# Risk assessment

## made simple

July 2015

SAYER | VINCENT

Sayer Vincent LLP

Chartered accountants
and statutory auditors

Invicta House
108–114 Golden Lane
London EC1Y 0TL

Offices in London, Bristol and Birmingham

020 7841 6360

svinfo@sayervincent.co.uk
www.sayervincent.co.uk
@sayervincent

SAYER | VINCENT

Published by Sayer Vincent LLP

Chartered accountants and statutory auditors

Limited liability partnership registered in England and Wales
OC390403



www.platform1design.com

# Introduction

Everyone thinks about risks and weighs them in their mind when they are making decisions or planning, but a *risk management process* is a structured approach providing consistency across the whole organisation.

Risk *assessment* is the first step in the process. The approach we suggest here provides a framework to share common understanding within the organisation and a tool for the prioritisation of management decision-making. It will help you to recognise existing control activity that is managing risks and identifying gaps where you need to do more.

Your organisation can then integrate risk assessment and the management of risks as part of planning, monitoring and performance management.

## Step 1 *Identifying the risks*

Risk can be defined as uncertainties surrounding opportunities and threats which have the potential to enhance or inhibit performance, the achievement of objectives and meeting stakeholder expectations. In other words, a risk can be anything which has the potential to prevent you reaching your goal. For charities and organisations, it can be very helpful if the risk identification process is rooted in the objectives of the charity. However, risk is also about taking appropriate risks to achieve objectives and should be about identifying opportunities as well as negative risks.

Starting from the charity's objectives, the charity should think about the risks, which might prevent the charity from achieving those objectives. This will produce a "top level" review of risks, looking at the overall scene both inside the charity and externally.

As prompts for identifying risks, it may be helpful to think in terms of:

- Failure to…
- Loss of…
- Concentration of…
- Non-compliance with…
- Lack of…
- Reduction of…
- Conflict between…
- Inability to…
- Inappropriate…
- Reliance on…
- Disruption to…
- Inadequate…
- Increase in…
- Delay in…

For example, the loss of funding from a major donor would pose a significant threat to the continuation of the charity's work in a particular field.

In generating the list of risks, it is important to consider threats **and** the consequence of the threat materialising. If it were identified that the charity is reliant on funding from one source, then that in itself does not articulate a risk. It is necessary to consider the consequences of that particular aspect. For this example, the risk may be that the funder is able to specify the purpose on which the funds should be spent, which in turn is taking the charity in a direction that is not well matched to the strategic direction it has chosen.

When thinking about risks, it is important to develop an understanding of the root cause. In most cases, loss of funding is not the risk, but the consequence. The root cause might be a breakdown in the relationship with the funders, or a change in their priorities. Thus, you may initially brainstorm a list of risks, but then refine it as you develop your thinking about causes and consequences.

## Categories of risk

When identifying risks, you need to think widely about internal and external factors that could affect the charity. The major risks to the charity are not likely to be only financial risks. Consider the following categories and examples of the risks that commonly arise:

| | |
|---|---|
| People | • key personnel leaving<br>• inability to recruit |
| Operational | • lack of clear plans<br>• lack of budgetary control |
| Financial | • authority levels not communicated<br>• poor segregation of duties |
| Strategic | • lack of focus<br>• too little knowledge about the group you serve |
| Funding | • short term<br>• poor cost recovery |
| Competition | • other charities raising funds for the same thing<br>• your idea being 'mainstreamed' so you are no longer relevant |
| Management | • inappropriate structure<br>• staff do not know where to go for a decision |
| Information | • too little information about your outcomes so you cannot demonstrate effectiveness<br>• data is scattered through the organisation in many different databases |
| Property | • reserves tied up in property you no longer need<br>• high level of dilapidations on leases |
| Reputation | • an accident involving a user<br>• confidential information about users is accidentally in public domain |
| Regulatory | • charity losing employment tribunal because procedures were not followed<br>• breach of data protection regulations |
| Technological | • old database no longer supported by supplier<br>• failure to meet the expectation of users in terms of response times and availability of information and services electronically |
| Political | • change in political priorities leading to cut in funding<br>• change in policy affecting beneficiary group making your charity irrelevant |
| Governance | • conflict of interest for a member of the board<br>• lack of requisite skills on board |
| Natural | • flood |

# Step 2 *Assessing the risks*

It is very likely that there will be an extensive list of identified risks, so the risks need to be assessed. The key factors are:

- likelihood
- impact

Likelihood refers to the probability that a threat will materialise. Impact relates to the effect that would be felt if the event did occur. Likelihood and impact are the common factors seen in all descriptions of risk assessment. A scoring system should be agreed. One system is:

## 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 | possible 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 |

The impact for an organisation can be difficult to assess. Often the financial impact can be assessed as the cost of putting something right, alternative action, or the financial penalty. However, reputational impact may be more significant and harder to assess. For example, fraud might cause a small financial loss, but the effect on a charity's reputation might be much greater. If you wish, you can create two measures for your worksheet to collect scores on financial impact and reputational impact.

