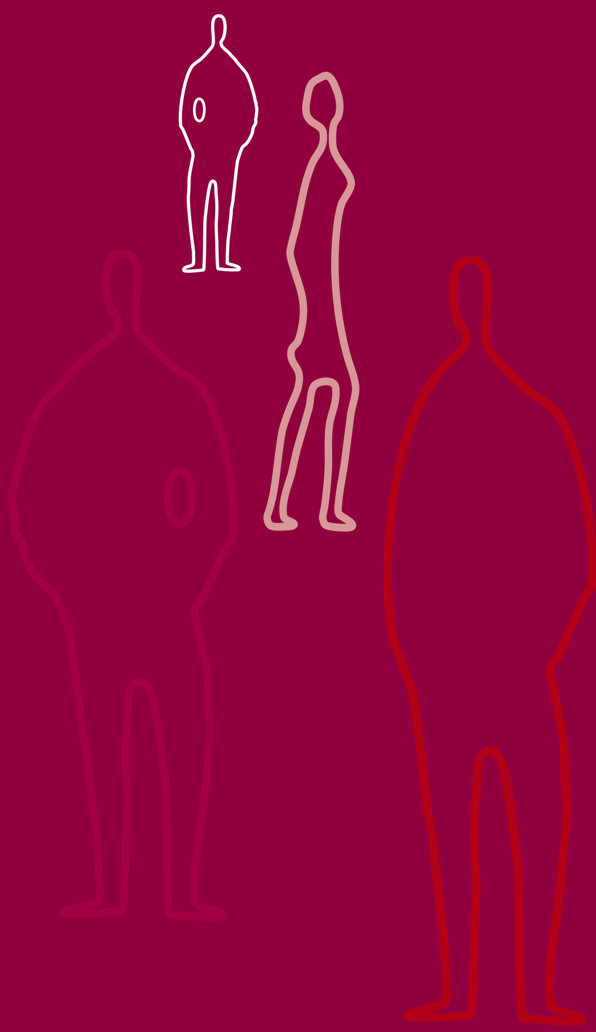
An Introduction to Risk Management in Business



Barclay Simpson
Recruitment Consultants

Contents

1. Introduction

There is an element of risk in everything that we do in our business and personal lives. The Chinese word for risk contains two characters; danger and opportunity. Business typifies this constant balance. If we remove all danger or downside risk, then we create barriers to exploiting opportunities or benefits. Conversely, if we ignore all downside risk or do not manage it effectively, then we increase the likelihood of a major negative effect.

In some cases we may be ignorant of the risks and the potential impact. The element of chance means that we may have enjoyed the benefits of taking a risk without the downside having manifested itself. If chance was not in our favour then we may have experienced an unpleasant surprise or unwanted event.

On a personal basis the management of risk is often instinctive and relatively simple. We have automatic reactions that help us control our exposure to negative physical and emotional events. For example, the nerves in our body send messages to the brain when a part of our body is close to a source of heat. The messages warn us that there is a risk of burning. Our reaction is instinctive – we withdraw that part of the body from the source of heat.

While some of these instinctive controls are useful in the management of business risk, the context is much more complex. Their identification and management is learnt through experience and training before it becomes instinctive or properly integrated into the running of the organisation.

Management and the staff in a business need assistance to gain this knowledge and put in place the appropriate controls and processes to manage the risks within acceptable tolerances. This is the role of the risk management experts. These experts must operate at the strategic or corporate level as well as at the operational level.

This guide describes the deliverables and benefits to a business; the management structures; the processes and tools to put in place an effective management of business risk. It also addresses the challenges to success and some of the pitfalls.

2. Deliverables

Successful management of business risk will deliver improved strategic planning and execution, better exploitation of business opportunities, enhanced stakeholder confidence and improved compliance with business practices, codes and the law. However, it must be stressed that this improved management will not entirely eradicate the risk of unwanted events.

2.1 Improved Predictability

The identification and analysis of risks will help avoid unexpected or unidentified events impacting the organisation's short and long-term performance. This is also true in the case of mergers, acquisitions or disposals where unplanned or unwanted events are considered in advance and contingency plans are developed as part of the risk management process.

Planning and budgeting processes that include risk assessment and control as well as sensitivity analysis will improve results predictability at the business level. Where the plans and budgets are aggregated to the corporate levels, so are the risks. This enables a range of acceptable performance or risk tolerance to be more accurately predicted.

