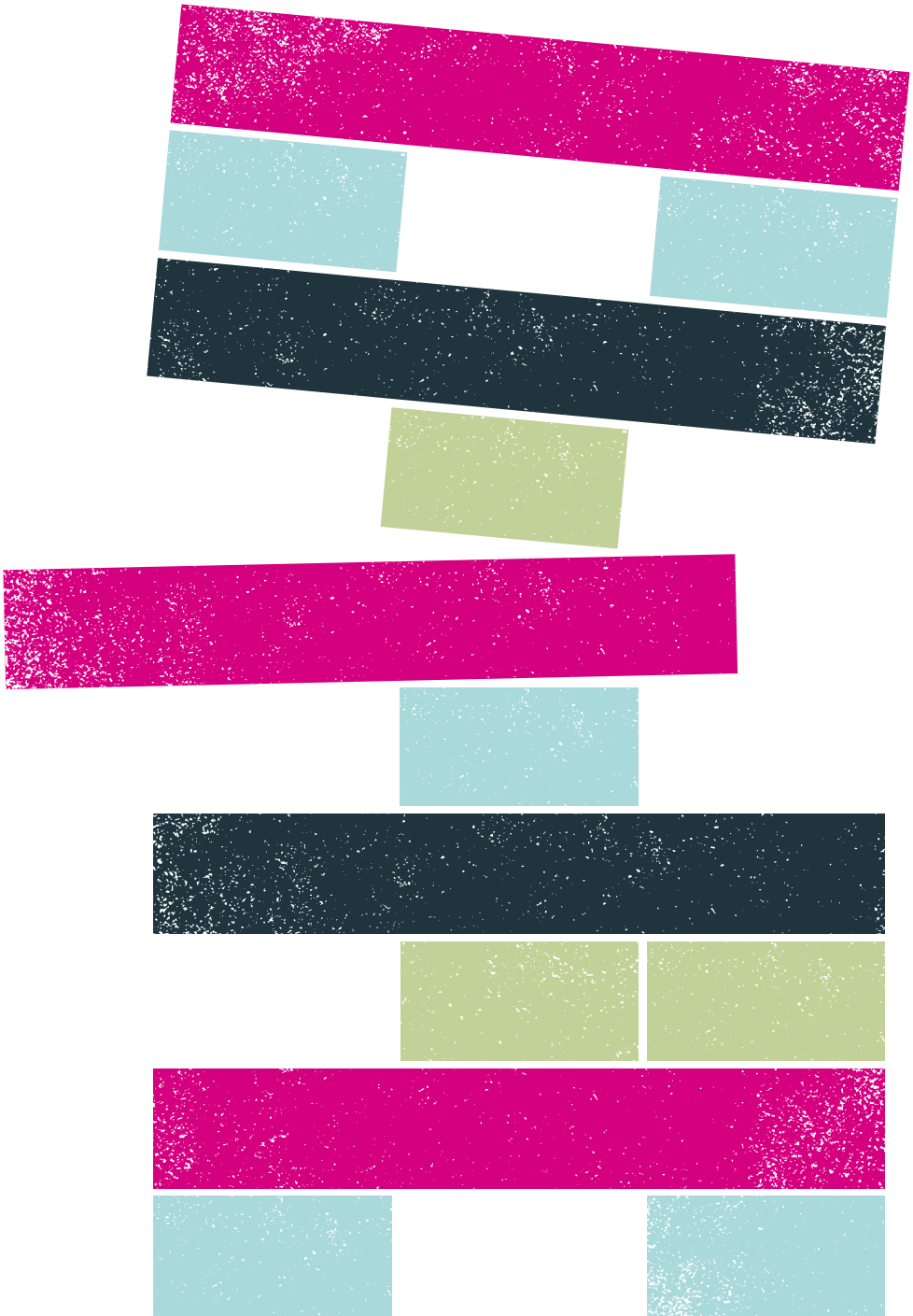
CFG INSPIRING FINANCIAL LEADERSHIP

SAYER | VINCENT

Rethinking Risk

Beyond the tick box



Published by Charity Finance Group and Sayer Vincent LLP

First published 2016

Designed by Steers McGillan Eves

Contents

Foreword

In my experience, many charities don't properly consider the risks their organisations are facing. Perhaps they don't know where to start, haven't the time, or don't think it's sufficiently important.

Others will take the approach whereby managing it has become a meaningless tick box exercise. In this instance, trustees or senior management will often put together a risk register of all risks that might befall the organisation, and perhaps jot down what they could do to mitigate these. Unfortunately, this approach doesn't manage risks, it merely identifies them – and such an approach can rapidly become tiresome or feel like a waste of time to those involved.

Charities continue to be challenged by a wide range of risks that can affect all areas of their organisation. From the risk of being subject to fraud and cyber-crime to strategic risks related to the wider operating environment, there are numerous threats that charities must be able to manage and plan for.

"How can charities of all sizes navigate the challenge of balancing risk and opportunity?"

That said, being overly risk-averse isn't helpful either: where on the one hand there are negative risks, on the other hand there are also opportunities that charities must be able to identify. An organisation's approach to risk must also encompass risk taking – where are you prepared to take risks in order to innovate and grasp opportunities?

How can charities of all sizes navigate the challenge of balancing risk and opportunity? This guide is a good place to start.

It outlines new and emerging ways that charities can categorise risks in a way that is helpful, and practical ways that charities can implement them effectively – there are methods that are easy to adopt that can prevent you from falling into a tick boxing exercise. The guide outlines steps to follow to avoid becoming complacent when adopting a formal risk management process across an organisation, and guidance on how trustees and senior managers can develop a clear mechanism for getting assurance on the management of risks.

We are very grateful to the charities that gave their time and knowledge for the case studies throughout this guide – we hope that hearing about the experiences of others will help to bring the issue to life. CFG also hold an annual Risk Conference, and at the November 2015 conference, we asked several of the attendees to fill in a short survey about what they were doing to manage risk. Some of their responses, dotted throughout the guide, will also help to shed light on the different approaches used and what has worked well (or not) in other charities.

It's vital that charities rethink their approach to risk. Doing so can help you to shore up your reputation, take risks in order to grasp opportunities, and be alert and responsive to wider strategic risks.

Everything that we do as charities involves risk. All of us, trustees and staff, have a duty to meet the challenge of those risks and do our best to manage them, in the interests of our beneficiaries. We hope that this guide provides a useful starting point, and subsequent steps to follow, to enable you to rethink your approach to risk.

Ian Theodoreson
Chair, Charity Finance Group

Introduction

Risk management is not new – it has long been a requirement of the charity Statement of Recommended Practice (SORP) for charities to state how they identify, assess and mitigate risks.

Over the last couple of decades we have seen the introduction in the commercial world of various codes and standards on risk including the Cadbury code and Enterprise Risk Management – providing much more comprehensive risk management in listed public companies. This made us all realise that risk was not just a topic for the finance people and that risk management needed to embrace all the operations of a company, not just reflect the internal financial controls.

Since then the topic of risk management has moved on considerably further. Most organisations including charities would rank risks to their reputation as the ones that will have the most impact. As we have seen in events affecting well-known charities, significant damage to your reputation can cause an organisation to close its doors or at least to suffer a drop in income.

Building up positive perceptions of your organisation is just as important as having a PR response plan. And much of what makes up positive perceptions is tied up in the day-to-day transactions your beneficiaries, customers, funders and donors have with your organisation. So reputation permeates every aspect of organisational life just as culture does. Through this guide, we refer to the need for the right culture. The attitude and behaviour of your people will determine your risk profile and your exposure to risk. Getting risk culture right is a 'no-brainer' and yet it is rarely on the board agenda.

Typically, risk management is seen as the production of long lists of risks which are meant to be the complete set of all the risks an organisation might face. This is impossible. No risk register is ever complete as we cannot predict the future. It would be better to ask whether the risk register reflects the appropriate level of risk-taking the organisation wishes to engage in. Context is everything in risk management. If your organisation's purpose requires you to take risks, but you have a culture that is risk averse – you have a problem.

Risk registers are limited in their scope, but they can help to communicate a complex picture of risk-taking and risk mitigation. More importantly, however, you need to obtain assurance that important risks are actually being managed effectively. The ideas presented in this publication use existing management tools, actions and reports to help the board to see how and where risk is already being managed. Integrating risk management into everyday organisational life makes sense – it's what we are already doing.

"You need to obtain assurance that important risks are actually being managed effectively."

All risks are not the same

This sounds obvious, but risk management processes do not always categorise risks in a way that is helpful. Typically, a risk identification exercise will look at categories such as governance, compliance, IT and so on. This may have been helpful as a way to develop a list of risks the organisation should think about, but it does not necessarily help to develop appropriate responses. In addition, categories such as governance and reputation cut across all areas of activity and they are an element to consider in every area.

Instead, it is helpful to focus on three broad categories of risk:

- Project risks
- Operational risks
- Strategic risks

Thinking in these broad categories of risk, we can then develop appropriate ways of responding to risks and managing them. And we can ensure that the responsibility for managing risk is appropriately allocated within the organisation.

Project risks
These are risks arising from a particular programme or project and are managed as part of the governance and oversight for that activity. This is essentially the operation of sound project management techniques.

Operational risks
These are the day-to-day risks that are managed.

Strategic risks
These are the big game-changing risks that influence the achievement of a charity's strategic aims. They might be major internal risks such as financial sustainability or compliance risks. Or they may be external events with high impact which you cannot control and which you therefore need to develop response mechanisms for.

Six ways of responding to risks and managing risks

Once we have identified risks and we are thinking about what we can do about them, we generally have six options:

1. Accept the risk and just monitor it to ensure we have not miscalculated and that we notice if the risk changes
2. Avoid the risk by stopping the activity
3. Transfer the risk by taking out insurance cover or contracting out an aspect of the activity
4. Develop response plans to mitigate the effects of an adverse risk event, or to take advantage of an unplanned opportunity
5. Reduce the likelihood of an adverse risk event by putting controls in place
6. Take management action to increase the chances of success

So let's take a look at how these six possible responses can interact with different types of risk. Remember, the purpose here is to manage a risk effectively, but we can also introduce another aspect – we want to manage risks efficiently as well. We do not want to over-manage a risk as this is wasting time and money. But we do not want to respond inappropriately as this is both ineffective and a waste of resources.

An underlying purpose to ranking risks for probability and impact is to prioritise risks for action and resources. We return to the topic of ranking risks later when we discuss risk registers, but we note here that it should be undertaken to help us identify an appropriate and proportionate response.

Case study – Amnesty International UK

Amnesty has now moved towards focusing on strategic risks as well as operational risk. They have looked at six strategic risks and analysed them in more detail to ensure they are linked with assurance processes.

Primarily, Amnesty didn't want to spend a long time working on risk-based calculations that weren't meaningful, or didn't fully explain the importance of mitigating the risk. Their focus is on mitigating risks, not just identifying them. The new approach puts more emphasis on the assurance processes.

One example of how this worked in practice was with regard to financial risk, where it was found that Amnesty weren't investing enough in sustaining their income stream through donations. Amnesty had to look at the quality of its fundraising strategy and how it fit into the current climate about values, regulation etc.

Throughout the risk and assurance process, Amnesty identified actions and who was responsible for mitigation, and what the current status was. Each of the six strategic risks identified were evaluated by their current level of assurance using a traffic light scale. Both boards (company and charity) now consider the risk register at every meeting and are supported by the finance subcommittee in doing so.

Project risk

Let's say, for example, that you are introducing a new database and you have set up a team to manage the whole project. The team has produced a risk assessment as part of their project management documentation and they have identified a number of risks including the three core risks that are present in every project:

- Project does not deliver the benefits identified in the business case
- Project is delivered late
- Project goes over budget

The options available in terms of managing these risks are:

1) Acceptance – this may be valid if the organisation is relaxed about these risks or the project is not going to have a major impact on other activities.

2) Avoid – if it seems highly likely that the risks would crystallise and the consequences of the project risks are so major or might have a major impact on other activities.

3) Transfer – contract someone else to undertake this project, building in the requirements for particular benefits, a timeline and a fixed budget. This will probably add to the costs as a contractor will price in the risk.

4) Response plans – the team could come up with contingency plans so they know what they would do in the event of some high impact events occurring.

5) Controls – the team could identify how they can reduce the likelihood of some risk events by looking at the root causes and putting controls in place.

6) Management actions – the team could identify the crucial points in the project where progress will be impeded, costs could escalate or quality compromised. The project plan could then ensure that project reviews are scheduled at these points. Additionally, a quality assurance manager could be appointed to work alongside the project team, helping them to ensure the project stays on track.

