Risk management
made simple

sayer vincent
consultants and auditors

Acknowledgements

This guide was produced with help from the partners and staff at Sayer Vincent.

Introduction

Since the charity Statement of Recommended Practice ('SORP') issued in March 2000 required trustees to make a statement in their annual report concerning risk management processes, charities have been undertaking risk assessment. A basic process for identifying and ranking risks is described in **Risk Assessment Made Simple**. However, all too often this has been seen as a negative process, identifying potential problems and then considering ways of avoiding them. In most cases, senior managers and trustees build up a long list of possible risks and then rank them for likelihood and impact. The prioritised list becomes the risk register, and managers plan actions to mitigate the effects or reduce the likelihood of an event happening. While this is often an effective way of making everyone more risk-aware initially, the process often becomes stale. In addition, there are some drawbacks to conventional risk registers which are described in the box.

In fact, risk management can be a more positive process whereby organisations can not only consider the areas where they are vulnerable, but consider how they may enhance their chances of succeeding in those areas. What actions can you take to increase the probability that you will succeed with your strategy? Constructive use of risk management techniques can draw out the positive management responses available to an organisation and develop the capacity of individuals to manage risks more effectively.

Drawbacks to listing risks

- Definition of the risk – a risk can only be ranked if you have precisely defined the nature and extent of the risk, so vague descriptions are incapable of measurement
- To overcome this problem, the list of risks is often extended, as you attempt to cover the full range of possibilities
- Numbers-based ranking is misleading – people are often misled into thinking this is a scientific method and that the ranking is 'true', whereas it is really just an expression of perceptions
- One person's view of what is high risk is different to the next person's view, so you may not be talking the same language.
- This approach feeds the misapprehension that risk management is about identifying all the risks and then controlling them. In reality, it is not possible to identify all risks and risk management is not about controlling or eliminating risk.
- The actions identified to mitigate the risks do not always properly respond to the risk.
- The control or mitigation may not actually be effective or properly executed.

step 1 Decide to become a risk-enabled organisation

The Institute of Internal Auditors have described the stages of risk maturity for organisations, with risk enabled as the top level. At this level, the organisation is using risk management processes to improve performance and decision-making. Discussions about risks take place as part of the planning processes and regular performance monitoring. So risk assessment is not a separate activity but embedded in routine processes. Managers and staff understand the levels of risk they are responsible for managing and report upwards when they notice a change in the ranking of a risk or activity.

Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled
No formal approach developed for risk management	Some risks are reviewed but infrequently	Regular reviews of risks: significant new projects reviewed for risk	Process established: risk reported upwards where high net risk	Managers responsible for effectiveness of risk management

The risk management process needs to be led by the trustees and senior management team, but it needs to be clear that operational managers have their role to play and are responsible for managing risks as part of their job. It is usual to have an annual process in place for operational managers to report on how they manage risks. Note that the emphasis is on managing risk, so the process focuses on actions to control risks.

So the first step is to be clear about who is responsible for different types of risks.

Assigning responsibility for managing and reviewing risk – example

Strategic and identified risks	Strategic and uncertain risks
Deal with through the usual planning mechanisms, reporting to Audit Committee	Register and manage at Audit Committee level, reporting to every Board meeting

Operational and identified risks	Operational and uncertain
Deal through normal management – policies and procedures should cover the controls needed	Register and manage at Senior Manager level, reporting to Audit Committee

step 2 ## Clarify the types of risks to consider

The main types of risks to consider are project, strategic and operational risks. These are different and require different documentation and management.

Project risks

These are risks arising from a particular programme or project and should be managed as part of the governance for that activity, regularly reviewed and monitored. This is part of good project governance and management.

Operational risks

The majority of operational risks are internal risks and predictable, therefore you can do something to manage them. You then need to ensure that the management actions are actually implemented and are effective.

Listing the operational risks can result in very long lists of all the things you have to manage day-to-day and are often covered by procedures. It is therefore pointless and repetitive to list every risk, noting the action to control the risk as an existing procedure. It is more useful to accept that many of the operational risks are fairly obvious and are part of day-to-day management.