A clear communication of the business risks and their control helps functional and business managers to justify their plans and budgets as well as helping the board to understand the risks and improve their confidence in the robustness of the planning.

2.2 Exploiting Opportunities

A common impression is that the risk management process is designed to minimise or remove risk from the business. Audit processes sometimes reinforce this. But this is not the case, a satisfactory risk management culture in an organisation delivers a clear understanding of acceptable risk types and levels to take (risk tolerance) within the context of the business environment. These may vary between subsidiaries or business units.

In a company's well-managed risk framework, there is the freedom to take more risk with reasonable controls in place. The board can balance the need to take high risks in some parts of the business against more consistent revenues in others. A risk averse organisation will have a higher level of control, a more cautious business plan and may well stifle opportunities for growth or be unwilling to take them. An aggressive risk-taking organisation without reasonable control increases the risk of missing its business targets and losing the confidence of shareholders and stakeholders.

Good risk management will not eliminate all unwanted events. If they do occur, their management can be turned into an opportunity to enhance the organisation's image. This has been achieved by good contingency planning, damage limitation and disaster recovery.

2.3 Improved Investor/Stakeholder Confidence

When unexpected events or results occur, investors and stakeholders view their management as an indication of the organisation's ability to run the business and achieve the expected results.

In cases where a major incident has been well managed the reputation of the group will have often been enhanced. Good and bad examples of this are evident in industries that have an impact on safety and the environment. Organisations that have vulnerable points in their business processes or manufacturing chains can enhance investor confidence through business continuity and recovery programmes.

Delivering predicted financial results and no unpleasant surprises year on year will help to increase the confidence of both investors and stakeholders. This can only be achieved by skilled management of the business including the business risks.

2.4 Compliance

A proactive approach to risk and control will improve mandatory compliance with legal, fiscal and regulatory requirements. The mandatory areas include:

- Finance, reporting, company structure and registration, etc
- Health & Safety legislation.
- Insurance cover is required by law in the UK and many other countries on certain risks. The key ones in the UK are Employers Liability and Third Party Motor.

Most of Corporate Governance, Risk Management and Control codes are "comply or explain" rather than mandatory. In some companies being compliant may be the sole objective without realising the added value of good management of business risk.

Compliance, is however, becoming more onerous. Corporate governance codes are already in place in most European countries with the UK and Germany leading the way. Outside Europe, the USA is the most dominant with more and more codes and requirements impacting non-US companies. The UK and Germany have the strictest compliance requirements for risk management.

2.5 Getting It Wrong

The impact of inadequate management of business risk in an organisation covers two main areas:

- **Negative impact:**
- Some incidents or events may not have been foreseen. These are often of a catastrophic nature and can impact the future of the organisation. Examples of these are the Andersen collapse following Enron, natural catastrophes, political unrest, major incidents involving the company, etc.
- Other types of events may have been foreseen but their impact was much worse or different than foreseen or perhaps not really considered a risk. Enron, WorldCom, the.com collapse illustrate these events as does the loss of customer confidence in Marks and Spencer during the late 1990s.

- **Lost opportunities:**
- Some organisations are very risk averse. As risks are identified more controls or processes are put in place to limit or eliminate the risk with the result that exploitation of opportunities and creativity is stifled.

3. Structure to Manage Business Risk

Having defined the deliverables that can be achieved from comprehensive management of business risk, a structure is needed to put the processes in place.

3.1 Process and Culture

To manage business risk effectively, an organisation needs the right culture and support as well as processes. When management at all levels of the business integrates assessment and management of risks in their decisions and planning, then the concept has moved beyond compliance and adds value to the business.

The Head of Risk Management's role is to facilitate this change in thinking as well as drive the changes and improvements in processes.

Many of the processes operating at the corporate and operational levels are described below.

3.2 Strategy, Management and Monitoring

To help improve the predictability of strategic and business planning a number of key elements and functions are needed:

Board

- The Board approves the risk management and internal control policy as well as the overall implementation plan.
- It defines and communicates the importance of management of risk, driving the culture from the Board level.
- The directors set the risk tolerance of the organisation defining which risks are unacceptable to the organisation and level of acceptability of the remaining ones. This links to the directors' fiduciary and legal responsibilities.
- The Board reviews and validates the analysis of risk and their control. In the UK this should be done at least annually to comply with the Turnbull Code. Many Boards carry out this review several times per year or on a continuous basis.