Typically in risk management, the focus has been options 4 and 5, particularly controls. But a focus on preventing risk events happening misses chances to manage risk in many other ways. Additionally, if the risks are not high or the organisation is happy to accept them anyway, then resources expended on managing the risks are wasted. Option 3 dramatically reduces the uncertainty and is an attractive option even if the costs are higher as for some organisations; it is uncertainty that is the key problem. Option 6 really helps the organisation to focus on improving their chances of success. This changes attitudes to project risk as well, as risks become ways of identifying where additional help might be needed. Project teams need to be open about the risks they are encountering rather than clamming up.

“Project teams need to be open about the risks they are encountering rather than clamming up.”

Operational risk

Operational risk covers a wide range of activities, from delivering the main activities of the organisation to all the core management functions. In fact, risk is not the right term in many cases, as we are often thinking here of predictable consequences of failures to follow procedures or manage aspects of the operations properly. These are not really risks in the sense of an uncertain or unknown future. Usually we are focussing on internal risks which should be areas under our control. So we are often focusing on areas where there is a high probability of the risk event happening, or indeed that we know it is happening. In considering the options open to us:

1. Accept	This is an option if the consequences of the risk are not significant (so it should probably not be considered a risk at all)
2. Avoid	This is not always feasible if the activity is core
3. Transfer	You can insure some operational risks and you can also contract out aspects of the service
4. Mitigate	Some operational risks may be out of your control, so you do have to consider contingency plans e.g. business continuity plans
5. Control	This is the most likely option for most operational controls – you need to put checks in place to ensure that your procedures are sufficiently robust and actually implemented
6. Management action	This may be appropriate if you have introduced new activities or changed how you work – the procedures may no longer be appropriate and management need to intervene

Illustration

You have conducted the risk assessment for the HR function of the organisation and you have identified the following problems:

- Failure to check references of new employees before they start work
- Lack of written appraisal notes on some employees
- Exit interviews not conducted by an impartial person in all cases
- Training records not maintained as required by your registration body
- No one has the expertise to update the employment contracts

For the first four of these points, the appropriate response will be to strengthen the controls in place. A re-design of controls and training may be necessary – if the old controls are not working, then a refresh may be needed. For example, it may be possible now to introduce an electronic recording system for these points, which will make it easier for someone to monitor compliance. This is option 6 – management action.

Although the final point could be covered by training, it is probably more effective to buy in this expertise, so the response is to 'transfer'.

In conclusion, identifying that a risk is an operational risk means that you can focus attention on appropriate responses, which are likely to be controls and management action, and occasionally transfer by outsourcing or insurance.

Strategic risks

Strategic risks are likely to be those that are external risks which you cannot control, such as a change in government policy. They may also be risks that are inherent in your business model, such as loss of funding. Sometimes an operational area is subject to significant problems and the risk profile has to be elevated to a strategic risk. For example, you have identified that the IT team is under-resourced and this risks the proper maintenance of back-ups and some IT security matters.

For these risks, you have already identified that they are important so you cannot accept or ignore them. You are unlikely to be able to avoid them as they are either inherent or outside your control. This also means that you are unlikely to be able to control the probability of the occurrence of these risk events, so introducing more controls is not relevant.

For risks that are outside your control, you should plan to mitigate the effects of the risk event, so the emphasis is on developing response plans. And for risks arising from the strategy and inherent in the business model, you need to consider appropriate management action.

In later sections, we do consider other risk responses such as changing the business model. We also explore strategic risk management in greater detail.

“Strategic risks are likely to be those that are external risks which you cannot control.”

Case Study: The Challenge Network

The Challenge Network (TCN) had grown rapidly. This growth, combined with the organisation's high profile in the National Citizenship Service programme, prompted a reassessment of their approach to risk management. In the past, their approach had been to consider risks individually and try to subjectively quantify them in terms of likelihood and impact. This inevitably led to risks being considered individually and ranked by order of perceived importance. There was no differentiation of the type of risk.

TCN has now split risks into strategic risks and operational risks. Strategic risks are more likely to be externally influenced, outside the organisation's control, but with a potentially high impact. These strategic risks are the focus of senior managers. Operational risks are more likely to be internal, within the organisation's control and with a higher level of probability, and are considered in the first instance by middle managers, although ultimately senior managers are responsible.

Managers are encouraged to look at a framework of risks and controls. This covers:

- Being clear about the mission, aims and objectives of the charity;
- Ensuring plans are in place for staff to follow, supported by contingency plans for when things may go wrong;
- Being clear about who is accountable for what;
- Making sure staff are properly trained in all respects to include risk management;
- Using good policies and procedures to control;
- Establishing and monitoring KPI's;
- Maintaining staff motivation and morale;
- Independently reviewing progress; and
- Maintaining the agility and dynamism of the organisation and not becoming over-burdened by bureaucracy and process.

Through this framework, managers aim to mitigate risks and identify areas of weakness. They then consider what further interventions can be introduced across their area (and the organisation more widely) to reduce the likelihood and/or impact of such risks. These are detailed in action plans identifying who is responsible for the actions and when they will be completed. A Legal and Compliance team then work with managers to ensure they have achieved their improvements and identify any subsequent risks. This overall consideration means that all areas of risk in an area are considered, rather than focussing on just higher ranking risks.

Governance of risk

While we mostly talk about the management of risk, it is helpful to differentiate and consider how risk should be managed at different levels within an organisation.

Who should be responsible for risk?

The board of any organisation – corporate sector, public sector or charity sector has ultimate responsibility for the effective management of risk.

The Charity Commission in its risk management guidance (CC26) is very clear. It says:

'Charity trustees should regularly review and assess the risks faced by their charity in all areas of its work and plan for the management of those risks.'

This is not a task that can be delegated to a committee as the full board needs to have a proper understanding of the key risks their organisation faces. This is fundamental to the proper fulfilment of their role as directors or trustees.

In the corporate sector, a board's oversight of risk can be led by the key executive directors – the CEO and CFO with day-to-day involvement and insights of the business. For a charity board, consisting of unpaid volunteers meeting often no more than four times a year, this is a hugely challenging role to fulfil. So in reality, large and mid-sized charities rely on managers to report risk matters to the board, and to manage the risks associated with implementing the strategic plan and delivering services. Consequently, it is important to establish appropriate levels of governance and risk management processes throughout the organisation.

"The board of any organisation has ultimate responsibility for the effective management of risk."

Our survey said…

Sayer Vincent and CFG carried out a small survey of attendees at CFG's Risk Conference in November 2015. Here are some of the answers received on how they managed risk in their organisation:

- *"A few key people control what happens"*
- *"We have a risk register, developed for the last two years. Discussed by Board annually and by Finance Committee at every meeting – usually quarterly. Also forms part of Senior Management Team meetings so created initially bottom up but with involvement from Board and Finance Committee."*
- *"Not really managed. Register etc. produced to comply with audit and year-end requirements. Controlled by directors/Trustees."*
- *"Through discussions at Board Level with Executive staff."*
- *"Executive team regularly (monthly) discuss risk: A risk 'matrix' visually communicates risk, supported by a detailed risk register. Number of risks is kept low by keeping them strategic. Trustees/Board are provided with a risk report from the executives at each meeting. Risk process and tools are audited (by external auditors) every two years."*

Governance by the Trustees or Directors

Trustees need to have a clear understanding of the risks facing their organisation and their organisation's strategy for responding to these risks. Trustees have a responsibility to collectively manage risks and work with their boards. It is important to communicate this responsibility to new Trustees when they are inducted into your organisation.

At the governance level, trustees need to grasp the major risk issues:

- The risk inherent in the business model is understood and the implications lead to appropriate risk mitigation actions, e.g. appropriate reserves policy;
- The trustees need to set the risk policy for the organisation (see below);
- They are responsible for ensuring that the organisation has appropriate risk management processes in place for the identification, assessment and management of all risks;
- It is likely that large and mid-sized organisations will set up an audit committee or an audit and risk committee to help with these governance functions.

The overall structure for the governance of risk is shown in the following table, and key aspects covered in greater detail in later sections of this publication.

Board
Understand risks inherent in business model
Ensure that resourcing and reserves policies fit model
Set the risk policy
Approve the risk management processes

Audit committee
Oversee the risk management process
Receive and interrogate risk reports, flagging major changes
Consider how the board can obtain assurance that risks are being managed effectively

Senior managers
Identify strategic risks and mitigating actions
Lead mitigating actions
Report to the audit committee and board on how strategic risks are being managed
Ensure that appropriate management of operational and project risk is in place

Case Study – Revolving Doors

Revolving Doors is a charity that operates more like a small business than like a complicated, large company. Trustees take the time to get alongside staff so they understand some of the business drivers and risks, and have a trusting and open relationship with staff which encourages frank discussions.

A key part of the approach to risk management is having a diverse set of skills and experience on the board, and Trustees with enquiring minds. Each board meeting discusses risks in a formal way initially, presented by the management team, but then have a free-ranging discussion.

Scoring risks or risk appetite are not central to the discussion, greater focus is given to understanding the actual risk and mitigation actions and resources needed. This can then be used to influence strategy or implementation of a course of action.

As an example, Revolving Doors spent a large amount of time preparing its commercial strategy; one of the biggest risks was the charity drifting away from its charitable purposes and aims. So trustees and senior managers spent a lot of time looking at this issue, and developed an ethical policy as a response.

What's important to your organisation?

A key aspect of the governance role is setting the risk policy or risk appetite for the organisation. This is about setting the tone from the top. In the words of the Charity Commission:

"Trustees need to let their managers know the boundaries and limits set by their risk policies to make sure there is a clear understanding of the risks that can and cannot be accepted."

Charity Commission guidance CC26, p.12

These boundaries will be determined by a number of different factors – including the nature of the charity's work and the capacity of the organisation. For example, a children's charity will have a zero tolerance approach to risks on issues around child safeguarding. But the same charity – particularly if its reserves levels gives it the financial capacity – may be prepared to be much more risk-taking when it comes to taking on new contracts and supporting more children in need.

This risk policy gives the management team the confidence that, to the levels delegated to them by the board, they will be able to make decisions on a daily basis that will be consistent with what the board of trustees considers to be important to the charity.

The 'Big Five' Risks and risk management processes

Risk management has traditionally been undertaken by identifying as many risks as possible and then applying an impact/likelihood scoring matrix. This may be undertaken at team, department and then board level. The resulting risk register will be extensive and so the board typically focuses on the top ten highest scoring risks. In practice, however, this leads to much debate and discussion on the scoring methodology and distracts attention away from how the risks are actually being managed.

To achieve better governance of the key strategic risks, many boards accept that there will be a set of headline risks (usually five, but up to six) which will always be key for their organisation. And it is likely that these are similar across many organisations. This does away with the need for subjective scoring methods and an arbitrary cut-off for risks that get board focus (it will always be the eleventh risk that comes back to bite you!). It also saves much time and debate at board meetings.

Headline risks

1. Impact	Are you making the desired impact in support of your beneficiaries and can you evidence it?
2. Financial sustainability	Are you managing the finances to ensure you continue to make an impact in the medium to long term?
3. Compliance	Are you meeting your regulatory, legal and donor compliance requirements and expectations?
4. Reputation	Are you able to respond effectively to any incident that could result in damage to your reputation?
5. Specific to the charity	Specific to the nature of the charity and may be a risk that is at the heart of what the charity stands for. For example, for a children's charity it might be child protection.

Later in this publication we look at how the board can obtain assurance on the Big Five strategic risks.

Boards then also need to consider ways to obtain reports on how operational risk is being managed. We look at this in greater detail in a separate section.

Case Study – Christian Aid

Christian Aid has made a number of changes to its approach on risk management. One of these has been splitting the finance and audit committee into two parts – an audit and risk committee and a finance, fundraising and investment committee. This is to ensure that senior leaders and trustees have enough time to look more deeply at risks and consider other issues that may impact the organisation, such as regulatory changes.

Christian Aid has also sought to embed risk at key meetings, for example, the oversight committee that looks at large contracts and grants. All such contracts and grants now have their own risk register attached to them so that the risks are better understood and managed.

The Director of Strategy and People Management has also introduced a new model to support thinking about risk: the 'Three Horizons Model'. This involves thinking about what the future might hold for the charity sector, for the world and for Christian Aid. Horizon 1 (H1) is 'business as usual', and the operating environment as it is currently constructed. It also considers what innovations the organisation may pursue to 'disrupt' this system. Horizon 2 (H2) considers the impact of these disruptions and what they mean for the organisation, alongside the balance between protecting the core business and investing in new approaches. Finally, Horizon 3 (H3) looks at the long term successor to the current business model. It is the culmination of all the previous innovations and is a sketch of what the future business model of the organisation may be. This has involved engaging with the board and thinking about what needs to be done in the short-term, what a change in thinking may be, and what change needs to happen.

