceptable levels of risk will vary from one risk category to another – for instance, a high level of strategic or equipment risk or opportunity risk may be acceptable, whereas the opposite may well be true of health and safety or reputational risk. In this case, an effective approach may be to ask for clarification of the acceptable levels of risk in each of the various categories.

Whichever approach is taken, getting a steer from those at the top can be hugely beneficial. It helps to get their buy-in, ensures a consistent approach, makes the risk assessment process more productive and can potentially save a significant amount of wasted time and effort by preventing managers and staff from barking up the proverbial wrong tree.

> The involvement of the Board or senior management team and their input regarding their risk appetite is often the difference between a successful risk management programme and one that flounders.

6.4 A culture of risk awareness

> *"Tell me and I forget. Show me and I remember. Involve me and I understand."*
>
> Chinese Proverb

A key objective of the risk management programme is to make people risk aware, as opposed to risk averse, and to embed that awareness throughout the business.

It's worth noting that the most successful risk management processes are those that involve not only senior management but all employees – in other words, a 'top-down and bottom-up' approach. Involving people, raising awareness and giving them responsibility for managing the risks within their control can have a significant impact on the overall resilience of the business.

It's all very well for executive management to make statements in the annual report about how wonderful the risk management system is, but that in itself doesn't make the organisation more resilient. If it isn't backed up by action then it's not worth the paper it's written on.

A successful risk management approach requires a two-pronged attack, which includes buy-in from both the executive and business managers. There needs to be commitment at Board level, but the operational parts of the business also need to be involved to make it happen.

The most successful organisations in this respect are the ones who manage to embed risk management in their culture – where executive support is visible; where risks and associated mitigation measures are identified at all levels; where risk registers are maintained by departmental managers and team leaders; and where risk management is seen by all employees as just a normal part of the way they do their jobs.

To this end, various people within the business have various roles to play. Depending on the size and nature of the business these key groups, and their associated roles and responsibilities, may include :

Directors/senior management

- Visibly support the risk management process
- Agree and publish a risk management policy, setting out the scope, objectives, roles and responsibilities
- Set and communicate the organisation's risk appetite (acceptable levels of risk)
- Be aware of significant risks, in particular strategic risks, facing the business
- Monitor the effectiveness of the risk management process
- Report to stakeholders on the effectiveness of the risk management process in achieving the business's strategic objectives

Risk management steering group

- Support and facilitate the risk management process
- Monitor risks and associated activities across the business
- Report on the status of key risks and mitigation measures to the Board/executive management team
- Ensure appropriate levels of awareness and involvement throughout the business

Business managers/team leaders

- Be aware of the risks within their particular area of responsibility
- Apply the risk management process to identify significant risks and implement or recommend mitigation measures
- Manage risks on a day-to-day basis
- Facilitate staff awareness
- Report on the status of risks and mitigation measures to the directors/senior management (perhaps via the risk management steering group)

Individuals

- Understand their roles, responsibilities and accountabilities within the risk management process
- Identify and rate risks and suggest possible mitigation measures
- Report on the status of risks and mitigation measures to team leaders/business managers

> A key objective of the risk management programme is to make people risk aware, as opposed to risk averse, and to embed that awareness throughout the business.

Chapter 7 brings things to a conclusion and suggests what your next steps might be...

Chapter 7

In this chapter we consider :

- *What we should do next*

7.1 Where do we go from here?

> *"Educated risks are the key to success."*
>
> William Olsten

Your risk assessment will have identified a number of risks and associated mitigation measures. Some of these mitigation measures will be achievable without requiring significant resource or expenditure, whilst others may require considerable financial investment and may take some time to implement. The level of investment that you are prepared to make and the level of residual risk that you are prepared to live with can only be decided by you and your management team. They will depend on available funds, the strategic view of senior management and the corporate risk appetite. However, once risks have been identified they cannot simply be ignored. You must now decide, and sign up to, which risks you are willing to accept and which you are not.

It should be borne in mind that effective risk management is an ongoing process rather than merely a one-off exercise, which needs the active involvement of people across the whole business. It's therefore important that the risks identified are managed and monitored, and also that risk assessments are conducted regularly - as part of the project or change management processes, when making key strategic or operational decisions and, quite simply, as a component of good management practice.

The transition to the more formalised and regular approach suggested in this book should not be overly onerous, provided that you keep things simple. It does, however, require senior management support and although this will entail some effort, the potential rewards include a more robust and resilient business that's more likely to achieve its strategic goals and objectives.

Once risks have been identified they cannot simply be ignored. You must now decide, and sign up to, which risks you are willing to accept and which you are not.

The potential rewards include a more robust and resilient business that's more likely to achieve its strategic goals and objectives.

If you've picked up just one thing from this book that has prompted you to think seriously about a significant risk, or risks, to your business, then reading it has been time well spent. But that's not really enough. By definition, if a risk is significant, then something really should be done to mitigate it. Therefore, if you now take no further action you're not only missing a trick, but you're knowingly putting your business at risk.

