irm

Risk management for charities

Getting started: supplementary guidance

Version 2.0

About IRM

IRM is the leading professional body for risk management. We are an independent, not-for-profit organisation that champions excellence in managing risk to improve organisational performance.

We do this by providing internationally recognised qualifications and training, publishing research and guidance and raising professional standards across the world. Our members work in all industries, in all risk disciplines and across the public, private and not-for-profit sectors.

IRM does not accept any liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly, whether in contract, tort or otherwise from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.

Registered Office: 2nd Floor, Sackville House,
143-149 Fenchurch Street, London, EC3M 6BN

T – +44 (0)20 7709 9808
E – enquiries@theirm.org
W – www.theirm.org

Foreword

Risk management is something that we probably all know we are supposed to do but too often it is seen as a complex scientific discipline; something that is done by highly qualified experts sitting in ivory towers. Or worse, a bureaucratic waste of time.

Nothing could be further from the truth. Risk management is something we all do without thinking in our everyday lives. Why do we look both ways before we cross the road? Because we're managing the risk that we might be run over by a car that's going too fast and fails to stop in time. If that happens we won't achieve our implicit objective of reaching the other side of the road in one piece. So a lot of this is second nature or common sense based.

We need to bring that kind of thinking to the workplace but we recognise it can be difficult to know where to start. The IRM's Charities Special Interest Group has created this guidance to help charities of all sizes make sense of risk management. The guidance is based on the approach set out in ISO 31000 and is entirely consistent with Charity Commission requirements.

This guidance supplements our leaflet, 'Getting started' and provides more detail on how to develop risk management in your charity.

Our authors

Originally in 2014 this guidance was produced by members of the IRM Charities Special Interest Group, principally:
Rebecca Bowry, Diabetes UK (now retired)
Alyson Pepperill CFIRM, Gallagher
Version 2.0 has been updated by Alyson Pepperill in 2018.

This guidance covers the following areas:

How to set up your risk management framework

We'll assume that you've read our leaflet on getting started with risk management so you have some idea of what it's all about. Now you can decide how best to implement it in your charity.

The charity's trustees have ultimate responsibility for risk and are expected to regularly review and assess the risks faced by their charity in all areas of its work and plan for the management of those risks. There is a legal requirement for many of them to make a risk management statement in their annual report.

In practice though, risk management is often delegated to the charity's senior management with the Board maintaining oversight of the effectiveness of the overall approach to risk and the management of key risks. And in reality everyone involved in the charity's activities has a part to play in risk management. To ensure this is co-ordinated effectively you will need a risk management framework.

Decide who will be responsible for risk management

Although risk management should be led by the senior management team or Board and must have their commitment, it's a good idea to have someone who is responsible for it across the charity. They won't manage all the risks but they will make sure there is an agreed policy and process, as well as co-ordinating risk management activity across the organisation.

In large charities there might be one person who focuses solely on risk management, but for most, risk management will be just part of a person's role and responsibility. In some charities there may also be people responsible for specific areas of risk such as health and safety or safeguarding.

If you would like to learn more about this subject please see our latest publication: Risk Governance for Charities: Risk Management Structures and Accountabilities.

Establish a policy

You will need to decide what is appropriate for your charity taking into account the complexity of your structure and the nature of the work that you do.

You'll need a risk management policy that clearly sets out how things will be done. Remember to keep this proportionate to the size of the charity and the work that you do. If you are a large international charity delivering a range of activities, then the process will be more complex than for a small charity focusing on one type of service in one location.

Your policy should cover:

- How risk management is important to the charity's objectives
- How it links to your culture and structure
- The process for identifying, assessing, recording, managing, reviewing and reporting on risks
- Risk roles and responsibilities
- Your risk appetite

Remember to review the policy from time-to-time so it remains up to date and appropriate.

And communicate it

Agree the policy with the Trustees and then make sure everyone knows about it and where to find it. Publish it in different formats and in different places to maximise exposure within the organisation.

