

# Risk management

made simple



July 2015

Sayer Vincent LLP

**Chartered accountants  
and statutory auditors**

Invicta House

108–114 Golden Lane

London EC1Y 0TL

Offices in London, Bristol and Birmingham

020 7841 6360

[svinfo@sayervincent.co.uk](mailto:svinfo@sayervincent.co.uk)

[www.sayervincent.co.uk](http://www.sayervincent.co.uk)

 [@sayervincent](https://twitter.com/sayervincent)



Published by Sayer Vincent LLP

Chartered accountants and statutory auditors

Limited liability partnership registered in England and Wales  
OC390403

Copyright © Sayer Vincent

All rights reserved

No part of this publication may be reproduced by any means, or transmitted, or translated into a machine language without prior permission in writing from the publisher. Full acknowledgement of the author and source must be given.

Sayer Vincent shall not be liable for loss or damage arising out of or in connection with the use of this publication.

This is a comprehensive limitation of liability that applies to all damages of any kind, including, (without limitation), compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

[www.platform1design.com](http://www.platform1design.com)

<b>Introduction</b>	<b>5</b>
<b>Step 1</b> <i>Decide to become a risk-enabled organisation</i>	<b>6</b>
<b>Step 2</b> <i>Clarify the types of risks to consider</i>	<b>8</b>
<b>Step 3</b> <i>Establish an organisation-wide risk policy</i>	<b>9</b>
<b>Step 4</b> <i>Implement operational risk management</i>	<b>11</b>
<b>Step 5</b> <i>Rank the effectiveness of controls and actions to manage risk</i>	<b>14</b>
<b>Step 6</b> <i>Identify strategic risks</i>	<b>17</b>
<b>Conclusion</b>	<b>19</b>
<b>Further information</b>	<b>20</b>
<b>Notes</b>	<b>21</b>



## Introduction

A simple process for identifying and ranking risks is described in *Risk assessment made simple*. After a time, this can become a tick box exercise and lose its effectiveness. In addition, there are some drawbacks to listing risks which are described below.

### 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.

In fact, risk management can be focused on the strategy and used to help managers consider how they may enhance their chances of success with plans and projects. 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.

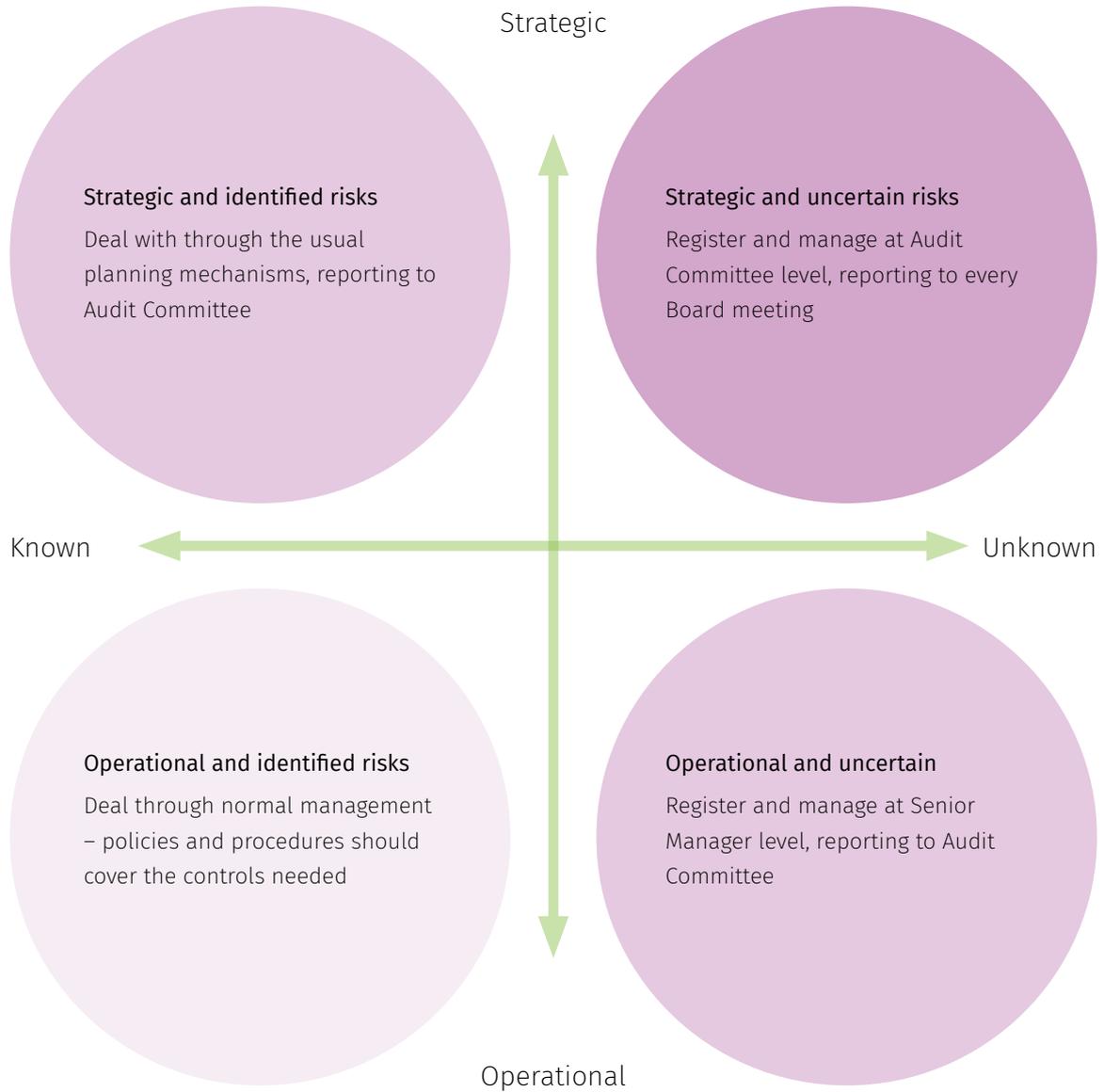
## Step 1 *Decide to become a risk-enabled organisation*