So, if you haven't already done so, why not take a little bit of time to think about the countermeasures you can sensibly put in place, then complete the risk management process by implementing them and monitoring them for effectiveness? Your business will be that much stronger as a result and it might just help you to sleep better at night!

The rest, as they say, is up to you.

7.2 Conclusion

> *"The most elegant forms of managerial decision involve problems that never have to be solved because they are prevented from occurring…they are anticipated and side-stepped. The deliberate non-catastrophe is one of the most effective contributions a manager can make."*
>
> James Martin

If properly done, risk management is a wise investment. It can help us when planning and starting up our new business ventures and during our ongoing business operations. It can help us to increase the chances of successfully exploiting new opportunities, The resulting risk reduction and resilience measures can pay dividends by improving processes and reducing the occurrence of everyday problems. Risk management can help us ensure that we have the correct types and levels of insurance in place. It can give us the confidence that as far as possible we are safeguarding our businesses and our livelihoods from the threat of failure, disruption or disaster.

We can't avoid risk. But we can manage it to our advantage. The most effective way to do this is to make risk management part of the business's culture. Whether it employs just a few, a few dozen or hundreds of people, your business needs to manage its risks and everyone in the business has a part to play, from the Chief Executive to the office junior.

We can't avoid risk. But we can manage it to our advantage. The most effective way to do this is to make risk management part of the business's culture.

By using a few simple techniques, as described in this book, each of us can identify the risks to our part of the business and the countermeasures that can be put in place to reduce the likelihood and/or the impact of the most serious, thus strengthening each part of the business.

Risk management isn't just the domain of the professional risk manager and it's not just for huge corporations. It's a versatile management tool that can, and should, be used by everyone.

Risk management is a versatile management tool that can, and should, be used by everyone.

Appendices

The appendices contain :

- *Some suggestions for further reading*
- *Some useful sources of information*
- *Acknowledgements and thanks*

Appendix 1 Further reading

BS31100 Risk Management Code of Practice - British Standards Institution, ISBN 978-0-580-57434-4

The Complete Guide to Business Risk Management (second edition) - Kit Sadgrove, (Gower Publishing), ISBN 978-0-566-08661-8

Five Steps to Risk Assessment (leaflet) – Health and Safety Executive (HSE Books), ISBN 0-7176-6189-X

Risk Management Simplified - Andy Osborne, ISBN 978-1-906316-48-8, www.riskmanagementsimplified.co.uk

Practical Business Continuity Management – Andy Osborne, ISBN 978-1-906316-01-3, www.practicalbcm.co.uk

Risk Management – Institute of Directors (Director Publications), ISBN 1-9045-2044-8

A Risk Management Standard (AIRMIC, ALARM, IRM) – downloadable from any of the associations' websites

Appendix 2 Some useful sources of information

Acumen Business Services Ltd
www.acumen-bcp.co.uk and www.acumen-bcp.co.uk/blog
Basepoint Business Centre, Crab Apple Way, Vale Park, Evesham, Worcs WR11 1GP
Telephone : 01386 834455

Association of Insurance and Risk Managers (AIRMIC)
www.airmic.com
6 Lloyd's Avenue, London EC3N 3AX
Telephone : 020 7480 7610

ALARM (public sector risk management association)
www.alarm-uk.org
Ashton House, Weston, Sidmouth EX10 0PF
Telephone : 0333 123 0007 or 01297 680417

Business Link
www.businesslink.gov.uk

Business Continuity Institute
www.thebci.org
10 Southview Park, Marsack Street, Caversham RG4 5AF
Telephone: 0118 947 8215

Continuity, Insurance and Risk (CIR)
www.cirmagazine.com

Institute of Risk Management (IRM)
www.theirm.org
6 Lloyd's Avenue, London EC3N 3AX
Telephone : 020 7709 9808

UK Resilience
www.cabinetoffice.gov.uk/ukresilience
Cabinet Office, 22 Whitehall, London SW1A 2WH
Telephone : 020 7276 1234

NB The above information is provided for reference and educational purposes only and should not be considered as an endorsement of any company, organisation, product or service. All details were correct at the time of going to press.

Appendix 3 Acknowledgements

Section 4.2 'Risk Response Options' and the final paragraph in section 1.5 'Me, a risk manager?' were based on original text by Ian Charters, first published in chapter 9 of The Definitive Guide to Business Continuity Management, Wiley,1999.

The diagram in section 4.1 'Addressing our risks' was based on an original by James Royds, formerly of Infosec Associates.

Elements of section 6.3 'Risk appetite' relating to obtaining the Board's input on the corporate risk appetite were inspired by a suggested approach presented by John Robinson of Inoni.

Elements of the roles and responsibilities shown in section 6.4 'A culture of risk awareness' were based on original text in section 6 of 'A Risk Management Standard', published by AIRMIC, ALARM and IRM.