The Corporate Risk Register focuses on H1 risks, being those that are the most predictable. However consideration of H3 has opened up discussions on a range of longer term risk opportunities and strategies that continue to be tracked. The quality of the conversation and discussion on risk continues to be a key part of its active management.

To see the 3 horizons model, refer to 'Seeing in Multiple Horizons: Connecting Futures to Strategy' by Andrew Curry and Anthony Hodgson.

Reporting on risk

All charities have to produce an annual report to accompany their financial statements. The requirements are simplified for small charities, but for larger charities subject to audit the Statement of Recommended Practice (SORP) sets out how trustees should report on risk in their report.

The SORP was updated in 2014 for implementation for accounting periods commencing 1 January 2015. The current version of the SORP increased the reporting requirements for risk matters. It states that the report should contain within the financial review:

"A description of the principal risks and uncertainties facing the charity and its subsidiary undertakings, as identified by the charity trustees, together with a summary of their plans and strategies for managing those risks".

Para 1.46 of Charities Statement of Recommended Practice (FRS 102)

Previously, trustees were obliged to confirm only that they had identified, assessed and considered mitigating actions.

The new version of the SORP echoes requirements for larger companies. The expectation is that a small number of strategic risks will be reported in the trustees' annual report. The approach outlined above for strategic risks can be adapted to the formal report now required.

An example of a SORP compliant risk statement

Principal risks and uncertainties
This example charity has a detailed risk register, which is reviewed every three months by the senior management team, every six months by the Audit Committee and annually by the board. Significant new risks are brought to the attention of the Audit Committee and the board as necessary.

The risk assessment process identified the following major risks:

- Fraud or mismanagement of the funds provided to delivery partners overseas;
- Failures to safeguard children adequately; and
- Significant changes at short notice to funding arrangements, particularly for long-term programmes.

The charity put measures in place to manage these risks and monitor the likelihood of these risk events, in order to minimise the financial and reputational impact they would have on the charity.

Using risk to help decision-making

To make good decisions, you need to understand both the benefits and risks associated with a proposed course of action, either of which could have unforeseen consequences. A good decision-making model will help ensure you gather all relevant information before you make the decision, but also acknowledges that there are a range of possible outcomes.

Decision-making by organisations is improved significantly when there are a range of possible solutions to choose from. The financial risk management tools described below are best used when comparing one proposed course of action to another. Decision-makers need to understand what they are saying no to, as well as the decision to go ahead, so all the options considered should be made explicit.

In addition, the decision to go ahead with something always means you may be closing the door to other opportunities. For example, you may decide to develop a new training course, which should generate revenue from fees. However, you will use some cash initially to develop the course. As you can't use this cash for anything else, it is known as the 'opportunity cost' of the activity, and you can compare this cost to the cost of alternative proposals or activities neglected. A proposal that requires a lot of money will prevent or delay other activities and so represents a greater risk to the organisation. Cash is not your only resource and you should think about opportunity cost in terms of time and capacity as well.

Tools for assessing financial risk

If you are considering a major new venture or expansion of your current activities, financial data will help you make good decisions. However, none of us has a crystal ball so our predictions about the future may not be reliable. The tools described here will help you to focus on the risks associated with some of your forecasts and quantify the uncertainty inherent in any forecasts.

Understanding your cost structure

Fixed costs are the central overheads, management and administration costs, such as the costs of the premises and administration. They are indirect costs that are incurred as a necessary part of providing infrastructure and oversight to the organisation's activities. These are costs that do not reduce quickly or easily if you reduce the amount of activities. You need to ensure that you have covered these costs simply to break even.

Variable costs are only incurred if you run the activity. You would immediately be able to cut costs if you ceased the activity. These are also called the direct costs of an activity. The income for an activity, such as fees or grants, has to cover the direct costs of the activity as well as contribute towards the fixed costs of the organisation. So we call the surplus income after you have covered direct costs the contribution. This is a familiar concept to organisations that have studied full cost recovery. However, the full cost recovery model shows you how to recover your overhead costs in a stable environment. We will now go on to consider the right approach for organisations considering major change.

Break even analysis
We can use our understanding about cost structures to help us understand the level of risk of a venture. Break even point is reached when the contribution is equal to the fixed costs (i.e. where total income equals total costs). We can use this concept for an activity or for a whole organisation. If we are considering a new venture, then it will help us to understand the point at which it will break even. And we can convert the financial information into the number of units that need to be sold, or the number of training places we need to fill. We use our judgement and experience to assess whether this point is likely to be difficult to achieve and so it informs us about the risk profile of a proposed activity.

Illustration

You have received an offer from a choir who want to put on a performance as a fundraiser. You need to organise the event, promote it and sell tickets. You find a venue which will cost £5,000. Print up flyers and tickets for £1,000 and decide to sell tickets for £10.

You will have to take a risk on the financial commitment of both the venue hire and the printing. So you need to recover £6,000 you have spent before you can break even. With tickets selling for £10, you will need to sell 600 tickets to raise £6,000. Converting the financial risk into a tangible target, you can now discuss with colleagues whether 600 is an achievable target.

Break point
There is an inherent assumption in break even analysis that additional activity can be taken on within the same level of fixed costs. But obviously you will only be able to expand so far on this basis, as you will run out of space in your premises, or admin staff will be over-stretched. So you may need to move to new premises or hire more staff. Usually this means a significant and sharp increase in costs – a step increase. The point where this step increase is needed is called break point.

Using break even analysis, we can also see that an increase in an organisation's fixed costs means it needs to have a matching increase in contribution from activities. This is where you may face a mismatch – the fixed costs are usually a step increase, whereas contribution from activities is a gradual increase over a period of time. So an organisation faces significant risks at this point and needs to consider these carefully before making a decision to go past break point.

"Decision-making by organisations is improved significantly when there are a range of possible solutions to choose from."

Illustration

A charity is funded from contracts for its services. Contracts are typically for three years but then extended for a further two years providing performance has complied with the contract requirements. The main risk for the charity is that contracts are for large sums, so winning or losing one contract makes a significant difference to the scale of their activity. Building up the size of the central services to cope with a new large contract is taking a risk, because it will be difficult to cut back on those costs later if they lose one or two other contracts.

The charity decides to plan for moderately ambitious growth. This establishes the size of the central office function and means that they can make decisions about the contract pipeline. They establish their policy as a risk management strategy – a target level of gross income and a cap on central costs.

What this also illustrates is that charities need to find the right balance between overhead costs and levels of activity. Most charities need to allocate overhead costs to their activities so these can make you too expensive if they are too high. On the other hand, if your income grows quickly, you can find that management capacity is insufficient. This opens up new risks of poor compliance activity and negative impacts on quality. When making decisions about new activity and growth, you need to factor in the management capacity needed to support it. This is an invisible, creeping risk that damages performance and can turn into a killer risk if you develop a poor reputation for delivery.

Payback period

There is also a cash flow aspect to breaking even – this is best understood by looking at the payback period for a project or activity. All activities require some time invested at the outset, and sometimes cash is required as well. As well as focusing on the cash invested, include staff time and effort if it requires additional staffing or effort diverted away from another activity which would generate funds. The payback period is the time needed to repay the initial investment. You can work it out by preparing a cash flow forecast for the activity, based on your understanding of the timing of events.

Illustration

You wish to publish a book about your specialist approach in order to raise your profile. You estimate it will cost £15,000 to write the book and that it can be sold at £25 a copy.

This translates into break even sales of 600 copies, so the question is how long it will take to sell that number. The publisher advises that sales are likely to be strongest at the beginning when the book will be heavily promoted, but will then drop off to a steady, but small stream of sales. So it is likely to take a year to sell 600 copies. This can easily be converted into a cashflow forecast for this activity, showing the timing of the expenditure and the receipts.

This emphasises the need for working capital and the point about opportunity cost – this project will tie up cash for a couple of years. If it is a small amount to your organisation then it might not be a problem, but it will depend on the context.

A new activity will have a higher risk profile if it takes longer to pay back. A long payback period means that there is more time for other changes to occur and disrupt your plans. For example, a competitor may launch a similar product, the legislation may change making your activity irrelevant, or technology may develop to make achieving the same outcome easier.

Return on investment
This is typically a financial measure and so it works best for fundraising activities where the purpose is to achieve a financial return. There are methods of calculating a social return on investment which are suitable for some activities and the same principles apply. You estimate how much income you think you will be able to generate from an activity and compare it to the costs of the activity in a ratio. It is usual to convert a lifetime return ratio into an annual return on investment in order to compare activities.

Illustration

You plan a new fundraising campaign which requires investment in advertising, website development and new videos. In all the external costs are likely to be £50,000. The income forecast predicts £200,000 in donations including Gift Aid. So the return on investment is 1: 4 or for every £1 you invest you expect to receive £4.

You can then compare this rate of return to other fundraising campaigns. However, you also need to consider the reliability of the forecast. Do you have previous experience of similar campaigns and evidence that makes this level of return likely? It might be easier to quote a range of likely income and then calculate the return based on top and bottom ends of the range.

It can also be more difficult to compare activities if one involves external costs but the other activity only involves internal costs. You would need to bring them onto the same footing to ensure you are comparing apples with apples.

Getting decisions right

We all make risk decisions every day. However, for organisations, the way decisions are made and ensuring that all risks in respect of a particular decision have been considered – including financial risks – can be critical to their long-term survival.

Whilst risk can be a threat to an organisation, an appropriate level of risk may also create opportunities. Using a structured approach to discussing and categorising risk within your organisation, together with the appropriate tools to assess any financial risk, should enable decision-makers to be presented with a coherent business case, allowing an informed decision to be made.

Better risk registers

Most organisations now have risk registers and there are benefits to adopting a formal process across the whole organisation. However it is important that charities do not become complacent: risk registers do not manage risks, they merely identify them.

A risk register is a tool that records identified risks and ranks them according to likelihood and impact. It is most useful when monitored regularly and updated to reflect changes. The register will usually record the current controls in place to manage the identified risks, as well as additional actions required to improve the controls.

Some organisations make really good use of the opportunity to have a meaningful discussion about risk. The danger is that the board and managers view the risk register as an annual 'tick box' exercise rather than a continuous process. Creating the risk register can be a useful process in itself because it provides a structure for discussion, but placing a risk on the risk register does not mean that the risk is being managed.

There is no prescribed format for a risk register, but there is plenty of guidance on good practice. Some organisations may be required to submit their risk register to a significant stakeholder such as a government body providing funding or as part of a due diligence process. In this situation, the risk register will be evidence of good governance and management.

Advantages of risk registers:

- Provide a structure for discussion and debate
- Clarify actions required and increases accountability for these actions
- Allow for analysis of operational risks that can be communicated to support strategic decisions
- Co-ordination and analysis of departmental risk registers may identify the cumulative effect of low-ranked risks across the board
- Help to prioritise actions
- Support and evidence resource allocation
- Can be requested by donors (for specific programmes)

However, there are often flaws in risk registers so this section explains some of those flaws, and possible actions to improve your risk register.

"A risk register is a tool that records identified risks and ranks them according to likelihood and impact."

Drawbacks to risk registers

- 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.
- Risk registers do not encourage horizon scanning – people tend to focus on the known risks and just update the existing register.
- Registers can be seen as just a bureaucratic process that does not add value.
- There is little scope for cross-referencing risks and seeing their inter-dependency.
- Can be seen as a stand-alone process rather than a part of planning and monitoring.

Suggestions to improve your risk register

This is a collection of ideas, most of which we have seen used in practice.

Provide more guidance on the scoring system
Most risk assessment processes ask for a score on likelihood and impact. The problem here is that each individual may interpret the scores differently. So providing guidance will help to reduce the inconsistencies. For example:

Likelihood	
1. Very unlikely	Barely feasible to occur
2. Unlikely	Extremely unlikely in the near future (current year) but possible in the longer term
3. Possible	Not very likely in the immediate future, but reasonably likely in the longer term
4. Likely	In the current year, and probable in the longer term
5. Highly likely	Probable in the current year, and highly probable in the longer term

Impact	
1. Insignificant	Nothing to worry about
2. Fairly serious	Possibly important, but can be managed although it would take up some time and resources
3. Serious	A threat which could cause us reasonable problems and would definitely take up time and resources
4. Very serious	Would hinder the achievement of our strategic objectives and/or would take up considerable time and resources
5. Major disaster	Could seriously undermine the standing and position of the organisation

Rank for reputational and financial impact
Most risk assessment processes ask for a score on impact, but this is a single ranking. If you split this into two elements – one for financial impact and one for reputational impact – it will be easier for people to score and it will be more informative. For example, a fraud might have a small financial impact, but the reputational damage could be greater. So you would create a ranking system like this:

Financial impact	
1. Insignificant	Less than £1,000
2. Fairly serious	£1,000 – £2,500
3. Serious	£2,500 – £5,000
4. Very serious	£5,000 – £25,000
5. Major disaster	More than £25,000

Obviously, the amounts would depend on the size of your organisation.