The Institute of Internal Auditors has 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 and risk assessment is not a separate activity. Trustees, 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.

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



## 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 reduce their likelihood and occurrence. 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 may fail to deliver on a major strategic aim. They are also likely to be **external** events 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, although it is possible to assign mitigating actions.

## 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 power failure) 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, for example, that performance will fall short of expectations or that we 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.

### Example risk 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, as well as other aspects of financial strategy, such as the pricing policy.

## 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, segregation of duties, authorisation at the appropriate level. Policies and procedures included in this section.

---

#### 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

Continuous review to see if 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 organisation can monitor risk and its mitigation.

---

#### Roles and responsibility

Job descriptions and appraisals should be consistent with plans and objectives, and individuals should be clear on their roles and responsibilities. Line management should support accountability, as should the corporate governance structure through to the Board.

#### Employee welfare

Strong employee engagement and a positive culture contribute to the management of risks. Staff surveys will help you to identify the strength of employee engagement. Monitor staff turnover, exit interviews and appraisals.

---

#### Training and supervision

Training to ensure that staff are competent to do the job expected of them. This means looking at how the strategy should be implemented and what skills are needed to implement it. Backed up by adequate supervision of staff.

#### Independent review

External and internal audit, regulatory inspections, accreditation with bodies such as Investors in People

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.

	What are you already doing?	What risks do those actions manage?	What further action is required?
Clear and understood aims and objectives			
Effective planning process			
Clear roles and responsibility with clear accountability			
Effective training and professional development			
Effective direct controls			
Effective monitoring			
Good staff welfare and good staff management			
Effective external review or external evaluation of what we do			

In notes below the table, you can expand on the 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 in details of the person responsible for the action and a timescale for the completion of the action.

### Who should complete the framework?

This exercise is for 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. The process works best if managers discuss their completed framework with their line manager or a group of middle managers share their frameworks to offer each other peer challenge. Larger organisations with internal audit functions can ask the internal audit team to review all completed frameworks to assure the quality of the process and ensure that all aspects of the organisation's operations have been covered.

For most organisations, this process is best undertaken annually and as part of the planning process. If additional resources are needed to manage risks, or a different approach needed, then the plans can reflect this. Personal objectives can also incorporate the additional actions to manage risk.

## Step 5 Rank the effectiveness of controls and actions to manage risk

Once you have established the framework of risks and controls, you can add the review of effectiveness of the actions to manage risk.

There are two aspects to effectiveness:

- How suitable 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 to rank the effectiveness of the actions 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.

