Guide to Risk Registers

Cardinus CEO Andy Hawkes explains how one document can be the foundation of risk management best practice throughout a company

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. This ad-hoc approach may give some practical protection against problems and disaster but it can still leave a business exposed.

The first step towards a planned professional approach to business risk management can start with one document, a risk register. 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, whose prime role is governance, and practice shows that it often throws up unexpected issues that 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 updating risk registers, and will often have complex methods of risk evaluation. Within the majority of mid-sized companies, creation of a risk register will be a task for the financial director or the accountant and will only be a modest part of their overall responsibilities. The purpose of this paper is to help these individuals and their companies devise something that's not too onerous, but which has real, long-term value.

Large businesses will regularly review and update their registers as part of a board process, this may not be practical for many mid-sized companies. However, an appropriate system is likely to include at least a quarterly review formally at board meetings or senior executive sessions. 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 and regulators now ask to see risk registers, and a well-presented document that illustrates how risks are addressed can have a positive influence on the company's reputation. 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.

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 20 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 five per cent 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 that will have the filtered impact on the company as a whole. If the exercise is carried out appropriately it will 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 although we attempt to quantify risks, to a great extent this is done on a subjective basis. It will rarely identify every risk that a business faces.

Even more important that putting the register together (which must still 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.

Below you can see a typical format for a first risk register:-

Risk ref	Risk and potential impact	Risk appetite	Risk owner	Impact	Probability	Current risk score	Current controls in place	Control owner	Review by	Review period	Due date	Overall current	Risk movement	Residual risk score	Future Actions	Expected risk score following future actions
4	Office closure – Pboro or EG	Low	AJH	Med	High	High	Dual office location, homeworker capability and Group infrastructure, combined with DR plans reduces impact	AA	BB	Monthly	Nov		None		Full business continuity and DR plan	

This can be tweaked to suit each individual organisation, but although the elements may be given different weights, it reflects the general principles that 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 that could be truly catastrophic, but 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 hand there will be risks with far lower potential impact, but that 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 that 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 that might otherwise have never been envisaged.

In the example shown below, each element has been given degrees of importance from one to three, whereas in practice it may be that a range of one to five 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.

Risk appetite

Different businesses have different appetites for risk, if you run a regulated business you will have a very low tolerance for breaches of the regulations as failure is likely to result in closure. New start-ups may have higher tolerance and, of course, different risks can have varying levels of risk appetite within an organisation. It is good to gauge the risk appetite of the board and shareholders once you have identified the risks and before you consider the controls and actions.

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 20 risks.

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

Fires or earthquakes might spring to mind 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 the 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 and data security

This is a whole area in itself but 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? What would be the impact on the business if critical client data were to be lost?

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 cannon' 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. This can extend to suppliers.

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 effect of short supply of microprocessor chips on the IT hardware sector a few years ago is a relevant example.

Regulatory, compliance, 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? Lawyers might be a good example here. 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?

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 and business continuity 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.

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.

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.

Creating a scale of risk

There are various models ranging from 10 x 10 matrices to more simple three by three versions. The basic fundamental is the likelihood versus impact matrix. Cardinus uses a five by three like this:-

	Impact		
Likelihood	**High (3)**	**Medium (2)**	**(Low (1)**
High (4) (certain)			
High (3) probable)			
Medium (2) (probable)			
Low (1) (unlikely)			

Article provided by Cardinus Risk Management