Think about training and guidance needed

If your charity really is just getting started with risk management you might need to arrange some training for key staff. If you have the technology it's worth considering an online module - these can work well where you just want to give people an overview and get them thinking about risks in the workplace. You can then limit detailed technical training to those who really need it. The IRM, for example, provides a short Fundamentals of Risk Management course regularly throughout the year.

You'll probably need to supplement any training with some guidance. This leaflet might meet some of your critical needs but you may need something tailored to the processes you have decided to adopt.

Risk process overview

Before we start let's be clear about a few definitions.

What is a risk? A risk is something uncertain – it might happen or it might not. A risk matters because, if it happens, it will have an effect on objectives.

And risk management? This is any activity undertaken to identify and then control the level of risk which objectives face. This should be a central part of any organisation's strategic management.

Controls and mitigation? You'll hear these terms a lot in risk management. A control is a specific action that will reduce the likelihood of a risk occurring. To mitigate a risk is to make the impact of it less severe.

So what's an issue? Risks and issues are often mentioned in the same breath. The difference is that an issue is an unplanned event that's already happened and needs action to manage it.

Effective risk management has many benefits but, in short, it means that objectives are more likely to be achieved successfully. People, income, reputation and stakeholder confidence are protected and expenditure controlled.

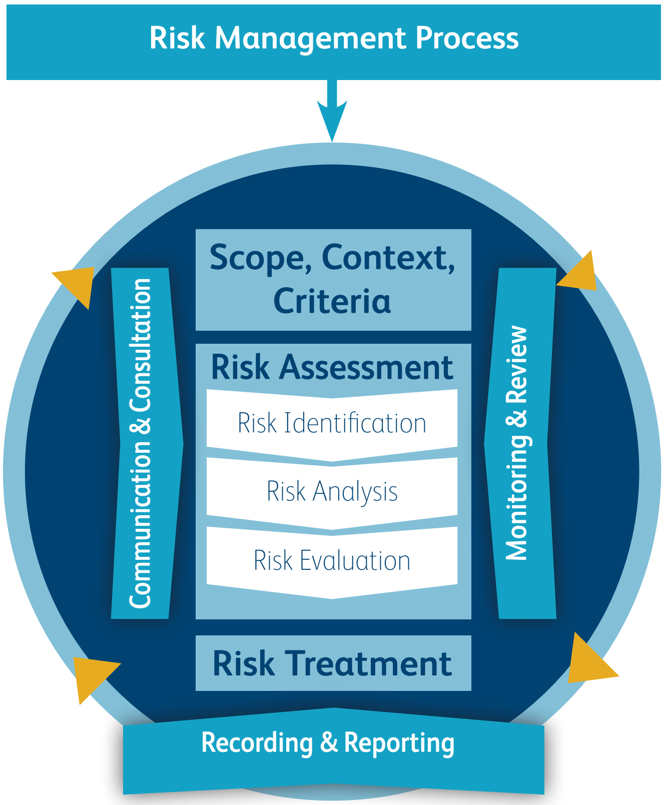
For risk management to be effective you will need to follow all the steps in this process. And the process needs to continue day in and day out. As circumstances change over time:

- new risks may emerge
- risks may become more or less likely to occur
- some risks might go away altogether.

Effective risk management involves an ongoing cycle of assessment, treatment, monitoring and review. The frequency and timing of these processes will vary according to the size and complexity of your charity as well as the changing landscape in which you operate.

We've set out in this guidance more detail on how to handle each element of the risk management process.

This diagram summarises the risk management process as set out in ISO 31000



What is the scope, context and criteria?

The purpose of risk management is the creation and protection of value for your organisation. It improves performance, encourages innovation and supports the achievement of objectives.

Risk management needs to be:

- integrated
- structured and comprehensive
- customised to and proportionate to your external and internal context as related to your objectives
- inclusive
- dynamic
- based on the best available information
- cognisant of human and cultural factors
- improved through continual improvement.

To achieve this you will need to:
1. define the scope of your risk management activities (e.g. strategic, operational, programme, or other activities)
2. understand the external and internal context in which you operate
3. define risk criteria by specifying the amount and type of risk that you may or may not take, relative to objectives.