Reputational impact

1. Insignificant	No impact on stakeholders' perception of us
2. Fairly serious	Potential impact but can be managed according to our response plan
3. Serious	Definite impact on reputation and needs careful management
4. Very serious	Could permanently damage our reputation and could require significant change
5. Major disaster	Could seriously undermine the standing and position of the organisation and even lead to closure

To illustrate how this might translate into some entries on a risk register:

	Likelihood	Financial impact	Reputational impact	Total
Key worker steals from a service user	2	1	3	6
Sensitive data is lost	3	2	3	18
A child in our care is groomed by a member of staff	1	4	5	20

Add a further ranking – risk tolerance

This brings the organisation's risk policy into the ranking of risks. The risk policy should provide a context for the ranking of risks and for the risk register as a whole. For example, sending funds overseas would be a high risk activity for a UK-based church that does not usually work overseas. But for an international development charity it is commonplace and in keeping with its risk appetite, therefore it would be a low risk activity. Charities usually want to take risks in some areas (such as piloting new ways of working) but they are risk averse in other ways (e.g. risk of harm to a beneficiary). This is why it is important for boards to have a strong understanding of their risk appetite and articulate this clearly. The additional dimension of risk tolerance can reflect this. For example:

1. Risk taking	Where the potential benefits of taking the risk are significant against the likelihood and impact of the risk which are limited
2. Risk orientated	Where the dangers of the risk are limited and reasonably offset either by the opportunities and advantages afforded by carrying it or by eliminating the costs of actions and systems needed to mitigate it
3. Risk equilibrium	Where the dangers of the risk are fairly evenly offset by the opportunities and advantages offered by carrying it
4. Risk averse	Where some risk is unavoidable but this should be kept to a minimum
5. Zero tolerance	Where the nature or impact of the risk is such that it is not acceptable within the organisation

The extra dimension allows you to differentiate risk rankings more effectively. For example:

	Likelihood	Impact	Risk tolerance	Total
Database crash	4	4	4	64
Key person leaves	3	2	2	12
New procedure fails	4	3	3	36

Identify consequences and causes

When the risk is being identified and described in a risk register, the language is sometimes too imprecise, but also the risk, the cause and the consequence are muddled. For example, charities often have as a risk "loss of income". In most situations, the loss of income is really the consequence of something else – the failure to deliver required outcomes, the breakdown of a relationship. So at the stage of identifying risks it can be useful to use a worksheet that asks people to think through the risk, the consequences and the causes. The worksheet can then be translated into a more coherent risk register. Identifying consequences also helps to rank the impact.

Illustration

Concern	Consequences	Causes	Restated risk
Reduction in income	Overheads too high as a proportion of costs and cannot recover through contracts; losses; possible restructure to cut overheads	Only winning one in four bids for funding because of a lack of skill and experience in bidding for new contracts	Lack of relevant bid-writing skills
Loss of key staff	Lack of capacity to deliver on strategic plan; cost of recruitment; delay to projects	Poor pay compared to others; lack of opportunities for promotion; poor leadership	Low morale; Pay scales not keeping pace
Loss of data	Potential fine from ICO; damage to reputation; penalties from regulator	Problems for staff working from home so they work around the procedures	Out of date IT policies and procedures

Review changes in risk regularly
In some organisations, the audit committee reviews the risk register at each meeting and spends time with senior managers understanding how the risk rankings are changing. This may be because the external environment is changing or because the organisation is managing the risks better. Showing the change in the status of the risk by arrows can be helpful to committee members and the board so that they get a sense of the direction of travel.

The audit committee can also review whether there are new risks that should be added to the risk register, and remove risks that are no longer significant. This approach to using risk registers keeps them relevant and makes them a useful tool for oversight and governance.

Cluster risks which have similar consequences
The control or management action may be the same for a whole cluster of risks so repetition can be avoided if you group these sensibly. For example, there may be innumerable ways in which someone could be injured on your premises. The consequences are very similar in all cases and you can probably summarise the necessary preventative control in a few words. This will reduce the size of risk registers and make them less cluttered.

Separate strategic risks from operational risks
Often risk registers are organised by categories such as governance, IT, reputation, technological etc. This leads to a mixed list of strategic and operational risks, making it difficult to see which are the more important risks. Separating strategic risks out and providing more information about these will promote greater discussion about the major risks. Your strategic risk register might consist of a page per risk describing the risk, its causes and consequences, the management actions already in place and further actions identified.

Identify responsibilities
Many risk management methodologies suggest that you should identify a ‘risk owner’. This can be counter-productive as many risks pervade all aspects of the organisation, such as reputational or health and safety risk. You actually need everyone to pay attention to risks such as these. It is more feasible and more practical to appoint someone to be responsible for the management actions you have identified as mitigating responses.

Ignore likelihood for important external risks
If you have identified an external risk as a significant threat or opportunity, then it is not useful to try to rank it for likelihood. If you are seeing it as significant, then this is a high impact risk. History has shown that we are very poor at judging likelihood. We tend to underestimate the probability of undesirable outcomes. This is either because we are naturally optimistic in outlook or we are blinkered to the possibility of negative outcomes that will have an adverse effect on us.

Assurance activities

The board needs to have a clear mechanism for getting assurance on the management of risks. A board should agree the risk policy and oversee the process to identify and assess key risks affecting the organisation. It should understand how the organisation intends to manage those risks, but it also needs assurance that the management of risk is effective.

Understanding how risks are managed

Taking the approach to identifying risks outlined above, it then becomes easier for boards to understand how risks are being managed. A vast amount of day-to-day management is about managing risks, so risk management should not exist in a separate function or be undertaken as a separate activity. An understanding of risk management should start from the existing management activities. First, we consider the strategic risks. Earlier we suggested that all organisations have up to five major strategic risks. Next, a board needs information about how the existing processes, procedures, policies and quality systems contribute towards the management of the key risks. This can be brought together into an assurance framework.

“A board should agree the risk policy, and oversee the process to identify and assess key risks affecting the organisation.”

Illustration of an assurance framework

The following set of five risks have been identified by a charity board as their Big Five, as discussed in the section on Governance of risk.

Now the board want to understand more about the existing management processes which will help to manage these risks.

Risk	Information and existing processes
Quality of service to beneficiaries	Beneficiary feedback, quality assurance audits
Financial sustainability	KPIs, management accounts
Compliance and reputation	Incidence response plans, H&S committee
People	HR handbook, performance management systems
Safeguarding	Safeguarding policy, staff training

What is apparent is that these are not typical controls, such as bank reconciliations and authorisation. The focus is not on internal financial controls, but on management processes that for well-functioning boards should appear on most board agendas.

An interesting exercise is to map these risks to the board agenda. If the board is discussing the right issues and the right strategic risks have been identified, there should be a high level of correlation between the two. If that does not exist, then either the board is wasting its time on unnecessary issues or the risks are wrong.

The other important point about this approach is that it is an integrated approach to risk management. The job of management is to identify, understand and manage risks. The board's job is to oversee this, but also to challenge and ensure that it is being done well enough.

Our survey said...

Sayer Vincent and CFG carried out a small survey of attendees at CFG's Risk Conference in November 2015. Here are some of the responses on the strengths and weaknesses of their current approach to risk management:

- *"Lack of communication upwards and engagement generally. Things take too long to resolve."*
- *"[We are] dependent on a few key people."*
- *"Primarily focused on finance."*
- *"We take legal/compliance risks seriously and report them. But risk [management] is not seen as an opportunity to help us to achieve our objectives."*
- *"We need to make sure it is embedded in operational planning. It tends to be reactive and the Board is not fully engaged with deciding risk appetite. [But] we are talking about it monthly [and] we are…embedding it in thinking."*
- *"[Risk is] shared throughout the business and reviewed regularly. [We have] a working document not just a tick in a box… [however there are] possibly too many risks articulated – should be more discerning."*
- *"[We have] Full involvement of the Trustees, [but] too much detail at Trustees' meeting without any involvement of most staff."*

Getting comfort

This is the trickiest bit for the board. Their source of information on how risks are being managed is the management team. To what extent can and should they rely on that? How reliable are the underlying processes? This is where the board needs the ability and confidence to ask challenging questions. The board's challenge should be fair and constructive. But the management team needs to recognise that challenge is a key element of a board's role.

Organisational culture plays an important part and the style of governance needs to be balanced to allow for critique not just criticism. The board needs to encourage managers to be honest and upfront with the board. If things are not on track managers need to feel able to report this, rather than reporting only good news.

For smaller charities, it may be enough to review reports and instigate regular reviews of policies and procedures. Many charities will appoint an audit committee to provide oversight of the risk management function. The audit committee can review in more depth the assurance processes underlying the key risks. For example, it can take one or two risks at each meeting and, with the support of the relevant managers, drill down into the underlying controls and gaining confidence that the processes to manage risk are operating as intended. The committee then reports to the full board.

Some risks may be so central to a charity that the Board considers that further independent assurance is required. In larger charities, this can be provided by an internal audit function – resourced either by an in-house staff team or an external provider. But there is a scale of potential risk assurance that smaller charities may consider without committing significant resource. This is explored further in the next section.

Case Study – Royal Opera House

Royal Opera House (ROH) describes itself as having a "solid and sound approach" to risk management. In order to further develop this, a team of internal auditors looked at risk management in terms of maturity. Trustees wanted the internal auditors to look at how risk was managed, in order to ensure that they had the appropriate controls and to give assurance to Trustees.

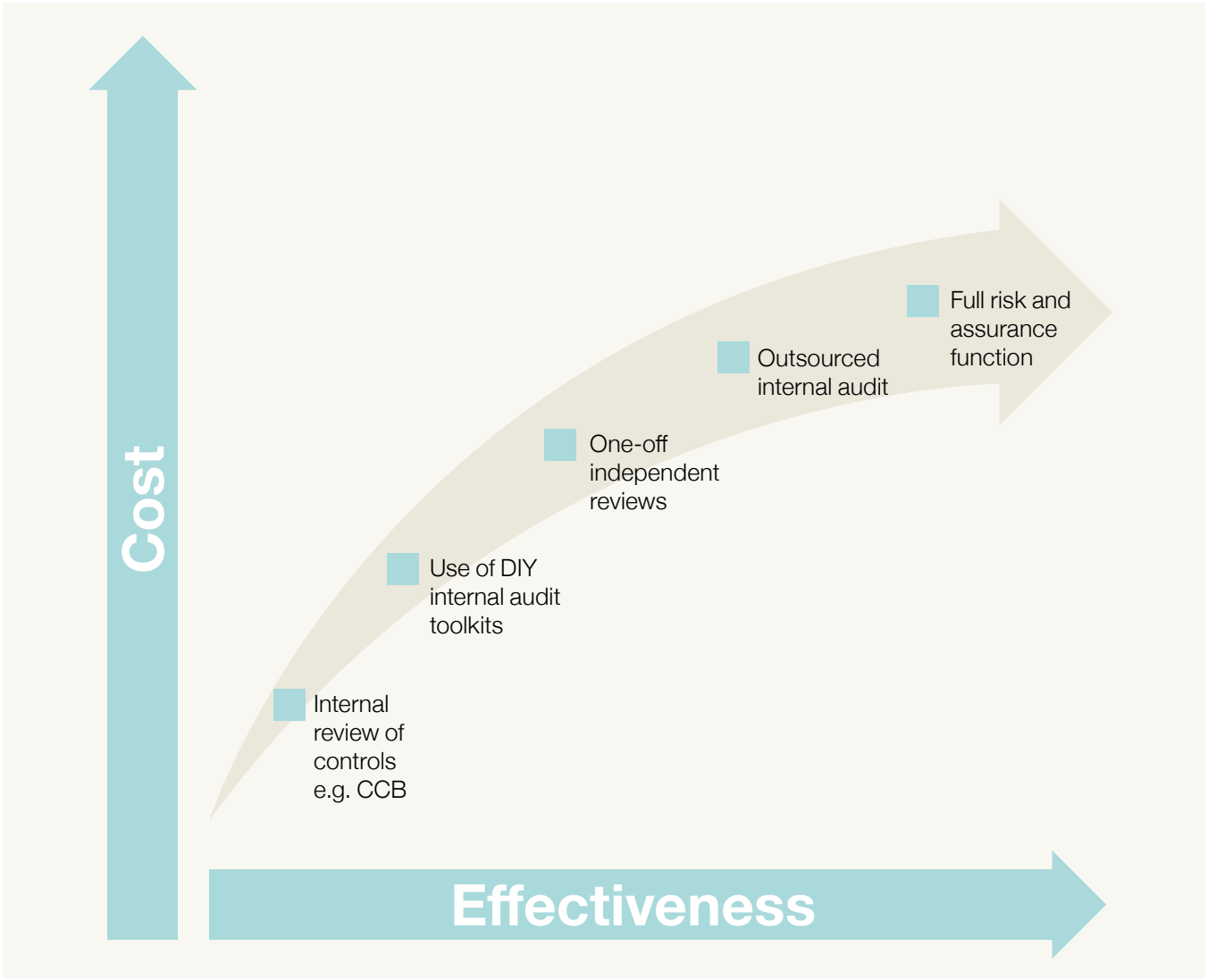
One challenge has been getting staff to buy into the process of managing risk. ROH regularly tests how it would respond to certain incidents, for example a fire incident, terrorism, cyber attack, etc.

