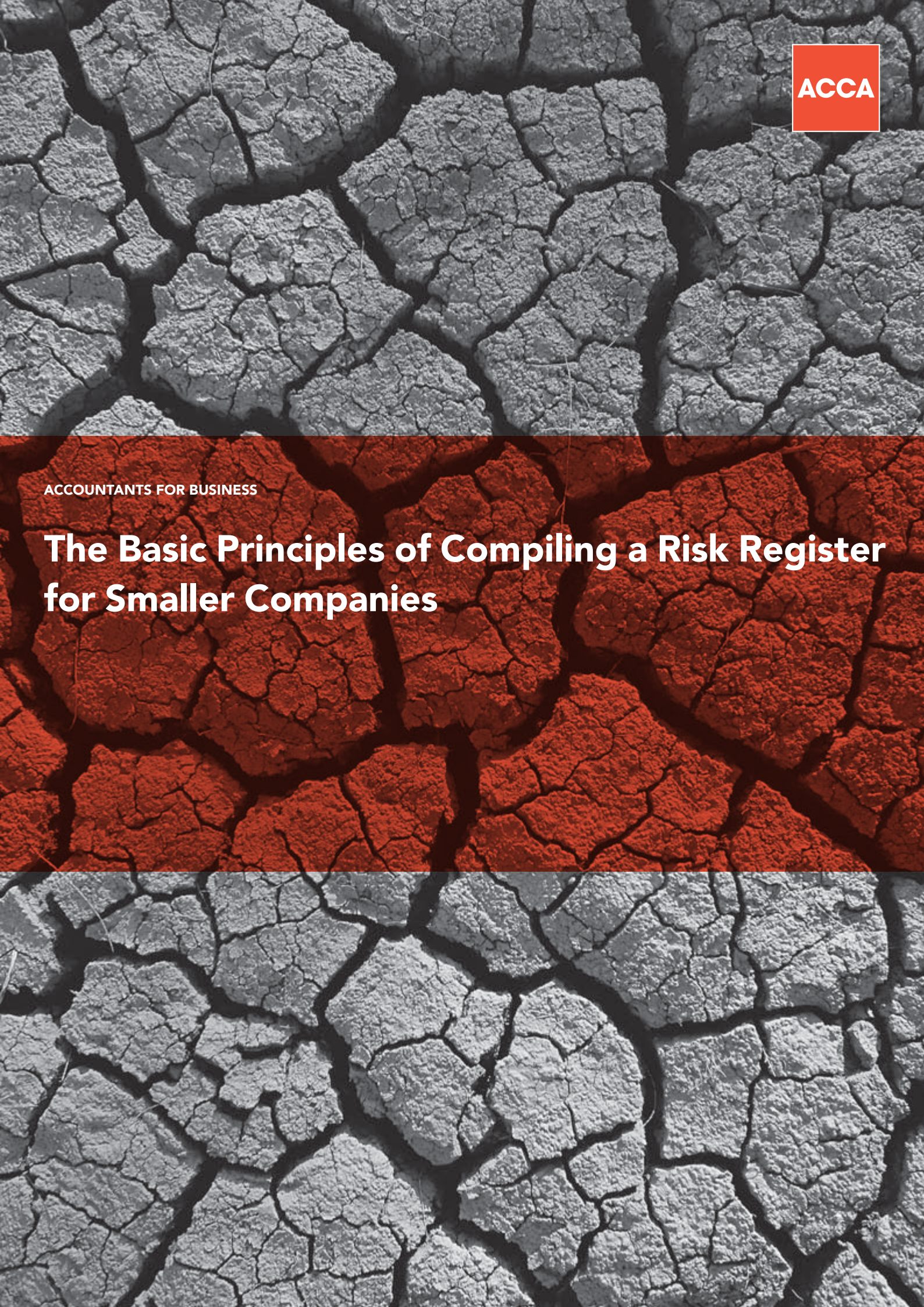

ACCOUNTANTS FOR BUSINESS

The Basic Principles of Compiling a Risk Register for Smaller Companies

ABOUT ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. We support our 131,500 members and 362,000 students throughout their careers, providing services through a network of 80 offices and centres. Our focus is on professional values, ethics, and governance, and we deliver value-added services through 50 global accountancy partnerships, working closely with multinational and small entities to promote global standards and support. We use our expertise and experience to work with governments, donor agencies and professional bodies to develop the global accountancy profession and to advance the public interest.