How to identify and assess risks

As well as considering how risks are managed within business as usual and annual planning and budgeting, you will need to think about the risks you might face whenever you are developing a new strategy or business plan and considering a new project or piece of work. Sometimes the risks will be so significant that you will need to change your plans to avoid or reduce the level of risk faced.

You'll need to be methodical about this. Here are some simple steps to follow:

Identifying risks

Confirm your objectives

Remember that if risks occur they will affect your objectives. Risks don't exist in a vacuum so make sure you are clear about what your objectives are for whatever work you're considering.

Be clear what success looks like

It can be helpful to think about all the things you will rely on to achieve your objectives and to recognise any key constraints and dependencies. If you wanted to bake a cake you would need a good recipe, the right ingredients, a suitable cake tin and an oven that works properly (as a minimum). Might there be problems with any of those things? Could you proceed without one of the ingredients?

Think about different risk categories

Risks come from a number of sources. Common risk categories include strategic, project, operational, financial, environmental, external, legal / regulatory and governance. Think about the categories that apply to your charity.

Consult other people

Involve relevant stakeholders when identifying risks. That way you are less likely to overlook anything critical. You can hold a workshop, interview people or do an email survey. Consulting people is also a good way of raising awareness of risk, securing buy-in and making sure the risks get managed.

Record the risks

This is important for monitoring and reviewing the risks in future. We suggest using our simple template which will help you capture all the information you'll need.

No	Risk event	Cause(s)	Impact	Owner	Score			Actions
					L*	I*	Total (LXI)	
1	I miss the train	I oversleep	I am late and miss the meeting	A person	2	4	8	Replace batteries in my alarm clock
2								
3								
4								
5								

* L= Likelihood, I = Impact

So you have a list of the main risks your charity is facing, but you'll probably be more worried about some than others. Remember, when it comes to risk different people have different views and you'll need a consistent method for assessing risks to remove any bias.

Assessing and scoring risks

How likely is the risk to occur?

If a risk is very unlikely to occur you will probably be much less concerned than if it almost certainly will.

Think about 'Black Swan' events

So-called 'Black Swan' events are risks that are highly unlikely to occur – in fact people might not even conceive that such a thing could ever happen - but they often have catastrophic consequences and could bring your charity to its knees. They are often called 'unknown unknowns'. Please think carefully about how you might cope with potential Black Swans.

What would the impact would be?

Remember there might be various consequences of a risk occurring (and some may be positive) and they may impact on more than one objective.

Score each risk and include this in your risk register

You could keep it simple and score each risk as high, medium or low likelihood. Or you could use a scale of 1-5 for both likelihood and impact. We have given an amended version of the criteria included in the Charity Commission for England and Wales' Risk Management guidance. The Commission puts extra weighting on some criteria, which we have left out for simplicity. Whatever criteria you use, the important thing is to understand which risks need the most urgent attention.

In interpreting the risk heat map below, likelihood is x and impact is y. The colour codes are:
Red - major or extreme/catastrophic risks
Amber - moderate or major risks
Blue or green - minor or insignificant risks

Impact	Extreme/Catastrophic	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Insignificant	1	1	2	3	4	5
			1	2	3	4	5
			Remote	Unlikely	Possible	Probable	Highly probable
			Likelihood				

Charity Commission's fully weighted example

Impact	Extreme/Catastrophic	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6
			1	2	3	4	5
			Remote	Unlikely	Possible	Probable	Highly probable
			Likelihood				

'RAG' each risk

It's usual to create an overall score by multiplying the likelihood and impact scores. Then classify the most serious risks as 'red', the least serious as 'green' and those in between as 'amber'. This makes it easier to read 'at a glance'.

What do the scores mean?

It's important that everyone understands what the scores represent and you might want to provide some further clarification e.g. where there is a financial impact a loss of £1m might be 'very high' and a loss of £100 'very low'.