Strategic risks

These are likely to be the big issues such as reputational risk, or the risk that the organisation will fail to deliver on a major strategic aim. They are also likely to be external issues with high impact which you cannot control and therefore you have to consider how you will respond to them if they happen. A good risk assessment process will analyse these risks to get to the root cause and then consider appropriate management responses. It is harder to assign specific responsibility for strategic risks as they are likely to be very high impact or pervade all parts of the organisation.

Focusing on the strategic risks is more likely to achieve a greater depth of understanding of the risk *drivers*.

step 3 Establish an organisation-wide risk policy

Any risk register or statement about risk is meaningless unless there is a clear context set out in a risk policy. As an organisation, you need to have a common understanding about the activities where you wish to be risk-taking and the areas where you clearly wish to be risk averse. For example, a charity may wish to take risks with some grant-making activities, but be averse to taking risks on its investment portfolio. Trustees and managers need to establish the organisation's attitude to risk in various situations so that personal preferences may be put aside in favour of a collective view.

All organisations need to take risks, and a risk management policy should describe where the organisation wishes to take risks as well as where risk should be avoided. In fact, there are a range of responses available to an organisation and the appropriate response will depend on the nature and level of the risk and whether the concern is that it has a high impact and/or high likelihood.

Responses to risks

- You can *accept* the risk – this may be after controls have been put in place to manage some risk, leaving a residual risk which you are prepared to accept.
- You can *transfer* the risk – this is achieved when you take out insurance cover as now a third party will be liable for the full costs because you are paying a premium. This may also be achieved in some cases of outsourcing if the contract specifies the transfer of risk.
- You can develop a response plan to *mitigate* the effects of an external risk. This is appropriate in situations where you do not have control over the event (such as bad weather, or a terrorist attack) but you can plan ahead to ensure that the organisation can respond more effectively.
- You can take action to *minimise the likelihood* that adverse events will happen, that performance will fall short of expectations or that we will lose money through poor practice. This is relevant for many operational risks where the risk is internal and under our control. For example, you risk losing data, but can minimise the likelihood of this happening by having good back-up procedures.
- You can *avoid* an activity altogether if you judge the risks to be too high. For example, you can decide not to take any money from governments to avoid the risk that you will be identified as supporting government policy.

ABC Charity works with people who have been disadvantaged through limiting life chances when young. It is therefore appropriate to take risks with our charity's resources to make opportunities available to those people. We are therefore happy to take a risk with people.

We will not however, take any risks relating to the protection of young people and vulnerable adults. Full vetting procedures should always be followed for all staff and volunteers and disciplinary action follows when breaches occur. A similar policy is adopted in relation to fraud and corruption.

The charity is fortunate to hold assets in the form of property and investments, and revenues are generated from fundraising. While some risk has to be taken to achieve good returns, it would be inappropriate to risk the capital value of the assets. Therefore the risk of loss should be balanced against the expected return.

Once you have established an organisational risk policy, this can provide the context for assessing risks at all levels.

The risk policy also feeds into the investment policy and the reserves policy. Once the organisation has a better feel for the level of financial risk it is prepared to accept, it can plan for downside risk, at least to the level of setting a range for the level of reserves it should hold.

step 4 Implement operational risk management

Managers should identify and map key risk areas, with the policies, procedures and controls they have in place and map those to the framework as described below. The framework works when viewed as a portfolio – the aim is to ensure that you have a balance between different types of controls and that you are covering all the main risks. Managers then 'sign off' on their control map annually, clarifying that assurance is their responsibility.

Outline for a balanced framework of risks and controls

Aims and objectives – a clear understanding by staff and volunteers on the strategic direction of the organisation and, at an operational level, of the objectives of their department and the particular initiative they are working on.

Direct controls – traditional control activity such as reconciliations, and segregation of duties, written procedures.

Planning – converting strategic plans into workplans for departments, teams and individuals. Also that there are contingency plans in the event of certain risks crystallising, such as disaster recovery plans and fraud response plans.

Monitoring – continuously reviewing whether the actions and initiatives being undertaken are achieving the desired outputs and outcomes. Key performance indicators tracked over a period of time and external benchmarking are all ways in which the charity can measure its performance.

Accountability – ensuring that job descriptions and appraisals are consistent with plans and objectives, and that individuals are clear on their roles and responsibilities. The line management should support accountability as should the corporate governance structure through to the trustees.