ABOUT THE AUTHOR

Tony Morton's experience is wide and diverse, having worked for four FTSE companies, in the UK, continental Europe, and overseas, in both head offices and within operating subsidiaries, from line functions such as works accounting and financial accounting, through a succession of management roles to finance director of five companies, two with public listing. Product areas included components for the motor and aerospace industries, sports goods, building products, defence electronics, North Sea oil support, and steel stockholding. He then spent 12 years in a large private company, where his responsibilities covered both finance and executive responsibility for a group of subsidiary companies in media, property, leisure and health. He is a non-executive director of an electronic publishing company, and is a member of both the ACCA Corporate Governance and Risk Management Committee and ACCA Financial Reporting Committee. Although the companies he has worked for have been completely different, he has found common threads in all, particularly in how to approach their financial health. He has created systems of internal control appropriately suited to the individual businesses, where identifying the risks faced is essential to that process.

CONTACT

Paul Moxey, Head of Corporate Governance and Risk Management, ACCA
paul.moxey@accaglobal.com

INTRODUCTION

This document is a simple guide to compiling a risk register for smaller companies with a functioning board. It is intended principally for the finance director or company accountant, who would often be best placed to carry out such a formal risk assessment process.

Most business managers have an instinctive understanding of the more common risks they face, and will have taken mitigating action, often without even realising it. Although this emergent, ad-hoc approach may give some practical protection against problems and disaster it can still leave a business exposed. A risk register formalises the consideration of risk, and opportunities, in a way that enables wider consideration and discussion within management or at board level. This in turn helps to ensure that all significant risks have been suitably identified, assessed and managed. A risk register can be particularly valuable to non-executive directors, and practice shows that it often throws up unexpected issues which need to be addressed. It is not, and should not be allowed to become, a bureaucratic exercise. Although a risk register tends to focus on negative risks, if used sensibly it should also address the opportunities which face the business.

Large PLCs will have dedicated staff creating, monitoring, and up-dating risk registers, and will often have complex methods of risk evaluation. Within the majority of smaller companies, creation of a risk register will be a task for the financial director or the accountant, and will be only a small part of their overall responsibilities. The purpose of this paper is to help such financial directors and their companies devise something not too onerous, but which has real value. Although many large businesses regularly update their registers, this is not practical for many smaller companies; however, an appropriate system is likely to include at least an annual review, when the risk register is presented formally to the board. An ideal time for this is either just before or during the budget process, or during a review of insurances.

Apart from the benefit to the board, many insurers now ask to see risk registers, and a well-presented document that illustrates how risks are addressed can have a positive influence on insurance premiums. Similarly a risk register can be useful as part of the documentation for a company sale, because although it may not answer all the questions a buyer may ask, it gives some useful leads, and indicates how well or badly risk has been covered in the past. It should be evidence that the company is well run.

The principles are equally worthy of consideration by owner/directors of small businesses. While the paper should be readily adaptable, their owner/directors may find it helpful to discuss the paper with their professional accountant. The accountant should be well placed to help in the preparation of a risk register and to act as a useful sounding board for considering risks. Even the world's largest companies can face serious loss of profit, reputation or even failure simply by not having contingency plans to guard against essentially foreseeable risks.

COMPILING A RISK REGISTER

The process of compiling the register will probably start off by identifying a wide variety of risks, but these should then be filtered to allow the company to concentrate on those with the greatest potential impact, so that what is presented to the board will be refined to perhaps no more than twenty key risks/opportunities. An appropriate filter is one related to the potential financial impact, perhaps being set as risks/opportunities with an impact of more than 5% of budget profit.

