

Fresh ways to approach risk management

When it was first introduced, the process of assessing risks had real benefits. It helped to prioritise management actions and involved trustees in key strategic thinking. However, several years on, organisations are reporting that they are still finding it difficult to embed risk management. So it may be that your organisation needs to refresh its approach.

Traditional approaches

In most cases, senior managers and trustees build up a long list of possible risks and then rank them for likelihood and impact. The prioritised list becomes the risk register, and managers plan actions to mitigate the effects or reduce the likelihood of an event happening. A typical risk register might look like this, at least to start with:

		likelihood	impact	ranking
1.1	Trustee scandal damages reputation	3	5	15
1.2	Fire	1	5	5
1.3	Data protection violation	3	4	12

So what are the drawbacks to this approach?

- 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 such as “fire” 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
- Whether you use numbers or “high, medium and low” you will still have the problem that one person’s view of what is high risk is different to the next person’s view. Therefore you may not be talking the same language.
- This approach feeds the misapprehension that risk assessment 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 aim of risk assessment

The aim should be to gain an understanding of the risks the organisation faces so that everyone is able to respond to unforeseen or unplanned events more quickly and more appropriately. Our ability to respond will be enhanced if we have thought about similar situations together, rehearsed what we would do if certain events happened. It is actually not likely that real life will reproduce exactly our imagined scenario, but evidence does show that teams that work through scenarios respond more quickly and effectively when real events take them by surprise. So the real purpose of risk assessment exercises is “risk readiness”.

Risk appetite

You need to develop a common understanding across the organisation about the levels of risk that you are prepared to take in different parts of your operation. It is particularly important the

understanding is shared between the trustees and the managers of the organisation. Signs that there are differences in risk appetite will be that proposals put forward by managers are challenged or that conflicts are apparent. For example, the trustees may be asking questions when they receive a monitoring report on an ongoing activity that reveal that they have not “bought in” to the underlying concept and plan.

Your risk appetite will not be the same for all areas. For example, you would probably have a zero tolerance attitude to child protection issues, but you might be risk-taking in new fundraising activities. It also has to be a corporate view, rather than an amalgam of individuals’ views. Developing a discussion about the levels of risk you would be prepared to take in different situations will enable you to explain the organisation’s risk appetite in a risk policy. This then provides the context for assessing risks.

Strategic risks

You can avoid preparing the long list of risks and go straight to the main risks facing the organisation at a strategic level. The trustees and senior managers should be focusing on these risks and spending more time considering how they will manage those risks. These are likely to be the big issues such as reputational risk, or the risk that the organisation will fail to deliver on a major strategic aim. They are also likely to be *external* issues which you cannot control and therefore have to consider how you will respond to them if they happen. A good risk assessment process will analyse these risks to get to the root cause and then consider appropriate management responses.

This does not mean that you ignore the operational risks altogether – it just means that these are dealt with at a different level. You should resist the temptation to develop detailed risk registers at the operational level and then add these all together, imagining that you will therefore capture every possible risk. This has been shown to fail on many occasions. Strategic risk and operational risk are different, and the responsibility for managing them is different. This is not to say that one should not *inform* the other, but good time can be wasted trying to make them fit together. They are different perspectives on the organisation and best undertaken separately.

Assessing and managing operational risks – focus on *uncertainty*

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

We should change the focus. Firstly, we can ask managers to consider the *uncertainty* in their plans and activities. This will help to draw out the upside risk and opportunities as well as simply thinking about things that could go wrong. For example, a manager planning a training event can identify that the key area of uncertainty is the number of people wishing to attend the training – there may be too few or too many for the venue. This is a *risk driver*. It may be worth the effort to then undertake more research to find out the likely numbers of people who will be interested.

Risk management can become more integrated with the rest of the planning and performance management processes of the organisation. Having developed an overall strategy, the organisation needs to consider how it will implement the strategy - developing actions and activities that you believe will deliver the desired outcomes. However, plans contain inherent uncertainty. All plans are based on a series of estimates and assumptions. We need to understand the possible variations and work out how we will monitor those so that we can respond effectively.

Mapping controls to manage operational risks

Risk registers usually show the identified risk and the control measures in place or actions to close control gaps. In practice, one control may apply to several risks. So reverse the process by thinking about the procedures and processes you have in place, then consider the risks that they are helping you to manage.

	Risk A	Risk B	Risk C	Risk D
Procedures # 1				
Procedures # 2				
Procedure # 3				

For example, if might be considering our recruitment process. We have a procedure in place to obtain two references from previous employers. Why do we have that procedure? The main risk it is helping us to manage is that we may make a poor decision in selection. We might have also thought that it helps us to manage child protection risk, but in reviewing the process, we realise that the right questions are not asked in the reference request letter. So we are not managing that risk as well as we thought. However, we also establish that we generally have two formal interviews and an informal interview involving several different staff. We decide that this is not increasing our level of risk management, simply taking up time repeating the same process several times. So the interview process will be streamlined and the reference process augmented.

This example shows that managers’ awareness of why they are undertaking certain procedures is increased by this approach. It will help them to improve processes and risk management activity.

Portfolio of controls

This approach works best when controls are viewed as a portfolio – the aim is to ensure that you have a balance between different types of controls.

<p>Aims and objectives – a clear understanding by staff and volunteers on the strategic direction of the organisation and at an operational level, of the objectives of their department and the particular initiative they are working on.</p>	<p>Direct controls – traditional control activity such as reconciliations, and segregation of duties, written procedures.</p>
<p>Planning – converting strategic plans into workplans for departments, teams and individuals. Also that there are contingency plans in the event of certain risks crystallising, such as disaster recovery plans and fraud response plans.</p>	<p>Monitoring – continuously reviewing whether the actions and initiatives being undertaken are achieving the desired outputs and outcomes. Key performance indicators tracked over a period of time and external benchmarking are all ways in which the charity can measure its performance.</p>
<p>Accountability - ensuring that job descriptions and appraisals are consistent with plans and objectives, and that individuals are clear on their roles and responsibilities. The line management should support accountability as should the corporate governance structure through to the trustees.</p>	<p>Employee welfare – good morale and highly motivated staff increase the chances of successful outcomes, where disgruntled staff present a range of risks to an organisation.</p>

<p>Training and competency framework – ensuring that staff and volunteers are competent to do the job expected of them, strongly linked to the strategic plans. This means looking at how the strategy should be implemented and what skills are needed to implement it.</p>	<p>Independent review – external and internal audit, regulatory inspections and Charity Commission visits – all are an opportunity for the charity to learn and improve.</p>
---	---

Looking at controls and the risks they help to manage should deepen the understanding managers have of risk management and provide new perspectives.

Becoming a *risk-enabled* organisation

Focusing on the strategic risks is more likely to achieve a greater depth of understanding of the risk *drivers*. These may be internal or external, and your response will be different depending on which they are. The likelihood of internal risks can be changed by management action and controls, if this is required. However, there some external risks you cannot prevent occurring, so the emphasis should be on mitigating the impact. Thinking in advance about how you would respond if an external risk materialises may be an excellent opportunity to develop a more generic response mechanism. *Risk-enabled* organisations are not afraid of taking risks, but they have thought through the consequences and developed contingency plans for various outcomes that may occur. In these circumstances, your organisation is better able to handle unforeseen events.