Employee welfare – good morale and highly motivated staff increase the chances of successful outcomes, where disgruntled staff or poorly managed staff increase the risks to an organisation.

Training and competency framework – ensuring that staff and volunteers are competent to do the job expected of them, strongly linked to the strategic plans. This means looking at how the strategy should be implemented and what skills are needed to implement it.

Independent review – external and internal audit, regulatory inspections, accreditation with bodies such as Investors in People or quality assurance programmes, registration with Care Quality Commission and similar.

The format of the full working document for the risk and controls map is illustrated below. It may be easier to build the picture up by first thinking about existing policies, procedures and management actions. Then think about the risks that these actions manage. You may find that you have redundant procedures, or that you are spending a lot of time on actions where in fact the risk is not significant. On the other hand, you may find that you have insufficient controls in a particular area. For example, you may have excellent procedures and manuals (direct controls), but insufficient training for staff. So a good balance needs to be achieved over all eight areas of the framework.

	Management actions and controls	Risks	Notes	Effectiveness
Aims and objectives				
Planning				
Accountability				
Training and competencies				
Direct controls				
Monitoring				
Employee welfare				
Independent review				

The column for notes should be used to refer to additional actions that have been identified as a result of considering the existing controls and the risks they manage. For example, you may have contracts with suppliers in place which contributes to the controls in the area of 'accountability', but you may also have realised that there is more monitoring activity needed. The framework can be used flexibly – there is some linking and overlap between the areas. You can therefore cross-refer if necessary between them and use it as you see fit. Where you identify further actions, you should also put a timescale for the completion of the action.

'Effectiveness' is explained in the next step.

Who should complete the framework?

This exercise is aimed at middle managers who have a clear area of responsibility and therefore 'own' a set of risks and controls. The policies, procedures and actions to manage risk are their responsibility and they can work on the framework with their team. On occasion, they may find an operational risk is so significant that it needs to be escalated to higher management as a potential strategic risk. Additionally, there may be risks that need to be managed at an operational level, but pervade the whole organisation. For example, child protection procedures may be a responsibility of an operational team, but for a charity working in the field of child protection, any defect in the procedures would have strategic impact.

So for most organisations, this system of risk mapping works best if you cover all operational activities by identifying middle managers who already have the appropriate responsibilities.

step 5 Rank the effectiveness of controls and actions to manage risk

There are two aspects to effectiveness:
- How appropriate is the response in terms of managing the risk – do the actions cover and respond to the risk?
- How well have the policies, procedures and management actions been implemented?

So as well as identifying the policies, procedures and management actions that manage risks, managers also have to review how effective those actions have been over the past year. The manager is asked on the form to rank the effectiveness of the responses on a scale A–E, with A being the top score. If you have a mixed response you can mark up or down accordingly. For example, you may have a response that is 'B' in terms of its appropriateness, but it has not been implemented well enough – 'C' on the scale for the effectiveness. So you might give this an overall ranking of B– (or C+) referenced to notes to explain the further action needed and the timescale for its completion.

		Response is appropriate to risks	Effectiveness of response
A	Fully managed	The management actions and controls fully mitigate the identified risks.	The management actions are operating effectively.
B	Substantially managed	In the main, the response covers the identified risks, but there is residual risk.	Substantially effective operation of the management actions and controls with some exceptions.
C	Some management in place	Several elements of the identified risks are not covered by the response.	Some management actions and controls are not operating effectively.
D	Limited management of risks	The responses are inadequate manage the risks.	The operational effectiveness of the responses is poor, either because they have not been implemented well enough or because execution has been flawed.
E	No controls	No identified response.	No effective response.