How a risk register is compiled will depend on the complexity of the business, but it is usually sensible to start from the ground up, either with departments, sites or business entities within the organisation. This information will be based on what is important to each one, but the documents are consolidated as they move up through the organisation and filters are applied, so that what is presented to the board will cover only those risks/opportunities which will have the filtered impact on the company as a whole. If the exercise is carried out appropriately it will, however, give management throughout the organisation the opportunity to take a formal look at the specific risks they face and how they deal with them. It is also important to emphasise that this is not a scientific exercise, and that although one attempts to quantify risks, to a great extent this is done on a subjective basis.

Even more important than putting the register together – which must, however, be done diligently – is the use to which it is put. It should not be viewed simply as another box ticked, but as something that will help management and the board to ensure that their risk policies are appropriate. It will rarely identify every risk that a business faces; for example, document shredding was quite clearly not foreseen as a risk by the accountants Arthur Andersen's following the Enron debacle, and one assumes that banks had not foreseen the drying up of wholesale funds as a secondary effect of toxic loans in the US.

UNDERTAKING A RISK ANALYSIS

A suggested format for a first risk register is shown on page 7. This can be tweaked to suit each individual organisation, but although the elements may be given different weights it reflects the general principles which will be found in all risk registers. The two elements of each risk to be assessed are Impact, should the risk occur, and Probability. On the one hand, there will be risks which could be truly catastrophic, but which are very unlikely to occur, either because of the nature of the risks themselves, or because of the mitigating strategies (Controls) in place; while on the other there will be risks with far lower potential impact, but which are much more likely to occur. The treatment of each of these will be very different. Having created a 'raw' Risk Rating the Controls against this will be considered. Having assessed Impact, Probability and Controls, the result will be an assessment of residual risk.

IDENTIFYING RISKS

A first attempt to identify risks will often be made by an appropriate senior person such as the financial director or company accountant. Following that, it is sensible to have a brainstorming session or sessions with others in the business, to tease out what risks may be relevant, to assess these, to identify what control measures may be or should be in place, and to assess whether the residual risk is likely to be acceptable or not. The process may suggest risk areas which are not adequately covered, and these will be addressed to determine what control measures might be implemented. Similarly, opportunities available to the company, which are perhaps not being fully capitalised on, will be assessed and programmes put in place to take advantage of these.

QUANTIFYING RISK

As noted above, the quantitative assessments of Impact and Probability will be largely subjective, but the very act of attempting the quantification gives others an opportunity to challenge the assessments, perhaps leading to the development of programmes which might otherwise have never been envisaged.

In the example shown on page 7, each element has been given degrees of importance from 1 to 3, whereas in practice it may be that a range of 1 to 5 is thought more appropriate. Initially the Risk Rating is assessed by calculating the product of Impact and Probability. This shows the internal measurement of importance. This number is then multiplied by an assessment of the quality of Control (which may be from internal or external factors), where a low number suggests good control and a high number poor or inadequate control. This gives a numerical assessment of residual risk, where the company can set the level with which it is happy, and at what point it is not. Any risks with a residual level in excess of this limit will require attention, although there may be nothing further that can be done; should this be the case, then the board will have to determine whether the business can actually accept the risk, or whether it should withdraw from that area of business. As noted above, potential opportunities should be assessed in a similar way, and where these have the potential to add significantly to profitability, programmes should be considered to actively harness these.

MATERIALITY

In preparing the risk analysis materiality must be considered within the individual departments and/or divisions, and finally at the company level. As already suggested, one way to set this is by using the measure of a proportion of profits, another by using a simple monetary sum. Such measurements need to be set at such a level that the risk registers presented either to the board, or to lower levels of the organisation, will not be so extensive as to make them unsuitable as a management tool. As noted earlier, for top-level control the aim should probably be to concentrate on no more than twenty risks.

TYPES OF POTENTIAL RISK

The portfolio of risks facing each business is unique to that business. Some businesses will face severe risks of a nature that are of no significance to another. For example, to a manufacturing business energy costs may be critical, whereas to an advertising agency these probably won't appear on the radar. Some potential risks to be considered, are listed here.