Management

- Management at all levels of the organisation is responsible for implementing the Board policies on risk management and reporting progress.
- The internal controls and processes implemented and maintained by management, should be adequate to ensure that business risks can be managed within the tolerances specified by the Board. Controls should be of a level that provides adequate freedom to exploit opportunities.
- Within business units or subsidiary structures, they ensure that adequate resources are available and that appropriate training is provided to all staff.

- Management should also set up a function of independent assurance of the effectiveness of the internal controls and processes. This should be much broader than the financial, IT and process controls traditionally carried out by internal audit. External service providers often cover areas such as environment, health and safety, physical assets, brand, business continuity, etc.

Key Business Processes

- Key business processes should include a risk assessment process designed to manage the business risks within acceptable tolerances. The processes include strategy, business plans, budgets, treasury, capital expenditure approval, mergers, acquisitions and disposals. Embedding the risk analysis and control into these processes assists both management and the Board to ensure that key business risks are identified and controlled within acceptable tolerances.
- Sensitivity analysis is often embedded in many of these processes. It should not be confused with risk assessment as it deals with variables around the assumptions used in the processes.

Head of Risk Management (Risk Manager)

- While the term "risk manager" is commonly used, the incumbent rarely manages risks directly as this is the responsibility of line management. They act as a facilitator to help the Board and management to create the processes and tools to manage risk within acceptable tolerances.
- The Head of Risk Management develops a risk management strategy and plan aligned with the organisation's strategy and drives its implementation. The strategy and plans are normally reviewed and approved by the Risk Steering Group and/or Board.
- The Head of Risk Management is often responsible for facilitating risk assessment at senior management and Board level as well as reporting progress on managing risk in the underlying businesses.
- In most organisations the responsibility for setting and managing risk financing and insurance lies with the Head of Risk Management, as this is an important tool in managing business risk. In some organisations this extends to treasury and other business functions.

Risk Steering Group

- The creation, implementation and monitoring of a risk management strategy, while developed by the Head of Risk Management, is often supervised and validated by a Risk Steering Group generally chaired by a Board member with senior representatives of the businesses as well as the Head of Risk Management.
- The Board delegates this authority to the Steering Group, as the management and control of the programme are too detailed for a main Board activity. The Steering Group routinely reports progress and key issues to the Board.
- An example of the role of this group is:
  - To steer and guide the implementation of the Group's Risk Management Strategy and Policy
  - To recommend changes in policy and the risk management plan to the Board

- To promote and support the improvement of risk management throughout the Group and to co-ordinate resources on group-wide initiatives
- To agree consistent risk processes throughout the Group
- To recommend appropriate levels of risk tolerance to the Board
- To monitor the total level of group exposure to risk
- To review progress and report to the Board
- To agree minimum standards of management of risk.
- To ensure that the Group complies with the Turnbull Code and/or equivalents in the countries in which it operates.

Audit Committee

- The make-up of the Committee and its role are already the subject of several corporate governance codes and outstanding reports that are likely to further influence future governance codes. In broad terms its role is to advise the Board on the effectiveness of the system of internal control.
- The breadth of its responsibilities varies according to the organisation. Some companies restrict its influence to financial control whereas others define its brief as covering controls related to all business risks including reputation, health and safety, corporate social responsibility, environment, etc. Some committees review the key business risks – a responsibility of the Board rather than the Audit Committee.

Operational Business Units

With the corporate level functions and processes in place, the business or operating unit implements the processes and reports on progress. As such operational management is directly responsible for implementing the risk management and control policies of the group including:

- Setting up and use of controls
- Managing risk within acceptable tolerances
- Reviewing effectiveness of control systems
- Reporting progress and problems

Areas of risk to be managed will include the everyday operational issues:

- **Financial control and cash control.** The traditional processes and systems of internal financial control are the key way of managing these risks. The challenge in these areas is to maintain a system of control that is adequate but does not restrict management's freedom to run the business.
- **Stock/inventory control.** As with financial control it is not economically or operationally effective to completely eliminate the risk. The level of control is a balance of risk control against restricting the operation of the business.