Trustees were supportive of this approach to mitigating risk and to the additional assurances it provided. However, with staff, it took longer – especially when people were used to doing things a certain way. For example, changes to procurement processes met with resistance initially because new processes differed from "how they had always been done". Following a technology project, ROH learnt that it was really important to engage staff with the process, even focusing on those who were likely to be the most resistant and getting them on board first. They also found it useful to adopt a staged roll-out when making changes, so that they were easier to manage.

Different levels of internal audit

It is often assumed that internal audit must be an independent function and the profession has endless debates about reporting lines. If we start from the assumption that you have a positive organisational culture (risk culture is covered in more detail in a subsequent section), then actually the term internal audit does not need to describe a critical function that is a thorn in management's side. A less combative approach will be more constructive. Internal audit activities can be undertaken at different levels and made to fit smaller organisations.

Cost is also a factor – the amount spent on assurance activities should not outweigh the benefits. If the risk profile of an organisation is low, then there is little benefit from a significant investment in assurance activities. Additionally, the exercise described earlier, of understanding where management activity already provides assurance on the management of risks, is crucial. Additional assurance can be focused on the high risk areas and areas where management activities cannot provide sufficient assurance.



Internal review of controls
For a small charity, it will provide information and evidence on the operation and effectiveness of basic controls. The Charity Commission publishes a guide 'Internal Financial Controls for Charities' (CC8) which contains a useful checklist. This could be the basis of an annual report to the trustees providing comfort that proper financial controls are in place and being operated.

DIY internal audit toolkits
Organisations can develop their own or buy suitable toolkits for specific areas of operations such as charity shops, project management, health and safety, data protection and information security. These will not always be written specifically for a charity, but nonetheless may offer a framework. A member of staff may need to be trained to use them. Some quality assurance frameworks, such as PQASSO, may provide similar levels of assurance.

One-off independent reviews
There may be specific areas of risk requiring expertise and knowledge that you do not have in-house, such as data protection or information security. Scoping a review to build in assurance activities is simple and an effective way of gaining high quality feedback on your systems and processes.

Outsourced internal audit
In order to commission services from an external provider, you will need to have good risk management processes in place, or ask the provider to help you to improve your risk management as the first assignment. It will usually be the first review the provider undertakes as they need to undertake further work based on an understanding of the organisation's risk profile.

The internal audit plan should be risk-based to give the board assurance on the key risks and should build on the organisation's assurance framework. The internal auditor should use the framework as a starting point and should test the effectiveness of the management of risk.

Cost effective ways of using an outsourced internal audit blend the use of DIY internal audit toolkits with the internal audit firm providing oversight and quality control on the internal activity. It can also be combined with specialist independent reviews and audits.

Full risk and assurance function
An in-house function needs to remain independent and should not be responsible for undertaking risk management. The people in the team can train managers and staff in risk management, but the focus of their activity needs to be on the provision of assurance that the planned management of risk is effective.

An in-house function can additionally provide support to managers to develop effective response plans (e.g. a fraud response plan) and play a role in whistle-blowing procedures. They can also investigate problems and help managers to respond to urgent issues.

Three lines of defence

For larger organisations, the methodology known as 'three lines of defence' offers a helpful framework for assurance activities. It is a coherent framework that brings together different elements and activities to provide good coverage and avoid duplication of activities.

The first line of defence is represented by operational controls. Operational managers are responsible for designing policies and procedures to manage risks, for guiding behaviours and documenting expectations of controls. This is covered in greater detail below.

The second line of defence is the supervision and internal checks operated to ensure compliance with regulations, policies and procedures. This might include DIY internal audit activity, management meetings to review reports and key performance indicators.

The third line of defence is separate from the first and second lines and provides senior management and the board with independent assurance on risk management. As a 'third line' assurance function, internal audit should not only evaluate the effective design and proper functioning of risk and control systems implemented by (first line) operational management, but also the way in which second line of defence monitoring functions – such as centralised risk management – operate. Internal audit should also evaluate whether the governance structure, from the board downwards, provides for the effective management of risk across the organisation, including whether the full spectrum of risk is being appropriately considered and reported.

Source: Institute of Internal Auditors' position paper on 'The Three Lines of Defense in Effective Risk Management and Control' – see Resources section

The first and second lines of defence typically report to senior management, while the third line reports to the board, usually via an audit committee.

The most cost-effective ways of designing the three lines of defence would be to invest most in the first and second lines, thus reducing the level of need for the more costly third line.

Mapping the first and second lines of defence

You can bring this concept to life with an assurance map. First we describe what the areas are:

First line of defence – broad areas to cover in controls	Second line of defence – examples of activities
Culture This is about the organisational culture, risk culture and values of the organisation, how well these are communicated and aligned to the purpose and strategy	• Managers live the values and lead by example • Plans and business cases are challenged to ensure they are aligned
Policies and procedures Documented policies that are kept up to date and reflect the values. Procedures that make sense and are actually implemented.	• Checks by staff in another department that procedures being followed • DIY internal audit
Roles and responsibilities How well people understand their remit and are accountable. Includes contractors and outsourced services. Adequate segregation of duties.	• Job descriptions reviewed by manager and HR before recruitment • Contracts reviewed by someone outside department
Training Appropriate, relevant training to ensure that the people with the right skills have the knowledge and tools to do their jobs. Also people are trained in the organisation's purpose, values, policies and procedures.	• Competency frameworks • Training records reviewed by HR
Managing people Regular supervision by managers and performance management such as appraisals. Appropriate reward policy. Staff welfare arrangements including terms and conditions, employee assistance. Volunteer management.	• HR review appraisals • Remuneration committee sets reward • Staff survey conducted • Exit interviews conducted by independent person and monitored by HR
Planning Adequately detailed plans prepared to implement the strategy and used to identify inherent risk. Risk assessments prepared for new activities and events. Business continuity and response plans prepared.	• Independent review of all plans and risk assessments • Test runs of business continuity and response plans

Illustration

Family Support Services has contracts to provide support to families with young children at an early stage to prevent the need for further interventions from social services. Social workers visit families in their homes to identify actions and implement them.

First line of defence	Second line of defence
Culture The organisation's values are covered in inductions and an annual staff conference. Safeguarding and personal safety are key concerns where staff are mandated to take concerns to the CEO and a nominated board member.	• Staff survey monitored for evidence that values are widely recognised and adopted. • Review of incident reports.
Policies and procedures There are established policies and procedures for working with families in their own homes as well as safeguarding, health and safety and IT policies.	• Annual review of policies • Periodic review of case files by quality assurance team
Roles and responsibilities Staff are assigned a certain number of cases and are responsible for delivering outcomes in the plan.	• Annual review of job descriptions by HR to ensure that they are up to date.
Training All staff are qualified social workers and undergo specific training for this programme.	• HR review training records and check that only staff who have been properly trained are put onto the programme.
Managing people Staff work in teams and meet weekly with their team leader to review cases. Workload is monitored as well as new risk issues with cases.	• Review staff survey results to check for signs of stress • HR undertake exit interviews
Planning There is a clear process mapping the way that staff should work with families, setting out the outcomes to be achieved at each stage. Families are assessed before they are admitted to the programme for suitability and to ensure no additional problems such as violence or substance misuse.	• Management reports monitor the achievement of performance at key milestones. • Senior managers monitoring overall programme.

This form of assurance mapping can be used both as a plan (illustrated above) and as a reporting mechanism, when it can be expanded to include notes about the actual findings. The benefit of this approach is that it integrates risk management activity into the normal reporting and monitoring. It also shows how certain monitoring activity, such as the staff survey, can provide assurance on a number of different areas of risk.

Managing risks to your reputation

One of the risks that is nearly always highly ranked on charity risk registers is reputation. And yet it is not really a risk.

Damage to our reputation is the consequence of other risks materialising.

What do we mean by reputational risk?

What we really mean are risks to your reputation. These are adverse or beneficial risks – in other words, actions or events that have an impact on an organisation's reputation. Some examples of risks that would be included:

- A charity representative saying the wrong thing in a media interview
- Offending a stakeholder group (staff, volunteers, beneficiaries, funders) such that they go to the press
- Losing credibility with government so that your ability to influence policy is reduced
- A gap appearing between what we say and what we do e.g. a children's charity investing in a company that uses child labour
- Fraudulent activity
- Charity's name misused by unauthorised people
- Abuse or similar inappropriate treatment of beneficiaries
- Death of a supporter while raising funds for your charity
- A fundraising activity goes viral

We could be dealing with many smaller incidents or a "killer risk", which is so significant it wipes out the entire organisation. For example, you can imagine a situation where a child protection charity would have to be closed because the founder was accused of having child pornography on a laptop computer in their possession. Note that they would not have to be found guilty – the accusation would be enough to completely undermine the credibility of that organisation. On the other hand, we could be thinking of a situation where a charity suddenly receives a huge amount of positive publicity because of an activity by a beneficiary or a supporter.

Potentially there is a long list of risks to your reputation, so this is a case of considering how you will respond to risks to your reputation whatever the cause, and how you can enhance your reputation.

Understand the nature of reputational risk

Risks to the organisation's reputation will be relevant to every member of staff and every volunteer. Everyone can have an impact on the organisation's reputation – adversely or beneficially. So you need to find ways of engaging people at all levels with this type of risk in a way that means something to them. In some sense, this is conveyed through the organisational culture and the values you hold as a charity. You will certainly be helping to raise people's awareness of this issue if you do communicate your values effectively to everyone in the organisation. However, you will also need to convey to people how an impact can spread and have an effect on the whole organisation. It can sometimes be hard for a member of a team out in the field to appreciate how a relatively minor event can spiral out of control to become a major risk to a charity's reputation.

The reputation equation

A charity's reputation is held in people's perception of that charity. So how are people's perceptions formed? It depends on what they experience of that charity – in what they read, hear, see or how they feel in their own dealings with that charity. People compare that to their expectation. If they feel disappointed when their experience of the organisation does not match their expectations, then this diminishes the standing of that organisation in their view. Whereas if they think better of an organisation after an interaction with them, then this enhances the organisation's reputation.

Oonagh Mary Harper describes this as the "reputation equation" in an article in *Corporate Social Responsibility* Monitor (2002)

Stakeholder expectations minus **Experience** equals **Reputation**

If you are matching people's expectations then you will be maintaining your reputation. It is also important to remember that expectations are not static. They respond to a variety of factors and boards need to have a flexible approach when considering reputational risks.

Stakeholders in a charity

Beneficiaries
Donors
Staff
Volunteers
Trustees
Funders
Users
Suppliers

Stakeholders

For a charity, the stakeholders in this context may be diverse. You should think about who the stakeholders are in your charity and how they interact with your charity. This will be how they experience your charity and build up their perceptions of your charity. You also need to understand what their expectations of your charity are.

In order to increase your knowledge of both stakeholder expectations and perceptions of your charity, you will need to consider gathering feedback from them. This may be through surveys and polls, reference groups or by having representatives on the board. One source of advice and guidance on how to gain this knowledge is available from AccountAbility at www.accountability.org.uk.

Once you start thinking about your reputation as an equation, then you can work on the components of reputational risk. In a *Harvard Business Review* article, Robert G. Eccles looks at different aspects of stakeholder expectation.