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

This review may be undertaken by an internal auditor with the assistance of managers.

The fully completed frameworks for each team or department of the organisation will provide assurance that operational risk is being managed.

## Example of a completed framework for HR

	Management actions and controls	Risks	Notes	Effectiveness
<b>Aims and objectives</b>	<p>The organisation's strategy sets out our values</p> <p>The annual staff conference emphasises the message</p>	<p>Lack of vision for the way in which people management should be handled – lack of values or unclear values</p> <p>Failure to communicate how people should be managed to all managers</p>	<b>Note 1</b>	<b>A</b>
<b>Planning</b>	<p>The Head of HR is part of the team reviewing departmental plans</p>	<p>Failure to plan staffing resources adequately leads to under-staffing or over capacity in certain divisions</p>		<b>B</b>
<b>Roles and responsibilities</b>	<p>Job descriptions for managers are clear that line management is part of their responsibility</p> <p>Staff manual clarifies what line management entails and sets out process for e.g. performance management</p> <p>HR advisors meet regularly with new managers to ensure they have enough support</p>	<p>Line managers fail to take responsibility for managing staff, e.g. do not carry out appraisals or follow procedures</p> <p>Line managers do not access specialist support when needed</p> <p>Line managers do not maintain adequate staff records, nor communicate changes to the appropriate departments</p> <p>Line managers unaware of the HR support available</p>		<b>B</b>
<b>Training and competencies</b>	<p>HR organises an annual training day on performance management for all new managers and those needing a refresher</p> <p>People management is one of the competencies required of all managers and part of their appraisal</p>	<p>Managers and staff fail to receive the training they need in HR policies and procedures</p> <p>Managers do not have the people-management skills they need, leading to poor management of people and higher risk of grievances and employment tribunals</p>	<b>Note 2</b>	<b>B</b>
<b>Direct controls</b>	<p>Staff manual sets out all the relevant policies for employees</p> <p>Manual is reviewed and updated every January</p> <p>Staff are asked to confirm annually that they have read the manual</p> <p>Staff manual is used in the induction of all new staff</p>	<p>Policies and procedures are inadequate or out of date, leading to possible non-compliance</p> <p>Policies and procedures are not well communicated</p> <p>Policies and procedures are not followed adequately by some areas or divisions, leading to poor practice and exposure to risks</p>		<b>A</b>
<b>Monitoring</b>	<p>HR collects and monitors levels of short-term and long-term sickness</p> <p>HR contacts managers in departments where sickness levels appear to be high or increasing</p> <p>HR undertake spot checks on departmental personnel records to ensure that these are kept up to date</p>	<p>Failure to collect and monitor key data such as sickness, other absence, equality and other data relating to strategic objectives</p> <p>Failure to monitor training or maintain records</p> <p>Failure to ensure the integrity and accuracy of data</p>	<b>Note 3</b>	<b>B</b>

<b>Employee welfare</b>	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	<b>Note 4</b> <b>Note 5</b>	<b>B-</b>
<b>Independent review</b>	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		<b>A</b>

## Notes – further actions – all responsibility of Head of HR

		<b>Timescale</b>
<b>1</b>	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
<b>2</b>	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
<b>3</b>	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
<b>4</b>	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
<b>5</b>	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 on actions to manage the risk.

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.

<b>Description of risk</b>	
<b>Impact</b>	
<b>Existing management actions</b>	
<b>Further management actions</b>	<b>Leader</b>

The strategic risk register should only contain a handful of risks – no more than ten. As these are high impact and probably external risks, there will not be many. The management actions are 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. These are common for areas such as business continuity.

## Example of a completed strategic risk page

<p><b>Description of risk</b></p> <p>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.</p>	
<p><b>Impact</b></p> <p>ABC Charity would have to reduce activities and potentially have to make staff redundant.</p> <p>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.</p>	
<p><b>Existing management actions</b></p> <p>Close liaison with key funders to ensure that we understand their expectations and regularly update them on our work and our impact.</p> <p>Evaluation project underway to provide evidence of the effectiveness of our methodology of working with our beneficiaries.</p>	
<p><b>Further management actions</b></p> <p>Research alternative forms of funding for the services we provide as well as alternative models for charging and pricing services.</p> <p>Draw up contingency plans to handle a cut in funding at various levels.</p>	<p><b>Leader</b></p> <p>Director of Business Development</p> <p>Director of Finance</p>