## Risk appetite

This is not an objective process; it is subjective and each person will come to different conclusions about the perception of a particular risk. Undertaking this as a collective exercise will focus the organisation's attention on a key issue: *risk appetite*. One person might score a potential event as low likelihood, whereas another person may perceive the risk as highly likely. The process of assessing the risks can be a very positive exercise in sharing the different perceptions of risk. As part of the process the organisation should come to a reasonable consensus about the level and types of risks it is prepared to accept.

To reflect this, it can be helpful to use a third measure, which is usually called "attitude". This is way of drawing out people's perceptions about a particular risk, and the additional scoring will weight the priority ranking to risks that receive a high score on level of concern as well as likelihood and impact.

## Attitude

| | | |
|---|---|---|
| 5 | Zero tolerance | where the nature or impact of the risk is such that it is not acceptable within the organisation |
| 4 | Risk averse | where some risk is unavoidable but this should be kept to a minimum |
| 3 | Risk equilibrium | where the dangers of the risk are fairly evenly offset by the opportunities and advantages offered by carrying it |
| 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 |
| 1 | Risk bearing | where the potential benefits of taking the risk are significant against the likelihood and impact of the risk which are limited |

You can use worksheets in a format such as the one below to develop your list of risks and assess them:

| Risk | Consequence | Likelihood | Impact | Attitude | Priority ranking |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

Multiply the scores to produce the priority ranking.

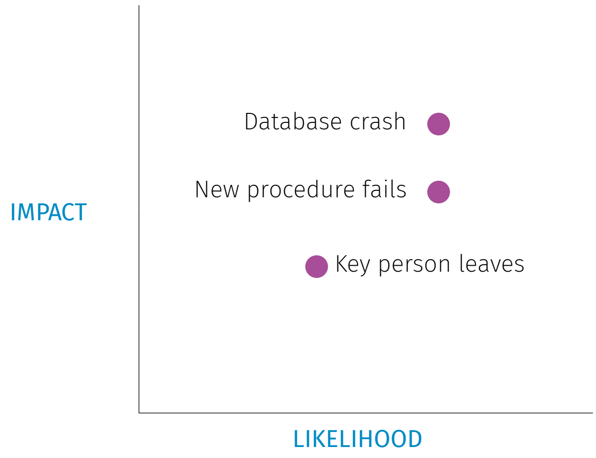
| | Likelihood | Impact | Attitude | Priority ranking |
|---|---|---|---|---|
| Database crash | 4 | 4 | 4 | 64 |
| Key person leaves | 3 | 2 | 2 | 12 |
| New procedure fails | 4 | 3 | 3 | 36 |

Using these factors you can prioritise the risks, so that the long list becomes more manageable. The focus moves to the risks with the highest ranking.
You can map the scores for likelihood and impact onto a grid format to organise and prioritise the risks:

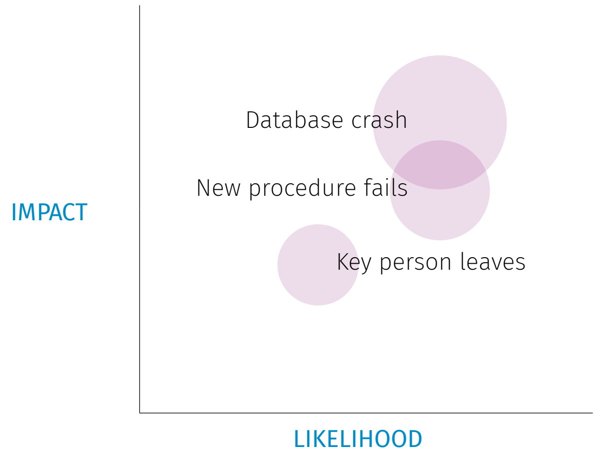
## A risk map

| IMPACT | | |
|---|---|---|
| | high impact<br>low likelihood | high impact<br>high likelihood |
| | low impact<br>low likelihood | low impact<br>high likelihood |
| | LIKELIHOOD | |

You can also prepare your map as a scattergram to provide a graphic illustration of key areas of risk. As an example, the above table showing the prioritised risks would be illustrated on such a map as follows:




In order to include the attitude ranking, you may choose to draw a risk map as a bubble diagram, where the size of the bubbles reflect the rating for attitude.