Business strategy

This is a very wide heading, and many specific issues are covered separately below. Perhaps the first question to be asked should be: how often is the business strategy reviewed in a formal way by the board?

Catastrophe

For example, fire or earthquake; but smaller catastrophes could also have a significant impact. For example, companies that are highly IT-dependent, or that are dependent upon online ordering, need to assess whether their power and phone connections are up to their task. (See also IT below.)

Competition

Competition covers both the market as a whole and individual players and products/services. A competitor developing a completely new product or method of serving a need could kill a traditional business. Consider the extraordinary effects that the Internet has had on so many business models. However, the effect may be limited, as it has been in retail, where it is unlikely that we will ever reach a point where everything is bought online. Just as competitors may create a potentially negative risk, outflanking the competition could be an opportunity.

Customer base

A business needs to consider whether it is over-reliant on a small number of customers, or on a particular market or business segment.

Erosion of prices

This can be caused either through market pressures, or through the pressures exerted by key customers.

Exchange rates

These can be significant to revenue, costs and to funding issues.

Fraud

Fraud can be both financially serious, and lead to reputational risk. Internally, systems and procedures should attempt to minimise fraud, with careful attention to schedules of authority (see below), and as far as possible making sure that no one individual has the ability to take actions on their own. Internal fraud can, however, be carried out by employees at the highest level in an organisation, and in assessing risk it is essential to consider what opportunities could be available to these people, even to chief executives. External fraud often requires collusion with members of staff, and an examination of transactions or contracts of a significant level of materiality should be part of the risk register process.

Funding
How secure are facilities for financing? Over-dependency on one lender may lead to trouble if they withdraw their support. Dangerous levels of gearing are also risks that need assessment. How important is additional funding to the company's future plans?

IT
This is a whole area in itself; but suffice it to note here that companies that are highly dependent on specific servers for the delivery of product, or perhaps for the retrieval of critical information need to give this area of risk a thorough analysis. For example, what critical software does the company possess, and what are the dangers connected with its support?

People
Is there a danger of loss of key staff? This can happen for a variety of reasons. Is there adequate second-line support and succession planning? Are salaries/bonuses and employee benefits appropriate? Are training programmes appropriate? Are there sickness/absence problems? Are there any 'loose canon' managers needing to be held in check?

Political risk
This is particularly relevant for international activities, but attention also needs to be paid to the increasing legislative pressures on matters such as health and safety and climate change.

Product
Is the business over-reliant on one product or product line?

Projects
These include building projects, large capital projects, major changes within the organisation, and acquisitions/ divestments. All involve unusual levels of cost and effort. It is easy to underestimate the impact of a particular project on the day-to-day running of the business.

Quality of service
The decision about what quality of service the organisation should offer will in part depend upon the product or service being provided; but the higher up the quality scale the company operates, the more serious a weakness in service can become; this can quickly lead to reputational risk (see below). Where service is outsourced to third parties, or where dealers or agents are involved it is worth looking carefully at these arrangements, to ensure that the expected standards are being met.

Raw materials, energy, services, or other 'bought-in' items
Do suppliers have a stranglehold? Is procurement spread sufficiently widely across a range of suppliers? Where a supplier is providing a key component, what happens if they fail to deliver? The example of microprocessor chips some years ago is relevant.

Regulatory, environmental, and taxation
Are there any changes afoot? In what ways may they affect the company's operations?

Reputational risk
Reputation in the market place and credibility with customers, banks and others can take years to build, but can be lost overnight. It is essential to identify where the company might be vulnerable and be prepared to deal with the unexpected. For example, who should deal with outside agencies such as the press? Who needs to be involved (eg lawyers)? In recent years both Virgin Atlantic and BA have been able to make PR capital from aircraft crashes, by concentrating on the heroic actions of their pilots. A slow response almost always indicates something sinister, and always damages reputation.

Schedules of authority
Are there adequate checks and balances, with clear limits on the authority of individuals, for example, to bind the company contractually, or to levels of spending? Operating issues also need clear lines of authority. (See also Fraud)

Technological changes
How are the company's products/services defined, and what might replace them? How might they be made or delivered differently?