Example of a completed framework for HR

	Management actions and controls	Risks	Notes	Effectiveness
Aims and objectives	▪ The organisation's strategy sets out our values. ▪ The annual staff conference emphasises the message.	▪ Lack of vision for the way in which people management should be handled – lack of values or unclear values. ▪ Failure to communicate how people should be managed to all managers.	Note 1	B
Planning	▪ The Head of HR is part of the team reviewing departmental plans.	▪ Failure to plan staffing resources adequately leads to under-staffing or over capacity in certain divisions.		A
Accountability	▪ Job descriptions for managers are clear that line management is part of their responsibility. ▪ Staff manual clarifies what line management entails and sets out process for e.g. performance management. ▪ HR advisors meet regularly with new managers to ensure they have enough support.	▪ Line managers fail to take responsibility for managing staff, e.g. do not carry out appraisals or follow procedures. ▪ Line managers do not access specialist support when needed. ▪ Line managers do not maintain adequate staff records, nor communicate changes to the appropriate departments. ▪ Line managers unaware of the HR support available.		A
Training and competencies	▪ HR organises an annual training day on performance management for all new managers and those needing a refresher. ▪ People management is one of the competencies required of all managers and part of their appraisal.	▪ Managers and staff fail to receive the training they need in HR policies and procedures. ▪ Managers do not have the people-management skills they need, leading to poor management of people and higher risk of grievances and employment tribunals.	Note 2	B
Direct controls	▪ Staff manual sets out all the relevant policies for employees. ▪ Manual is reviewed and updated every January. ▪ Staff are asked to confirm annually that they have read the manual. ▪ Staff manual is used in the induction of all new staff.	▪ Policies and procedures are inadequate or out of date, leading to possible non-compliance. ▪ Policies and procedures are not well communicated. ▪ Policies and procedures are not followed adequately by some areas or divisions, leading to poor practice and exposure to risks.		A

	Management actions and controls	Risks	Notes	Effectiveness
Monitoring	▪ HR collects and monitors levels of short-term and long-term sickness. ▪ HR contacts managers in departments where sickness levels appear to be high or increasing. ▪ HR undertake spot checks on departmental personnel records to ensure that these are kept up to date.	▪ Failure to collect and monitor key data such as sickness, other absence, equality andother data relating to strategic objectives. ▪ Failure to monitor training or maintain records. ▪ Failure to ensure the integrity and accuracy of data.	Note 3	B
Employee welfare	▪ Managers are required to undertake an annual appraisal, a mid-year review and occasional 1–2–1 meetings. ▪ Informal means of resolving disputes are now incorporated into the staff manual. ▪ Whistle-blowing policy and procedure in place and communicated to all staff. ▪ HR interviews all staff leaving.	▪ Low staff morale, disgruntled staff leading to possible damage to reputation, high level of grievances, disciplinary action. ▪ High staff turnover. ▪ Poorly managed exits, with associated risk of employment tribunals, damage to reputation. ▪ Failure to take adequate action to manage risks to individuals.	Note 4 Note 5	B–
Independent review	▪ Investor in People in place and independently reviewed. ▪ Annual staff survey.	▪ Lack of feedback on staff satisfaction leads to inertia or poor practice (e.g. failure to undertake staff survey for a long period). ▪ Lack of external benchmarks leads to out of date practice. ▪ Failure to keep up with good practice.		A

Notes – further actions – all responsibility of Head of HR	
	Timescale
1 The induction of new staff should incorporate the video of the last staff conference so that new staff joining understand early on what the culture is on these matters.	From Jan
2 All managers with responsibility for line managing staff should be asked to confirm annually that they have completed the training in performance management in the last two years.	From next annual round in Jan
3 At present the spot checks are annual for all departments. Introducing new system whereby a department that fails in an area of record-keeping will have a repeat visit six months later to ensure that record-keeping has improved, with the authority to escalate to Director level if not remedied.	From Jan
4 The informal dispute resolution service that HR can provide is not well known among managers and HR will launch a pro-active programme to communicate this plus offer a drop-in service to ensure that managers and staff come to discuss possible problems at an early stage.	In team plan for next year
5 Poor manager behaviour may be the cause of problems and the whistle-blowing policy should be amended to make it clear that staff can use this for concerns about bullying.	For approval next Staff Committee

step 6 Identify strategic risks

A different approach is needed for strategic risks. These are risks that:
- arise from the strategy
- are external and so outside our control
- are pervasive – in other words they cannot easily be managed by one team, but need co-ordinated action across the charity, although you may decide to ask one manager to lead the response.

You should consider strategic risks for impact. Although it is normal to rank risks for both impact and likelihood, our experience is that likelihood is difficult to assess and often subjective. When considering risks to reputation and similar risks, we are concerned with high impact risks more than any others. So the strategic risk register will consist of the high impact risks and the ones considered most important. There is then no need to assign a value to rank the risk – the emphasis is on managing risks.