# Step 3 *Establishing action points*

Appropriate action will depend on the nature of the risk. Consider the following actions as responses to risk:

- Avoid the activity
- Minimise the likelihood e.g. improve your procedures
- Mitigate the effects e.g. develop a response plan
- Transfer the risk e.g. by taking out insurance
- Accept the risk i.e. continue in same way in the knowledge that there are risks

In general terms, the appropriate actions for the four quadrants on the risk map are:

### Suggested actions

| IMPACT | | |
|---|---|---|
| | high impact<br>low likelihood<br>**Mitigate effects/ transfer** | high impact<br>high likelihood<br>**Avoid/minimise likelihood** |
| | low impact<br>low likelihood<br>**Accept** | low impact<br>high likelihood<br>**Minimise likelihood/accept** |

LIKELIHOOD

Where the likelihood is high for an internal risk, then the charity can take action to minimise the likelihood. Where the likelihood is high for an external risk, then there is little the charity can do to prevent the threat materialising. The charity therefore has to consider whether it can manage the situation if the event did happen i.e. mitigate the effects of an event, or whether it has to cease the activity to avoid the risk altogether.

The charity will also have to consider a level of risk which is it prepared to accept. If the risks are known and managed, then this is a good outcome for the charity. In this situation, no further action may be required.

The charity will also need to balance the cost of controlling the risk against the cost of mitigating the risk should the threat materialise. The cost of controls need to be proportionate to the risk and the aim is not to eliminate all risks, but to manage them.

It is important to identify the appropriate actions to manage risks so that effort is directed in the right way. It is better therefore to first consider what the controls ought to be and then to check what you have in place. An example of a format you can use for this:

| Risk | Likelihood | Impact | Appropriate controls | Existing controls | Further action needed |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Step 4 *Develop a risk register*

A register draws together the key information for the highest priority risks:

- Clear identification of the risk.
- Consequences of that risk becoming a reality.
- Action required to manage the risk – the controls appropriate for the risks identified.
- Describe the controls already in place.
- Further action required, identifying the timescale and responsibility for the action. This will then need to be monitored.

This risk register should be shared with the full trustee board. Although a committee may take the lead on the risk management process, the whole board should be aware of the highest ranked risks. The management team should be able to explain the actions being taken to manage those risks.

### Example page in a risk register

<table>
<tr><th>Risk</th><th colspan="3">Consequences</th></tr>
<tr><td>Database containing names of all members will crash</td><td colspan="3">• Loss of income<br>• Damage to relationship with members</td></tr>
<tr><th>Appropriate controls to manage the risk:</th><th colspan="3">Existing controls in place:</th></tr>
<tr><td>• Database backed up daily<br>• Back ups stored off-site<br>• Restore of data tested monthly</td><td colspan="3">Daily back-up system in place</td></tr>
<tr><th colspan="2">Further actions necessary</th><th>Who</th><th>Timescale</th></tr>
<tr><td colspan="2">• Ensure contract with IT support company is valid and provides for immediate action</td><td>TY</td><td>Urgent</td></tr>
<tr><td colspan="2">• Provide training for membership team</td><td>ST</td><td>Medium term</td></tr>
</table>

## Step 5 *Monitoring and reassessment*

Regular review will ensure that the trustees and management are aware of the current risks facing the charity. These will change, as will the extent of exposure to them.

The wider risk register needs to be reviewed regularly. For most charities this will be at least annually, but this should be more frequent in a period of change. It is useful to report changes in assessed risks. For example, has the perceived likelihood of a risk increased or decreased? Some organisations incorporate a simple arrow symbol into their report to show the direction of change.

Audit committees should monitor whether planned actions to manage risk have been completed. You should also consider whether the management actions do actually produce the desired effect. In larger organisations, internal audit will have a role in assessing the effective of policies and procedures to manage risk.

In order to reap the benefits of this process, risk review needs to be brought into the cyclical planning process of the charity and be embedded within the processes of the charity.

Consider how you might review the risk profile of a new strategic plan. Additionally, risk review needs to be brought into the operational plan and work plans for teams. You may need to add a responsibility for undertaking regular risk assessments into job descriptions and ensure that it is included in the objectives for managers. There may be quite simple ways in which an understanding of risks can be brought into all aspects of operational decisions, such as including a short risk review on forms for new activities and planning documentation.

# Conclusion

Once your charity has an established risk assessment process, you will be well on the way to managing risk as an integral part of the governance and management of the charity.

The benefits of risk assessment processes include:

- A structured way of dealing with current and future risks.
- Creating the right culture so that the organisation can learn from mistakes and take advantage of opportunities.
- Helping to focus decision-making and actions on the priority issues for the organisation emanating from the objectives.
- Involving individuals at different levels in the organisation and promote greater understanding of the objectives and strategy.

# Further information

## Charity Commission

### How to manage risks in your charity

www.gov.uk/how-to-manage-risks-in-your-charity

### Charities and risk management (CC26)

www.gov.uk/government/publications/charities-and-risk-management-cc26

## NCVO – KnowHow NonProfit

### Risk assessment toolkit

http://knowhownonprofit.org/studyzone/how-to-carry-out-a-risk-assessment-1?gclid=CN_sjOPJlbYCFW_KtAodZBQAmA

## The Institute of Risk Management

### Various guidance in their knowledge and resources section

www.theirm.org

# Notes

## Made simple guides

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


## Made to measure

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

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

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

For more information, go to www.sayervincent.co.uk

SAYER | VINCENT