CREATING A SCALE OF RISK

Turning to the example of a risk register format illustrated on page 7, the scale of risk may be as follows.

- Under Risk Impact: it may be helpful to think of 3 representing critical, 2 serious, and 1 significant. If the risk is not significant then it shouldn't be registering.
- Under Probability, 3 represents frequent (at least once/twice a year), 2 probable (within 5 years/more than once in 5 years), with 1 representing remote (not more than once in 5 years/more than 5 years away).
- Under Control Rating, 3 represents poor controls or inability to control, while 1 represents fully under control.

This can easily be turned into a five-point scale rather than a three-point one, if it is considered that a little more sensitivity can realistically be assessed. The basic format can be adjusted to suit individual circumstances, and clearly will not fit into the size of boxes shown in the example format. It is important to consider and note control measures, actions required, and to have a Control Owner. The Control Owner is at each level within the company the person who has responsibility for the risk at his/her level, but as noted below where a risk is sufficiently serious to show at a higher level within the organisation then a manager at that higher level must be shown to have responsibility.

With a three-point scoring arrangement the maximum frightening 'score' would be 27 (3 × 3 × 3), or for the five-point system 125 (5 × 5 × 5). As a suggested guide, the 'red alert' might be triggered at around 12 in a three-point scheme, or around 45 in a five-point one. It is valuable to note the risk score from the previous period, since clearly an increase in the assessment of risk may also warrant attention.

RESPONSIBILITY FOR MONITORING RISKS

Many risks will be controlled by internal monitoring or actions. Others may require hedging or insurance, accepting that they cannot be avoided. The risk register will have identified those risks where the controls are sufficient; however, simply having insurance, even if it covers interruption of business, will not cover a major disruption; customers will look elsewhere, and may well have established other sources of supply by the time the company is back in business. Disaster recovery planning is an essential part of any risk management programme. It does not necessarily require an enormous expenditure, but it does require a plan that specifies who does what, and how critical processes are dealt with after a catastrophe. There are also companies that can provide an insurance 'service' of office accommodation and IT for a reasonable premium.

As with any other management issue, clear identification of responsibilities is important. Each risk needs to be the responsibility of a specific individual for monitoring and control. At board level this should mean board members; if a risk is sufficiently serious to make it to the risk register the responsibility should not be borne by a manager below board level; although he or she may be the person most intimately involved, a board member must shoulder final responsibility.

CONCLUSION

It is hoped that this short paper will help those embarking on a risk register exercise to construct something useful, with effort commensurate with the potential benefits, in a practical and easily understood way. For anyone wishing to produce something more detailed, or where this relatively simple methodology may be considered too superficial, there are many examples which can be found on the Internet, or by reference to other companies.

If this paper does no more than help a business to recognise the potential effect of one or two risks that could be better managed, it will have achieved its aim.

RISK REGISTER

Date Modified: _____ **Created by:** _____

Risk No.	Risk	Impact	Probability	Risk Rating	Control Rating	Level of Residual Risk	Prior Year Residual Risk	Movement Year on Year	Notes	Control Measure	Further Action Required	Completion Date	Comments	Control Owner

NOTES

1. Measurements on a 1, 2, 3 scale where under impact and probability, 3 is the most serious, but where under Control Rating, 3 represents poor controls. Under Risk Impact it may be helpful to think of 3 representing critical, 2 major and 1 significant. Under probability, 3 represents frequent (more than once pa), 2 probable (within 5 years/more than once in 5 years), and 1 remote (not more than once in 5/more than 5 years away).
2. Risk Impact x Probability = Risk Rating. Risk Rating x Control Rating = Residual Risk. Residual Risk - Prior Year Residual Risk = Movement Year on Year
3. Residual Risk ratings in excess of 6 require regular Board review, and of 12 or above should lead to clear plans. Probability ratings of 3 also suggest regular review.
4. Materiality set at £xm

TECH-AFB-TRR

ACCA 29 Lincoln's Inn Fields London WC2A 3EE United Kingdom / +44 (0)20 7059 5784 / www.accaglobal.com