- **Health and safety.** While traditionally an operationally-managed risk with local specialist expertise, the management of health and safety is now monitored in the Boardroom. Directors of an organisation can be held personally and criminally liable in the event of a serious workplace accident.
- **Employment and human resources practices.** HR departments are aware of the increasing legislation to protect employees' rights as well as the increasing tendency for legal action. Assisted and occasionally challenged by the risk management professionals, new skills are being used to manage these risks.
- **Security.** This covers 2 areas: personal security and protection of the physical assets of the company.
  - Personal security is partially covered by an effective health and safety culture but also includes political and terrorist risks whether in the normal place of work or by travelling on business to areas of political and personal security risk. Evacuation plans, for example generally cover workplace risks but specialist advice may be needed for staff travelling on business.
  - In the case of physical assets, security generally relates to the risk of theft or malicious damage. This is covered below.
- **Physical asset risk control.** Physical assets include real property and equipment, materials, goods, data and intellectual property. These assets may be exposed to damage, loss or destruction from natural hazards (wind, flood, earthquake, etc), fire, explosion, theft, breakdown, malicious damage, etc. Control of these risks within acceptable risk tolerances will help ensure the continuity of business operations. Methods of control include design of buildings and equipment to resist natural hazards, layout of manufacturing and processes to reduce single point failures, automatic fire protection, security measures against theft. Expertise in these areas is often outsourced.
- **Supply chains.** Today's businesses focus on reducing working capital and the time to deliver their goods and services. To support this approach, more supply chains are being managed at the corporate level to exploit synergies and are mostly just-in-time. As a result the risk of supply chain interruption is increasing, as there is minimal product or components in the chain and little spare time to make up for interruptions. Methods of control include the same ones as used for physical assets as well as ensuring duplicate supplies and limiting bottlenecks.
- **Business continuity.** Proper management of the above risks will minimise the risk of interruption of the business and ensure the continuity of business operations. Where there is interdependency between different operations or locations, in-depth studies are made to evaluate the overall impact on the company.
- **Legal, statutory and trading standards compliance.** Compliance with the law and other mandatory requirements is becoming ever more complex at national, European and world level. Expertise in identifying and managing these risks may be outsourced at the operational level particularly if the organisation is multi-national.

- **Local community relations.** Aligning themselves with corporate policy on ethics and social responsibility, operational management often have considerable freedom to implement these policies according to local needs. Positive handling by management will often not only reduce the risk but also create an opportunity to enhance its brand locally.
- **Environmental management.** As with local community relations the positive management of the environment is used to enhance customer and community relations as well as the brand.

3.3 Risk Management Experts

Risk management experts perform key functions in an organisation. Within their own disciplines, they drive, facilitate and support the improvements in management of risk. They operate as consultants with little or no line authority. In many organisations, this work is not well separated from the auditing of the effectiveness of the controls. The result can be a conflict of interest where the same person is setting up processes and controls as well as auditing their effectiveness.

Depending on the size of the group these roles may be full-time, combined with other responsibilities or outsourced. Within their own skill areas they assist operational managers to improve awareness, create tools/processes, train and assist management to implement improvements. They are normally embedded within the businesses, as they will have expertise specific to the business or country in which they operate. Nevertheless they usually have a dotted line reporting to corporate risk management. In this way they can provide feedback and ideas to the corporate centre that may impact the Group's risk management strategy or implementation plan.

The main skill areas include:

- **Risk management processes and tools.** This includes developing processes to identify, analyse and manage business risks, preferably coherent throughout the Group, so that risk can be grouped, aggregated, etc. For specific types of risks individual tools are developed to assist with their evaluation and management. Sometimes these skills are outsourced but the processes will still need to be adapted to the organisation.
- **Change-management and training.** A major part of progressing the organisation's approach to management of business risk is overcoming the natural resistance to change. Given that they have little or no line authority, all risk experts use negotiating and selling skills to obtain buy-in from management.
- **People protection.** Health and safety experts will normally have a qualification officially recognised by the country in which they operate. Human resources professionals will be familiar with the employment practices requirements for staff in each country. Where business travel requires visiting countries that are considered to have a personal risk, companies will often use the services of a professional organisation to provide risk awareness and mitigation skills to the employee and/or his family.