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

### Charity Commission

#### How to manage risks in your charity

[www.gov.uk/how-to-manage-risks-in-your-charity](http://www.gov.uk/how-to-manage-risks-in-your-charity)

#### Charities and risk management (CC26)

[www.gov.uk/government/publications/charities-and-risk-management-cc26](http://www.gov.uk/government/publications/charities-and-risk-management-cc26)

### NCVO – KnowHow NonProfit

#### Risk Assessment Toolkit

[knowhownonprofit.org/studyzone/how-to-carry-out-a-risk-assessment-1?gclid=CN\\_sjOPJlbYCFW\\_KtAodZBQAmA](http://knowhownonprofit.org/studyzone/how-to-carry-out-a-risk-assessment-1?gclid=CN_sjOPJlbYCFW_KtAodZBQAmA)

### The Institute of Risk Management

#### Various guidance in their knowledge and resources section

[www.theirm.org](http://www.theirm.org)

#### *Managing Reputational Risk*

By Jenny Rayner

Published by John Wiley & Sons

#### *Intelligent Internal Control and Risk*

#### *Management*

By Matthew Leitch

Published by Gower

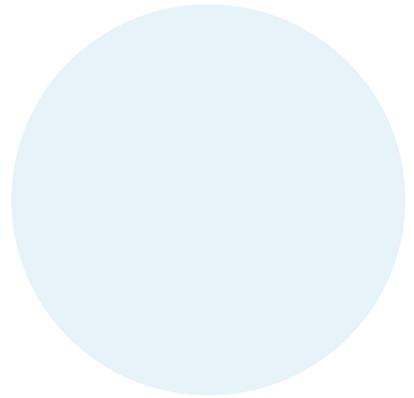
*Matthew Leitch website – articles and tools for risk management*

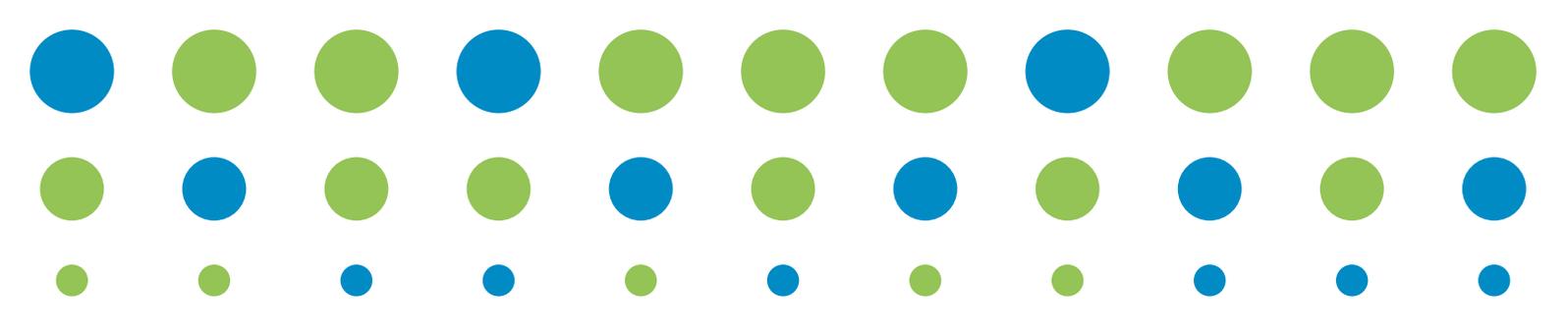
[www.internalcontrolsdesign.co.uk](http://www.internalcontrolsdesign.co.uk)

[www.workinginuncertainty.co.uk](http://www.workinginuncertainty.co.uk)

# Notes







## 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.



## Made to measure

Sayer Vincent is a firm of chartered accountants working solely with charities and social enterprises. Through tailored audit and advice services, we provide trustees and managers with the assurance that their charity is managing its resources effectively.

As well as being commercial accountants, Sayer Vincent people have an in-depth knowledge of the governance and management of charities and social enterprises. We can advise on a range of business activities to achieve the best financial outcomes, keeping in mind the context of your organisation's objectives.

Working with Sayer Vincent, you will feel that you have extra people on your team.

For more information, go to [www.sayervincent.co.uk](http://www.sayervincent.co.uk)



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.