Your organisation's reputation may exceed its true character. This is an expectation gap that is dangerous as you will constantly live in fear that the public will discover the truth. You have two choices; either you bring the reality up to the public expectation or you manage expectations down.

It could be operating in reverse and the true character of your organisation is better than public perception. This is tough as you are fighting against a tide, but PR experts quoted by Eccles recommend that you put out positive stories and try to make sure the media coverage is tipped towards positive news. Slowly, you will be able to redress the balance. Rayner recommends that you do more work on understanding your stakeholders' expectations, as described below.

Expectations change and you may be caught out because you are operating to an old understanding of stakeholder expectation. Look at a simple scenario such as communication. We used to write letters and send them in the post, so you did not expect a reply for weeks. Now we communicate electronically, we expect instant replies. The important point that Eccles makes is that you need to have a way of spotting these changes and bringing them to the table in your organisation.

Eccles makes a further point which is relevant to charities and not-for-profit organisations as much as big corporations:

"Senior executives tend to be optimists and cheerleaders. Their natural inclination is to believe the praise heaped on their companies and to discount the criticism. But looking at the world and one's organisation through rose-tinted glasses is an abdication of responsibility. Being tough-minded about both will enable a company to build a strong reputation that it deserves."

Robert G. Eccles, Harvard Business Review, February 2007

Ways to improve your management of reputational risk

Develop your reputational risk strategy by starting with your stakeholders – what are their expectations? Do you know how they perceive you? How would you like them to perceive you? You need to see reputation as a bank account – you can pay in to help the organisation deal with the small things that will inevitably go wrong. So map stakeholder groups to the drivers of your reputation and assign departments to take a lead in these areas – building the reputation capital of your organisation, not simply having a plan to react to public relations problems when they happen. What we suggest here are some ideas to promote some fresh thinking about managing reputational risk.

Source: Managing Reputational Risk, Jenny Rayner, 2003.

Reputation drivers

Charity reputations can seem to be ephemeral and intangible, but they are rooted in some straightforward and basic tenets of good practice. These are the elements that drive perceptions about the organisation:

- Ethical standards
- Corporate governance and leadership
- Regulatory compliance
- Financial performance
- Delivering to beneficiaries
- Delivering to funders and donors
- Workplace talent and culture
- Communications

These are the areas that each charity can examine and questions can be asked to see if it is likely to be establishing and maintaining a good perception of the organisation.

Ethical standards	• Does the organisation monitor/respond to specific social and ethical issues which would be of concern to its stakeholders or at odds with its vision?
Corporate governance and leadership	• Does the board set an appropriate tone for the organisation? • Does it have a realistic and compelling vision for the future? • Does it actively demonstrate good governance?
Regulatory compliance	• Is the organisation complying with all relevant laws and regulations? • Does it anticipate and keep up with regulatory developments? • Does it become involved in legal disputes?
Financial performance	• Does the organisation have sustainable income sources? • Does its funding base suggest it will be able to continue in the longer term?
Delivering to beneficiaries	• Is it consistently meeting the needs of its beneficiary group? • Does it actively identify the changing needs of its beneficiary group and seek to address these? • How good are the services offered? • How are complaints handled?
Delivering to funders and donors	• Is it consistently meeting the needs of this group? • How accountable is it to them? • How are complaints handled?
Workplace talent and culture	• How well are employees and volunteers treated? • Is it able to recruit, develop and retain quality employees and volunteers? • What is the charity like to work or volunteer for?
Communications	• Does the organisation provide meaningful and transparent information to all stakeholders, allowing them to understand its values, goals, performance and future prospects?

Mapping reputation drivers to stakeholders
A practical tool in managing reputation is to consider which reputation drivers are going to be of most consideration to particular stakeholder groups.

	Ethical standards	Corporate governance and leadership	Regulatory compliance	Financial performance	Delivering to beneficiaries	Delivering to funders and donors	Workplace talent and culture	Communications
Beneficiaries								
Employees								
Volunteers								
Donors								
Funders								
Media								
Government								
Charity Commission								
Partner orgs								
Others								

Then focus on which part of the organisation is closest to the reputation driver and the stakeholder group, and best placed to take a lead on managing aspects of this risk. Instead of a vague idea that your reputation is both your biggest asset and your biggest risk, you now have manageable components of reputation which can be managed more effectively.

"Most companies, however, do an inadequate job of managing their reputations in general and the risks to their reputations in particular. They tend to focus their energies on handling the threats to their reputations that have already surfaced. This is not risk management; it is crisis management – a reactive approach whose purpose is to limit the damage."

– Robert G. Eccles, Harvard Business Review

"Instead of a vague idea that your reputation is both your biggest asset and your biggest risk, you now have manageable components of reputation."

Build up reputation capital

This opens up the whole discussion around managing risks to your reputation. It is not simply about reacting to adverse publicity. If you are going to properly manage the risk, then you need to consider building up your reputation capital. This allows you to manage smaller risks to your reputation – they will bounce off as you build up resilience by having a large stock of good reputation. People will make allowances for small things to go wrong and will not adjust their perception of your organisation until many smaller adverse events force them to adjust their perception, or one killer adverse experience forces a major shift.

Ways in which you can pay into your reputation account are mostly about raising awareness of what your charity does and who it helps. Often the publicity and communications of charities is aimed at potential donors, but this is not just about marketing. You should consider ways of communicating the impact of your work and how you help your beneficiaries. This applies to charities that receive all their funds through grants and contracts just as much as those seeking donations from individuals. The purpose of improved communication about your achievements is to build up your reputational capital.

You can also achieve an increase in reputational capital by being honest about failure and problems. For example, your charity may experience a significant fraud in a branch. This is not a killer blow to your reputation but an opportunity to demonstrate openness and honesty with your stakeholders. Think carefully about the order in which you manage communications, as a funder would probably expect to hear from you personally before they read about it in the press. Since you have control over this communication, make sure that you explain the circumstances and what you have done about it. In a similar way to handling complaints well, a failure or problem can become an opportunity to engage stakeholders. After such an incident, they are more likely to understand the nature of the challenges you face in trying to achieve your objectives.

Example – The Samaritans

Claire Squires was running in the London Marathon in 2012 to raise money for the Samaritans. A fit and healthy runner, she collapsed and died a mile from the finishing line. Spontaneously, people donated to the JustGiving page that she had set up for the event. Over £1 million was raised in a short time. The Samaritans had to take care to stay with the spirit and tone of the fundraising that was happening as a result of the news story. The charity needed to be careful not to hijack the story to get their own message across. An 'in memoriam' fund within the charity allows them to use the funds raised for purposes that are fitting.

Example – Teenage Cancer Trust

Stephen Sutton was diagnosed with bowel cancer at the age of 15 and died in 2014 aged 19. Already actively involved in Teenage Cancer Trust and an ambassador for the charity, in 2013 Stephen wrote a bucket list of things we wanted to do. At the top of his list was to raise £10,000 for Teenage Cancer Trust. Stephen put a photo of himself on his Facebook page – his 'thumbs up' photo, which was picked up by some celebrity supporters of Teenage Cancer Trust and then went viral. Not only did Stephen raise millions for the charity, but it was an extraordinary opportunity for the charity to raise awareness and tell its story of how it helps young people with cancer.

Example – Meningitis Now

Early in 2016 the tragic story of Faye Burdett's death hit the news, after her parents shared images of their toddler on social media. The child had died from Meningitis B.

Younger babies are now given a vaccination against this strain of meningitis, but Faye had not qualified for the jab. Her parents started a petition which quickly gathered momentum. Sue Davie, chief executive of Meningitis Now, released statements to the press: "Although the introduction of the Men B vaccine on the childhood immunisation scheme for young babies was a momentous achievement, saving thousands of lives, there are still so many, like Faye, left unprotected. We continue to campaign to see the Men B vaccine rolled out, particularly to at-risk groups, to insure a future where no-one in the UK loses their life to meningitis."

While the charity would not have wanted to use a child's death themselves for promotion services, once the parents had started the campaign, it fitted well with the advocacy the charity was already undertaking. It also gave the charity an opportunity to raise awareness of the risks of meningitis.

Proactive responses to opportunities

Sometimes an event occurs which is entirely outside your control but which can be turned to your advantage. There are numerous examples of charity fundraising activities going viral such as the ice bucket challenge or the 'no make-up selfie'. It is impossible to know which campaign might go viral and it is not limited to fundraising. Some charities have successfully turned news stories into opportunities to tell people more about what they do.

"If you are going to properly manage the risk, then you need to consider building up your reputation capital."

Reputational risk response plan
In addition to working on building up positive perceptions, you need to be prepared for negative PR events or negative coverage of your organisation. Developing and testing a response plan is similar to a business continuity plan.

- You need to decide what sorts of events will trigger the response plan. For example, a minor story in a local paper may not be enough if you are a national charity, but it may be enough to trigger a response if you are a local charity.
- The plan should be clear on the roles and responsibilities. This is the value of testing the plan as gaps in understanding may surface.
- Who will be your spokesperson? If you need to provide a comment, it often needs to be rapid and the person needs to be properly briefed. If the spokesperson is too junior, the media may interpret this as an organisation not taking the matter seriously. On the other hand, you do not want to put a senior person such as the chair in an awkward position if they do not have all the facts and figures at their fingertips. You may also want to have different people nominated for different types of situations.
- Since a situation can blow up quickly, it is a good idea to have a second person named as the 'understudy' as finding someone and briefing them quickly might be difficult.
- Internal communications are just as important in a response plan. Board members, staff and volunteers need to know that you have a situation under control if they start seeing media coverage.
- Different types of incidents may need different responses, so you may need to think through a few scenarios. The purpose of a response plan is that you have thought through in advance what actions you will take, even when this is nothing.

The response plans need to be communicated to all relevant personnel including board members and kept up to date with regular reviews.

Some organisations run a full test of their response plan by creating a fictitious event and then seeing how everyone in the organisation deals with it. Only a few people know that it is a test so it makes it close to the real thing. The review after the event is important to make sure that you get all feedback and can implement changes to the plan.

It's about culture
It is mostly about culture. If an organisation lives its values then the behaviour and decisions will reflect this. In the section on assurance activities, we considered how organisations need to confirm compliance with values and codes of practice. Reputational risk lies in the gap between what you say and what you do.

Innovation and opportunities

Often the emphasis in risk management is the avoidance of hazard, but we also need risk management to encompass risk-taking. In an earlier section on the governance of risk, we stated that one of the roles of the board was to set the risk policy. This should describe where an organisation should be prepared to take risks as well as where it should be risk averse.

Risk-taking and innovation are not the opposite of risk management. Innovation does involve taking risks, but they should be managed risks. Not all risk-taking is good just because it is being done in the name of innovation. Equally, an organisation that takes no risks is unlikely to achieve its mission.

"New commissions are expensive, but if you start trying to play safe, you end up with a bland product no one will come to see. You have to allow a few of those new productions to fail. It's only by taking the greatest risks that you produce something amazing, such as War Horse or Matilda."

– Sally O'Neill, Chief Operating Officer, Royal Opera House, *Economia*, February 2015

A failure to grasp opportunities often appears on a strategic risk register. It is worth pausing to understand why that might be a risk and how a charity might apply risk management to innovation.

"Risk-taking and innovation are not the opposite of risk management."

Managing risk to innovate

Effective risk management should enable organisations to innovate and take risks. Good risk management processes mean that you understand the risks and weigh them carefully.

Having strong risk management processes in place and communicated through the organisation breeds confidence in taking risks. Regular reporting on risk and assurance processes allow the board to see how risks are being managed in the organisation, building confidence that the organisation can take on new activities.

"Discipline makes daring possible"

Dr Atul Gawande – 2014 Reith Lectures – *The Century of the System*

Gawande spends some time in one of his lectures discussing the possibilities that could be opened up to medicine if better systems were in place. A simple example he used – checklists help to ensure that no surgical instruments are left in the patient's body during an operation. Feeling secure that the simple things won't go wrong because a highly skilled nurse is keeping track, allows the surgeon to take more risks, such as trying out new procedures. What's stopping this happening? Mostly it is resistance on the part of doctors, who think they don't need checklists. What's needed is behaviour change, which is mostly about shifting the culture – 'how we do things around here'.

It also requires a change in emphasis away from a focus on downside risk and a change in mindset to embrace risk.

You need the right systems and culture in place to ensure that the organisation can innovate, secure in the knowledge that there are safety nets to catch you so you do not fall too far.