- **Asset protection.** The business assets included are property, equipment, IT, intellectual property, data management, supply chain, cash, etc. These areas of expertise are often outsourced in all but the largest organisations. The same experts may well review the effectiveness of the controls as expertise in the audit department may not be adequate to make a detailed assessment of the controls in these areas.
- **Financial and treasury risks and controls.** The key risks are normally managed directly by the treasury team with outsourced expert assistance to set up the appropriate controls. As this is tied into the financial management of the company, the external auditors usually routinely audit the function.
- **Legal, secretarial, compliance.** A core of expertise for managing the legal and secretarial risks is normally found within the organisation although specific needs may be outsourced. Where there is a corporate business risk function, then compliance risk expertise may be split between secretarial and corporate risk with a close co-operation on steering and reporting.
- **Business continuity, contingency planning and disaster recovery.** As stated above, business continuity is more certain if the business risks are well managed. In some specific areas e.g. critical processes and major disasters, the creation of flexible and responsive contingency planning or disaster recovery processes need specific expertise. This is often outsourced.
- **Risk financing.** The expertise to transfer risk via insurance and other financial instruments is usually found in-house but often supported by an external broker, actuary and other specialists. The programmes may include management of in-house funds and captive insurance companies.
- **Contractual risk, mergers and acquisitions.** While contractual expertise rests with the legal department, other risk experts are frequently able to provide expertise in managing specific risks in contracts and due diligence processes.
- **Environment.** The broad concepts may be relatively simple but specific expertise is sometimes bought in where it is not available internally. The reporting lines for environmental management are often separate from other risk areas but necessitate close co-operation between experts as their work is closely related.
- **Corporate Social Responsibility.** Many organisations regard this as part of human resource management or combine it with environmental management. Policies may be interlinked with ethics, code of conduct, etc.
- **Assurance experts (risk based).** Internal audit functions have evolved in many companies but few have the breadth of skills to evaluate the effectiveness of all controls. As a consequence the experts who create and implement them may carry out the assurance of the controls. This may also be true in areas of financial control where Internal Audit is used to help create or improve them. There is consequently a danger that the independence of the auditing process is compromised.
- **Reporting and data management.** While not a specific skill to risk management, it does require powerful data management and reporting processes. More and more companies are buying specific software to manage data related to business risk assessments, insurance and claims, crisis management, etc. In some cases in-house solutions have been developed.

4. Processes and Tools

Although many business risks are generic, each business sector and organisation has its own specific risks. The concepts of management of risk are common and transferable. The following processes and tools can be found in or adapted to most businesses.

4.1 Risk Management Standards

Standards have been developed in a number of countries including Australia, Canada and the UK. They vary in content and application, the most recent and broadest being the UK produced version. (See Airmic website www.airmic.co.uk) This standard provides a framework for managing upside and downside risk and includes ISO risk definitions.

4.2 Key Process Elements

- **Risk identification** is often confined to downside or negative risk although more companies are using the process to identify and evaluate upside risks (opportunities). To assist with analysis, risks are often grouped to satisfy the specific needs of the organisation. They may include financial, strategic, operational hazard, growth, compliance, etc.
- **Risk assessment** evaluates the impact of the risk on the group. It contains two elements- magnitude and probability. Most businesses use a number of levels to define magnitude or probability. These vary according to their specific needs and may be qualitative or quantitative. The qualitative may be High, Medium, Low without hard definition while quantitative may define levels in £millions and % probability. This assessment assists in prioritising the importance of each risk and shows several levels of assessment. These are:
  - Without controls (worst case scenario)
  - With controls (with the assumption that they are effective)
  - With planned improvement completed
- **Risk tolerance** is a key part of the process that is often not formalised or clearly understood. Delegated authority is normally in place, but the company's capacity to take risk and its willingness to do so may not be clear to all staff. There may be inconsistencies between the levels of operational, strategic and insured risks.
  Where defined, risk tolerance will be a function of financial capacity, willingness to take risk, business profile, mix of mature, developing and declining businesses.
- **Control.** Groups struggle to have the right level of control to avoid stifling opportunities while ensuring that risks are maintained within accepted tolerances. The controls found within businesses are:
  - **Business Process** is a fundamental part of the internal control. The main processes to plan for and manage an organisation include strategy, business plans, budgets, business reviews, capital expenditure, project approval and management, etc. Many of these processes will have embedded sensitivity analysis and increasingly, a risk analysis. With a comprehensive evaluation of the risks, these processes are more complete and more likely to achieve their objectives.