The responsibility for the construction of the draft strategic risk register rests with the senior managers. Existing controls and actions to manage those risks will be identified and then further actions added where considered necessary. Although strategic risks need to be managed across the whole organisation, it is useful to identify the lead person who is responsible for developing further control actions. A suggested format for the strategic risk register is shown below.

Description of risk	
Impact	
Existing management actions	
Further management actions	**Leader**

The strategic risk register is likely to only contain a handful of risks – maybe ten, but it is not likely to be too many as these are high impact and probably external risks. The management actions are likely to be ways in which the organisation can respond to mitigate the risk, since it is unlikely that you can prevent the risk event happening. So this shifts the emphasis to developing response plans, rehearsing these.

Example of a completed strategic risk page

Description of risk

Risk that key funders will withdraw or significantly reduce funding, because they perceive that the ABC Charity is not being effective or is not undertaking activities that fit their funding priorities.

Impact

ABC Charity would have to reduce activities and potentially have to make staff redundant.

A reduction in charitable activity would have the knock-on effect of making the management and administrative overhead proportionately higher. This may make ABC Charity look expensive to potential funders. Cutting management and administration staff would reduce the charity's capacity to grow again.

Existing management actions

- Close liaison with key funders to ensure that we understand their expectations and regularly update them on our work and our impact
- Evaluation project underway to provide evidence of the effectiveness of our methodology of working with our beneficiaries

Further management actions

- Research alternative forms of funding for the services we provide as well as alternative models for charging and pricing services
- Draw up contingency plans to handle a cut in funding at various levels

Leader

Director of Business Development
Director of Finance

The strategic risk register should be regularly reviewed by senior managers and provided to the Audit Committee (or other committee as appropriate). The Audit Committee's job is to scrutinise, challenge and add to the strategic risks before this is shared with the whole trustee board. A review of the strategic risks is an integral part of developing a new strategy and continuous monitoring and planning strategy.

Conclusion

Adopting a revised approach to risk management will increase the level of understanding of risk across the whole organisation and develop the risk management capacity of all managers. Focussing on risk management rather than risk assessment will:

- Enable your organisation to develop an approach that helps you to understand the risks and opportunities you face
- Establish a pro-active approach to managing risks that recognises we cannot identify every possible risk and we cannot eliminate risk, however we can increase the organisation's capability to respond to unforeseen events
- Develop a risk policy that describes the organisation's attitude to risks and opportunities, innovation and change
- Prepare a risk register that provides senior managers and trustees with a useful tool for understanding and monitoring the strategic risks
- Provide a framework for risk management activities by departments and teams that enables them to manage, monitor and report on operational risks.

Further information

Risk assessment made simple
Free to download from www.sayervincent.co.uk

Managing Reputational Risk
By Jenny Rayner
Published by John Wiley & Sons

Intelligent Internal Control and Risk Management
By Matthew Leitch
Published by Gower

Matthew Leitch website – articles and tools for risk management
www.internalcontrolsdesign.co.uk
www.workinginuncertainty.co.uk

Institute of Internal Auditors
www.theiia.org

made simple guides

Made Simple guides are aimed at finance professionals and other managers working in charities. They cover technical areas such as tax and VAT treatments as well as information management areas and aim to provide practical guidance to busy managers and trustees in charities.

The content of guides is correct at the time of going to print, but inevitably legal changes, case law and new financial reporting standards will change. You are therefore advised to check any particular actions you plan to take with the appropriate authority before committing yourself. No responsibility is accepted by the authors for reliance placed on the content of this guide.

Other guides in the series

Risk assessment made simple

Reserves policies made simple

Trading issues made simple

Subsidiaries made simple

VAT made simple

Grants and contracts made simple

Pricing made simple

Gift aid made simple

Tax effective giving made simple

Employee and volunteer taxation made simple

Accounting software made simple

Mergers made simple

Information security management made simple

IT strategy made simple

Business cases made simple

Websites made simple

Knowledge management made simple

Selecting package software – the formal approach made simple

Selecting package software – the adaptive approach made simple

SORP made simple

Collaborative working made simple