Systems

By systems, we do not necessarily mean prescribed procedures or IT – we are using the term in a loose sense to include a range of tools and reporting mechanisms that should be present in an organisation. These are not themselves recognised as risk management tools, but do help us to manage risks. We set out below some ways that might provide some helpful structure to enable your organisation to innovate.

Set up a development fund

Many organisations have found it useful to designate some funds for innovation and development. If your charity does not have unrestricted funds available, then you may be able to apply for development funds to take an idea forward. Some funders are interested in funding innovative ways of working with particular problems.

Like an external grant-making trust, you will need to develop the criteria for making awards from the development fund. As this is about innovation, you may want to have an early stage award of a small amount, scaling up the requirements and funding available if an idea does mature. It is not always cash that is required, of course, it may be time. But to release someone from other tasks may require back-filling their role. So this does still amount to cash.

In order to foster innovation, it's a good idea to make it easy for initial ideas to get a limited amount of support, but as the idea progresses through stages, it should be subject to increased scrutiny.

You also need to be clear about the risks of innovation both internally and externally. There can be risks in taking new ideas forward, but if there is clear communication about these risks and the reasons why new ideas are being pursued some of these risks can be reduced.

Piloting new ideas
Once an idea has reached a certain level of maturity, it may be ready to pilot. This should be treated like a project with a beginning, middle and end. At the end, there should be a proper evaluation of the pilot outcomes so that you can assess whether the pilot delivered the level of benefits expected. If it succeeded, it may be ready for the next level using a decision framework or a business case. These stages can be linked to ranges of financial and time commitment to provide directors with a degree of assurance that new activities are being explored in a controlled way.

Decision-making framework
For many innovation projects, this is about a risk/reward decision, so this is similar to commercial decisions. It's just that the reward is not always financial in the context of not-for-profit organisations. It can be useful to provide people with a framework so they understand what might be needed for a decision. An example is provided below, but you can adapt this to your own organisation.

Decision	Describe the decision to be made
Reason for decision	What change is needed? What is the problem you are trying to solve?
Benefits	Describe the main benefits anticipated from the change or decision. How will it contribute to the achievement of the strategic objectives?
Options	Set out the main options including the recommended solution – what are the pros and cons of each option?
Consultation	Who will this decision affect? What will be the impact on beneficiaries, staff, donors and others? Have you asked them about this decision or researched the effects on them? How might it affect other departments or teams?
Financial impact	How much initial funding will be required? What is the financial impact of this decision? How will it affect the longer-term finances of the organisation? Include summary financial forecasts, explaining the key assumptions you have made. You may include more detailed financial forecasts in the appendices.
Risk assessment	What are the risks involved? What are the consequences of them materialising? Do you have contingency plans to help you deal with these risks?
Plan	What is the timetable for any decisions and the major stages of this plan?

Full business case

A business case is a document that describes the need for change and projects that will enable the change. Implementing projects requires resources to be invested, including management and staff time and money. There are many competing demands on an organisation's resources and some projects may not be worth this effort. Documenting the need for change and how the change will be achieved in a business case provides senior managers and the board with information to evaluate the project and understand the impact the project will have on the organisation.

The business case also provides the framework for the approved project and organisations refer to it throughout the project when people suggest changes – typically to the scope of the project, timescale or costs. It is helpful to review and update the business case at key points to make sure that the reasons for the project are still valid and that it is achieving what it set out to do.

The format of a document setting out a business case can vary, and your organisation may have specific information requirements for decision-making, but if the following components are present, it will form a good basis for a collective decision.

Section	Purpose for decision-makers
Introduction	States the aim of the business case – the proposed change and purpose of the project
Reasons	Explains current issues and why the project is needed
Key outcomes and success criteria	Highlights the expected immediate and long-term benefits of the change
Options and costs	Outlines the main options for addressing the issues, including summary costs
Recommendation	Expands on and justifies the recommended solution

The following sections are written based on the recommendation

Impact analysis	Presents an assessment of the impact of the project on the organisation including financial and cultural impact, and an assessment of the organisation's capability and readiness to carry out the project
Risk assessment	Summarises the key risks and how they will be managed
Outline plan	Gives a high level plan of main activities, timescale and key decision points
Project governance and organisational standards	Shows how the project will be structured and levels of decision-making; also includes any standards that need to be considered

Portfolio of innovative ideas and opportunities

A commercial undertaking would not expect to succeed by publishing one book or running one training course. It's a similar story with innovation. To achieve success with innovation, you need to have many new ideas to increase the likelihood that one of them will be a success. Of course, this means that more of the ideas will be non-starters or will fail. It is not possible to predict the future and so you will not know which ideas will gain traction. This is so obvious with fundraising, particularly on social media. We have all been surprised by the success of seemingly random fundraising activities, such as the ice-bucket challenge. But this is in the nature of innovation and taking opportunities. If you have many more ideas at the early stages of innovation then you increase your chances of success.

Culture

New ideas will often come from frontline staff as they identify need and better ways of doing things. Therefore you need to have a culture that allows ideas to flourish. Suggestion boxes and other encouragement are the basic building blocks. Organisations that innovate well celebrate the people involved and their ideas when they are successful.

"To achieve success with innovation, you need to have many new ideas to increase the likelihood that one of them will be a success."

Risk culture

In all sectors – public, private and charity – it has become apparent that culture is a key force in driving the fortunes of entities. We have realised that good systems and controls are not enough to guarantee that nothing will go wrong. Anyone determined to get round the formal systems will not find it difficult. What is likely though is that the right culture in an organisation will help to foster the right behaviour and deter those interested in undermining it. For culture to be a powerful force for good, it needs to be prevalent and led from the top of the organisation.

What do we mean by culture? In this context, we mean the combination of attitudes and behaviour that is visible and characterises the 'way we do things around here'. One of the challenges for charities and not for profit organisations is that people join their organisation because they have a strong belief and commitment. That sounds like that should always be a good thing, and mostly it is, but it can go awry when the individual has a set of firmly-held beliefs that are slightly at odds with the organisation's values. This can lead to destructive behaviour, such as the long-standing employee who sabotages a change programme. This is part of risk management too, and you need to consider how people are likely to behave in different settings and how their personal risk attitude may set them at odds to the organisation.

How we develop our attitude to risk

We absorb sensory information such as sounds and visual images and this is processed by our brains. Our brains have to make sense of this sensory information. The first function of the brain is to check whether the new sensory information fits with anything already stored. Have I seen, heard, tasted, smelled or felt this before? Then a part of your brain will check whether this represents a threat or not. You may have experienced a sudden feeling of fear or anxiety – this is your amygdala firing as your brain is registering that there is a threat of some sort. And as many of you will recognise, this all happens in a flash, as you will know if you have ever experienced brain-freeze in an interview or similar.

Now, you may be wondering, what has this got to do with risk? Well, this sets the context for our own attitudes to risk. You will store the memory of that fear reaction to that situation. Next time a similar scenario starts to play out, your brain will check for previous similar experiences and you can find yourself involuntarily reacting to that new sensory information. You will have to make a big effort to intervene and make a change to what you say and do next. There is nothing to say that your unconscious reaction won't be correct. If you are driving and suddenly a cyclist swerves in front of you, it is likely that you will have a quick reaction to avoid the cyclist, which would be a good thing. It is not so much that the unconscious thinking is bad or that rational thought is better. It is more a matter of understanding that a large part of our behaviour is driven by past events and unconscious attitudes to risk.

Unconscious bias

Our attitude to risk can be affected by unconscious biases. By their very nature, we are unaware of them, so we need to be on the lookout for these, both in ourselves and in group situations.

Confirmation bias
We look for information that confirms an opinion we already hold. Unfortunately we are then likely to ignore evidence to the contrary. This will often be presented as a logical analysis.

In-group bias
We are social animals and our standing with our own 'tribe' is very important to us. We will experience positive feelings of well-being if we are in tune with our group, as oxytocin is released. The danger is we might be feeling good, but go along with a decision to avoid disturbing the sense of social well-being. It also has a flipside as we will then have marked others as the 'out group' and may be antagonistic to those in that group.

Gambler's fallacy
Calculating probabilities requires a lot of effort and uses a lot of energy, so we try to take shortcuts. We use past experience to make a quick and easy decision and often this serves us well. However, it might also lead us to make errors and we often misjudge the situation and ignore probability data. For example, if you ask a person to repeatedly guess whether a coin is going to fall heads or tails, they will start to infer that there is a greater probability for one or the other because of the way the coin has already fallen on a number of occasions. In fact, the probability remains 50% on every occasion.

"Our attitude to risk can be affected by unconscious biases."

Familiarity heuristic
This has been shown to have significant impact on the way we make decisions ("heuristic" here means shortcut). If you ask an amateur which football team is likely to win the league, they will probably just reach for the name of a team they have heard of. An expert would have a lot more data about the current team, the coach, the players off with injuries and recent performance. So the expert would take a lot more time to compute their answer. Ironically, they are not likely to be any more accurate in their prediction than the amateur. This is because the amateur picks the name of a famous team, and that team is likely to be famous because they have been so successful. So the familiarity heuristic can act as a shortcut to picking the best, but it will not always be successful.

Take a different example. Your charity needs to select a new computerised records system. You prepare a specification, drawing on the knowledge of the service delivery teams who will be using the systems. You undertake research into all the possible providers and you talk to some similar charities to find out what they use. You shortlist the suppliers and the decision will be made by a small panel, which now includes a couple of trustees. The panel has been provided with the background research and the proposals by the suppliers. When it comes to interviewing the suppliers, the trustees on the panel will be responsible for making the decision. It represents a major decision, so that has to be authorised by the trustees.

However, the trustees are busy people, so they have not had time to go through all the papers and they rely on the staff member who has undertaken this work. In fact, what is happening at the interview stage is that the trustees are probably using the familiarity heuristic and will choose the supplier they already know, or they have heard good things about. It won't necessarily be the wrong decision, but it is not based on all the research. Afterwards, when the decision is communicated, the charity will say that they went through a rigorous selection process. This may be true, but it was probably not the selection process that led them to the decision.

Availability heuristic
When making choices, we are also likely to use the 'availability heuristic'. This is another shortcut – we pick the option that is held in short-term memory. So we are more likely to pick an option that we recently considered as this comes to mind easily. It won't necessarily be the immediately recent option as we can hold a number of things in our working memory, but certainly our choices are influenced by recent conversations, reading and thoughts.

Choices are also affected by how much we like people. So in our example of selecting a supplier, the interview process will be heavily influenced by the likeability of the people presenting to the panel.

In summary, we like to think that we are making entirely rational decisions, but this is not true. We are driven by unconscious biases as well. And the whole point is that they are unconscious, so we need to think about ways in which we can counter their effect.

Six thinking hats of Edward de Bono

One the ways in which we can tackle the problem of inappropriate unconscious bias is by bringing this into consciousness. Techniques such as the 'Six Thinking Hats' and the 'Thinking Environment' may help to achieve this.

You might be able to counter some of the effects of unconscious bias and group behaviour by using a method introduced by Edward de Bono called the Six Thinking Hats. The idea behind the methodology is that it will bring into conscious thought different aspects of the issues being considered. Each hat represents a different way of thinking:

Colour	Way of thinking	Questions you should be asking
White	Information	What are the facts? What else do we need to know?
Red	Feelings	How do I feel about this? How do you feel about this? How will other people feel about this?
Yellow	Benefits	What is the upside? What will this help us to achieve?
Black	Risks	What could go wrong here? Are there opportunities we are missing? Have we thought of everything?
Green	Ideas and creativity	What else could we do here? Could we do things completely differently?
Blue	Meta level	How well are we working together? Is this process working for us?

"You might be able to counter some of the effects of unconscious bias and group behaviour by using this method."

Experienced users of the system may have their own opinions on the best order in which to use the hats, but the recommended starting place is as follows.

How to use the 'Thinking Hats' within your organisation

When considering a specific problem or topic it is best to start with the WHITE hat as this allows all the background information to be presented and documented.

Once the problem or topic is fully defined then the RED hat is used to ask participants how they feel about the problem or situation. Participants' feelings are documented. The general tendency for a proportion of people in a meeting, at this stage, is to present the negative aspects of the problem or situation.

The next step is to use the YELLOW hat to capture the positive aspects of the problem or situation from all participants. This step is then followed with the BLACK hat when everyone considers the negative aspects of the problem or situation.

Next use the GREEN hat where everyone is encouraged to use creative thinking to overcome the negative issues but also develop new alternatives to solving the problems or resolving the situation. The RED hat is used again at this stage to gauge the feelings of participants.