- **Physical protection** of the group's assets will help ensure their conservation and minimise the likelihood of damage. Achieving this takes into account the design, layout, built-in redundancy, and protection of those assets. The requirements are specific to each situation but may well include specialised building construction, fire and explosion protection, separation of key processes, etc. Design is normally within the building and protection codes of the country although fire protection is increasing designed using international codes.
- Unforeseen major incidents may occur and disrupt the business even when the group's assets have been well protected and steps have been taken to mitigate other risks. **Contingency planning and disaster recovery** normally include IT risks and catastrophes. The degree of planning, preparation and testing of such processes varies between organisations.
- The organisation interacts with third parties (partners, customers, suppliers) using contracts to clarify the agreement. The risks to these relationships are identified and managed under **contractual transfer and acceptance of the risks.**
- **Risks are transferred using financial tools** where the control of risks within acceptable tolerances may not be economically feasible. If the Board does not wish to accept the residual risk after it has been managed using the above controls, then part of it may need to be transferred. External transfer is normally through traditional insurance programmes, hedging and derivative instruments. Internal instruments including funds, and captive insurance companies are commonly used in large organisations.
- The adage of "what gets reported, gets managed" holds true to risk management. Within corporate governance codes there is a requirement to **report progress.** Most organisations report on their key business risks and escalate them up through the organisation. Measuring and monitoring the results is not always very sophisticated. Where this is in place it may include measuring reduction of risk, cost, incident statistics. Near miss reporting and incident reporting may be formal or informal.

4.3 Control Assurance

A key part of the control system is the independent assurance of the effectiveness of the controls. External auditors, Audit Committees and some form of internal audit are in place in most organisations. The internal audit function is becoming increasingly focussed on the business risks and a risk-based approach to the assurance of the internal controls. However as discussed above, the independence of the assurance process is not always apparent due to the overlap of control implementation and assurance.

5. Challenges and Pitfalls

Management of business risks has always been embedded in good management of businesses. In recent years it has become more clearly identified. The techniques to manage risk have been polished and repackaged creating a number of challenges and pitfalls:

- **The role of the audit and risk committees is evolving.** Directors are becoming more clearly personally liable for the effect of the company's actions. Many audit committees restrict their review of internal controls to traditional financial areas and perhaps Health and Safety. The broader business risks and their controls may represent a larger threat to the organisation. Risk committees in some groups are similarly narrow in their scope, focussing mostly on insurable or hazard risk. Larger organisations may have developed the scope of both committees to ensure that they cover the broad spectrum of business risk in support of the group's strategy.
- This introduction to risk management highlights the key aspects of identifying and managing business risk within acceptable tolerances. An important part in the process is **the independent assurance of the effectiveness of the controls.** Some companies have combined the implementation of risk processes with the internal audit function. Others have put the "cart before the horse" by absorbing risk management into internal audit. These two functions are very different in their approach, objectives and skill sets. Their integration tends to create a lack of independent assurance, impedes the development of the risk processes, and may well not comply with developing corporate governance codes. The separation of the two functions with good working relations between them will maximise the benefits for the organisation. This will necessitate a clarification of roles in all areas of risk (see 3.3 above).
- **The risk management experts' roles** are to drive the strategy, help, facilitate and advise. Management's role is to implement. It is inevitable that the risk management function may be viewed as interfering in the management of the businesses. To be successful, the risk expert must be accepted by managers as a help and support to achieving their objectives.
- There are no easy ways of **documenting and reporting the added value of good risk management** since many of the benefits are subjective. The challenge is to develop relevant ones for the particular organisation. There is always the question "if we hadn't done that or spent that money, would our business have suffered?" Benchmarking against other organisations can demonstrate value as can documenting reduction in incidents and near misses. Consistent achievement of strategy and business plans within acceptable limits; increased but better controlled exploitation of opportunities; consistent compliance with fiscal, legal and code requirements are probably the best measures. However risk management is only a contributor to achieving these objectives.
- The increase in corporate governance requirements, while generally positive in improving management of an organisation, can create a "box-ticking" approach to risk management masking the benefits of good management. The challenge for organisations is to understand those benefits and exploit the opportunities that good practices create.

Appendix

Key Business Risks

The risk groups and specific risks highlight some of the key risks that may impact performance and are common to many businesses and organisations.

Risk Group	Risk
Strategic impacting strategy and long-term business plans of the organisation.	
	Market and customer trends
	Economy/political stability
	Competition
	Tactical decisions (investments, mergers, acquisitions and disposals)
	Achieving predicted business performance
	Major catastrophe/incident (enhance or destroy image/brand)
	Ethics, culture
	Board composition
Operational impacting day to day operations and achievement of budgets and performance targets	
	Capital expenditure
	Projects
	Treasury & Cash management
	People (Key staff, health & safety, employment practices, etc)
	Fraud/stock losses
	Accidents/incidents
	Management and motivation
	Supply chains
	Customer service/maintenance
	Natural catastrophes
	Liability for product and to third parties
Compliance risks	
	Legal, fiscal, trade, health & safety, etc