Generally, most participants who were previously concerned about the problem or situation would now be feeling more positive after having gone through the process of using the different hats. Finally, it is always appropriate to use the BLUE hat as this allows participants to evaluate whether the process has offered solutions or conclusions. The BLUE hat also provides process control to ensure the right technique or approach was used by participants. If a solution or resolution was not identified then another approach or process would be suggested as more appropriate in solving the problem.

Thinking environment

Nancy Kline has developed a methodology which can be applied to meetings to make them more effective which is called the 'thinking environment'. There are ten components of a thinking environment which are:

Attention	We can help others to think well by giving them our full attention – no interruptions
Equality	Everyone is valued equally as a thinker. Everyone gets a turn to speak. Equality keeps the talkative people from silencing the quiet ones.
Ease	It is important not to rush people – it damages the quality of the thinking and often takes longer in the end.
Appreciation	We support each other's thinking by appreciating more than we criticise.
Encouragement	Replacing internal competition with wholehearted, unthreatened search for good ideas.
Feelings	Thinking stops when we are upset, but can start again if we are allowed to express enough of our feelings.
Information	Starting with accurate information is essential if good independent thinking is the aim.
Diversity	Making sure all opinions are represented – have the right people in the room.
Incisive questions	The power of an Incisive Question is that it can cut through assumptions and limiting beliefs.
Place	Creating the right environment that makes people welcome shows them respect.

A meeting run along these lines will have an agenda which states the items as questions. For example, a review of management information would be on the agenda in the form of a question such as, 'What actions does the latest management information prompt us to take?' The point is to provoke some thought before attendees arrive for the meeting. No one should be in any doubt that the meeting agenda items all require a contribution from every person present.

What does a good risk culture look like?

An effective risk culture is one that enables and rewards individuals and groups for taking appropriate risk. Much of what has been written about risk culture has focussed on the negative aspects of excessive risk-taking, particularly in the financial services industry. In fact, in the context of charities and not for profit organisations, it is equally important to ensure that the culture promotes appropriate risk-taking as some boards are seen as too risk averse. The reputation of the sector as a whole has been damaged by reports of aggressive fundraising techniques, sales of mailing lists and poor impact reporting. These are issues of risk culture which can be addressed by considering the ingredients that blend together to form a successful risk culture:

1. Values and ethical principles that support appropriate risk-taking.
2. A clear and consistent tone from the top. The board and senior managers need to live the values and lead by example.
3. Alignment of plans and budgets to the values. For example, you are unlikely to get the right behaviour if you agree an ethical code of fundraising but then send the message that the fundraising target is the priority.
4. Willingness to hear bad news. Sometimes staff know that a project or planned activity is unlikely to succeed but fear reporting it early as this can be seen as negativity or they worry that they will be blamed.
5. In the same vein, the organisation should convey to all staff and volunteers a willingness to learn from mistakes, using evaluations and project reviews constructively.
6. Whistleblowing should be easy, with a clear policy and procedures so all staff and volunteers know when it is appropriate to use whistleblowing and how to do it. Most staff will find it difficult to overcome a social bond they will have formed with fellow workers, so they will be reluctant to speak out at first.
7. Swift and fair disciplinary procedures to deal with poor behaviour, bad service, theft, breach of the organisation's rules and abuse will convey a strong message to staff. It is important that there is no favouritism and that you act consistently.
8. Rewarding the right behaviour. In not-for-profit organisations, there will not generally be a bonus or other financial reward, but there are other ways of rewarding staff. For example, promotion or special mentions in newsletters.
9. Appropriate attitudes among all staff and volunteers as reflected through staff surveys and behaviour to make sure that the values and ethical behaviour is reinforced.
10. Diversity of views among board members and staff to ensure that inappropriate risk attitudes or behaviour are challenged.

Culture in an organisation is both the result of the behaviours and attitudes of the people in the organisation and the influence on those people. It can easily become a self-reinforcing cycle, which may be a virtuous circle or a vicious circle. Much of culture is intangible and therefore has to be handled carefully.

Gerry Johnson wrote about the 'cultural web' which is a combination of six components, some of which are visible and some of whose elements are less obvious.

Stories
The past events and people talked about inside and outside the organisation.

Symbols
The visual representation such as logos, styling of offices and dress code.

Power structures
The pockets of real power. This may be one or two key senior executives, a whole group of executives, or even a department.

Organisational structures
This includes both the structure defined by the organisation chart and the unwritten lines of power and influence.

Control systems
The ways that the organisation is controlled. These include policies, financial systems, quality systems, and rewards.

Rituals and routines
The daily behaviour and actions of people that signal what is expected to happen in given situations.

Stories are incredibly important, and you only have to listen to the talk when you first start work in a new organisation to get a feel for who the heroes are, what actually gets rewarded or noticed, who really holds the power and what the appropriate behaviours are. We all have to learn this when we start in a new setting, and we are extremely adept at it. We are, after all, social creatures!

Our survey said...

Sayer Vincent and CFG carried out a small survey of attendees at CFG's Risk Conference in November 2015. Here are some of the responses on how organisations were embedding risk management:

- *"Through communication rather than training"*
- *"[We are] dependent on a few key people."*
- *"Still planning that!"*
- *"Often not at all. Risk strategy usually an afterthought of the organisational strategy."*
- *"Risk is considered but needs better alignment."*
- *"Risk strategy is formulated by the same people that formulate the organisational strategy."*
- *"Strategic thinking takes risk into account [but] could work more closely… 'reserves' often understood as financial resources, not people, capability, office space etc."*

Changing the risk culture of an organisation

First, the board needs to understand the current risk culture of the organisation, then decide what they want it to be. They can then focus on moving from where the organisation is to where they want it to be. Points to consider in their review:

- Consider whether the organisation ever condones or ignores inappropriate risk-taking or risk averse behaviour
- Challenge box-ticking approaches to risk management
- Is the achievement of the organisation's strategic objectives jeopardised by risk-averse behaviour?
- Do you have a preponderance of a certain personality type e.g. if everyone employed has a strong adherence to rules, then the organisation may have difficulty innovating or being creative.
- When recruiting new staff, do you consider whether greater diversity is needed in terms of personality types?
- Is the risk policy communicated effectively?

The board and senior management team can then work with some of the tools set out above which are described by Johnson as the 'cultural web'. It is particularly important to relate stories to positively position the behaviour you want, create the rituals you want and base them on policies and procedures that form a consistent whole.

"It is particularly important to relate stories to positively position the behaviour you want."

Assessing the health of your risk culture

The Institute of Risk Management has created a 'Risk culture aspects model' which is reproduced below:

The above model is designed as a self-assessment tool to provide the board with insight into the eight key indicators of the health of a risk culture. Diagnosis can be by means of a simple questionnaire or structured interviews. This will provide pointers to areas of strength and weakness to allow prioritisation for plans and actions.

Case Study – Amnesty International UK

A challenge for Amnesty International has been moving the organisation to think of risk more from the bottom up rather than top down, and ensuring managers are allocated the time to develop risk management approaches within their teams. Amnesty conducted a series of workshops and meetings to enable managers to take some hours out of the day to talk about risk within their teams. For a lot of managers it was a learning curve, as previously it was only the senior management team that assessed the risk register. There were some challenges in getting staff to a place where they understood and were confident about the approach, especially given the need for individual teams to have their own risk assessments and score them.

Amnesty has also decided to undertake a 'deep dive' into different risk areas at board meetings. For example, talking about reputational risk with the crisis response communications group. For each topic there is considerable preparation work done exploring what the risk is and how Amnesty would respond. While this has not always resulted in an engaged response from the board, it was still effective because it highlighted for senior leaders the areas not getting board level engagement.

Conclusion

One of the themes we have returned to again and again throughout this publication is that risk management is an integral part of management. It is how you would define management. Risk management offers a set of tools for the ordinary manager that they can use as they go about their job.

The first of these tools is to think of risks in three broad categories of project risks, operational risks and strategic risks. This facilitates productive thinking about the actions you need to take to manage risks and it ensures that managers at an appropriate level have responsibility for risk.

The challenge in risk management is to communicate effectively how risks should be managed and are being managed. Risk registers should be part of this system, but they often fall short. We need to remember the presence of a risk on a risk register does not mean that it is being managed. Bringing risk registers to life with better processes and better presentation can improve their use.

At a board level, the major risk issues are the big picture areas, such as the level of risk inherent in the business model, the risk policy for the organisation and ensuring that appropriate risk management processes are established. The board needs assurance that the risks are then being managed effectively in practice. Keeping a focus on the strategic risks, the board can rely on many of the normal management processes and reports to gain knowledge of how these risks are being managed. This is another demonstration of the integrated risk management approach. Boards may need more evidence of good practice, quality, compliance and this can be provided through various levels of internal audit and good controls.

Another theme running through this publication has been the importance of culture in an organisation. It is not enough to state values – the whole organisation needs to live those values. The success of every organisation depends on it. A positive culture in an organisation with appropriate attitudes to risk is likely to ensure it achieves its strategic goals and enjoys a good reputation.

Finally, risk management is not about avoiding risk – it is about taking risks, but in a managed way. It is the duty of charity trustees and staff to make sure that they do this effectively and in the best interests of their beneficiaries.

“Risk management is not about avoiding risk – it is about taking risks, but in a managed way.”

Acknowledgements

The authors would like to thank all the contributors to this publication. On the CFG team: Andrew O'Brien helped to shape the whole publication, steered the project and provided helpful comments. Heather McLoughlin undertook the interviews and prepared the case studies. Kelly Ventress edited and oversaw the design and production of the publication.

We are grateful to the following for providing case studies:

- Rob Ovens, Finance Director at The Challenge Network
- Eliot Lyne, Interim Director of Finance at Amnesty International UK
- Gaynor Miller, Head of Internal Audit & Risk Management at Christian Aid
- Gary Lashko, Chair of the Board of Trustees and Company Directors at Revolving Doors
- Mindy Kilby, Director of Finance at The Royal Opera House

Authors

Kate Sayer, Partner, Sayer Vincent LLP

Judith Miller, Partner, Sayer Vincent LLP

Jonathan Orchard, Partner, Sayer Vincent LLP

Arlene Clapham, Risk and Assurance Manager, Sayer Vincent LLP

Charity Finance Group

Charity Finance Group (CFG) is the charity that champions best practice in finance management in the charity and voluntary sector. Our vision is of a financially confident, dynamic and trustworthy charity sector. With this aim in sight, CFG delivers services to its charity members and the sector at large which enable those with financial responsibility to develop and adopt best practice.

With more than 1350 charities in membership, managing over £21 billion, we are uniquely placed to actively shape policy and legislation, drive efficiency and help charities to make the most out of their money.

Sayer Vincent LLP

Sayer Vincent is an award-winning firm of chartered accountants with a clear focus on charities and social enterprises. We aim to help social purpose organisations become more effective and want them to be able to deliver more for their beneficiaries. Our reputation is built on an established track record of delivering value for our clients and providing a personal service.

We are an ethical firm that bases all its decisions and the way it operates on the fundamental principle that people are more important than money.

www.sayervincent.co.uk

Resources

Charity Commission Guidance

The below can all be downloaded from **www.gov.uk/topic/running-charity**.

- CC8 Internal financial controls for charities (July 2012)
- CC19 Charity reserves: building resilience (January 2016)
- CC26 Charities and risk management (June 2010)
- CC49 Charities and insurance (May 2012)
- Charities SORP (FRS 102)

CFG and Sayer Vincent

- Beyond reserves (2012), available from **http://bit.ly/beyondreserves**.

The Institute of Risk Management (IRM)

Visit **www.theirm.org** to access all of the below IRM resources.

- Risk management standard (2002)
- Risk culture: under the microscope – Guidance for boards (2012)
- Risk culture: resources for practitioners (2012)
- Risk appetite – guidance paper (2011)

Institute of Business Ethics

A large number of surveys, briefing papers and other publications on relevant topics can be found at **www.ibe.org.uk**.

Thought provoking books and papers

- *Intelligent Internal Control and Risk Management*, Matthew Leitch, 2008
- *Governance and Management of Charities*, Andrew Hind, 1995
- *The Three Lines of Defense,* Position paper from the US Institute of Internal Auditors, 2013
- *Managing Reputational Risk,* Jenny Rayner, 2003
- *Reputation and its Risks*, Robert G. Eccles, Scott C. Newquist and Roland Schatz, Harvard Business Review, February 2007
- *Six Thinking Hats*, Edward de Bono, 1985
- *Time to think*, Nancy Kline, 1999

Charity Finance Group

15–18 White Lion Street
London N1 9PG

info@cfg.org.uk
www.cfg.org.uk
T: 08453453192

Registered charity no. 1054914
Company no. 3182826