Consider developing a guide to your own likelihood and impact definitions like these:

Likelihood	Certainty	Number of instances	Time period
Highly probable / Very high (5)	Almost certain	1/10	Once in 3 months
Probable / High (4)	More likely than not	1/100	Once in a year
Possible / Medium (3)	Fairly likely	1/1,000	Once in 5 years
Unlikely / Low (2)	Unlikely	1/10,000	Once in 10 years
Remote / Very low (1)	Extremely unlikely	<1/10,000	Not in 50 years

Level of impact	Strategic	Operational	Financial	Reputational	Compliance
Very High	Would require a fundamental change in organisational strategic/ critical objectives.	Fundamental organisational changes would need to be implemented. Delay of 1 year + in delivery of project.	If the risk materialised the cost to the charity would be greater than £3 million.	Significant and irreparable damage to reputation. Sustained negative publicity resulting in loss of public/ professional/ political confidence in the charity.	Serious breach of governance regulations that would lead to status of the charity being reviewed.
High	Would require a significant shift from organisational strategy/critical objectives that would require BoT input.	A significant amount of work would need to be done at all levels to resolve the matter. Delay of 6-12 months delivery on the project.	If the risk materialised the cost to the charity would be between £1 milllion and £3 million.	Significant and irreperable damage to reputation. High negative impact on the charity's reputation. Could impact on charity's ability to influence public/ professionals/politicians. Generates significant numbe of complaints.	Significant breach of governance regulation requiring immediate notification of regulatory bodies.
Medium	Would impact on the organisational strategic/ critical objectives and would require management discussion.	A significant amount of work would be required by a team to repair operational systems. Delay of 3-6 months in delivery of project.	If the risk materialised the cost to the charity would be between £500k and £1million.	Minor damages but widespread. Significant localised low level negative impact on the charity's reputation/ generates limited complaints.	Breaches governance regulations and would require significant work to rectify.
Low	May have an impact on achieving organisational strategy but this could be resolved.	Low level processes would need to be revised but the matter could be resolved. Delay of 1-3 month's in the delivery of project.	If the risk materialised the cost to the charity would be between £100k and £500k.	Minor damages in a limited area. May have localised, low level negative impact on the charity's reputation/ generates low level of complaints.	May breach low level governance regulations but can be rectified.
Very Low	Little impact on the organisational strategy.	Has no impact on the day to day operation of the charity. Less than 1 months delay in delivery of project	If the risk materialised the cost to the charity would be no more than £100k.	Has no negative impact on the charity's reputation/no media interest.	No impact on the charity's governance structures.

How to treat risks

Identifying risks alone is not enough to make them go away! Now you've identified and assessed your risks you should decide what, if anything, must be done to reduce the likelihood of the risk occurring or minimise its harmful impact if it happens and when to decide to tolerate the risk at the level at which it stands, or terminate the activity if the risks are too high. A common way to approach this is to decide whether to Treat, Tolerate, Terminate or Transfer the risk (the 4 T's)

You'll probably decide to 'treat' most risks

For the most severe risks you will almost certainly decide to take action. Considering what would cause the risk to happen, and the impact it would have on your objectives, is the best way to decide what action to take. For example, if the risk is staff leaving, you need to understand whether the issue is poor morale or if salaries are higher elsewhere. Can they be replaced quickly? What cost is attached to this?

In reality a risk might have a number of causes so remember that you might need to consider more than one course of action to address the risk. On the other hand you might find that one action will address a number of risks. For example, a programme of staff engagement might improve staff morale and reduce staff turnover as well as improving their knowledge and reducing the number of mistakes they make.

Don't forget to consider the cost of any action you take and make sure it's proportionate – you wouldn't spend £1m to prevent a loss of £100k for example.

But sometimes it's OK to do nothing

You don't have to leap into action for every risk. If there's a fairly low likelihood of it happening, or the impact would be low if it did, then you might decide to 'tolerate' the risk and do nothing unless it becomes more serious. But make sure everyone knows that's an informed decision.

Remember to review the risk regularly. Things change and something that seems very unlikely at first could become more likely or its impact increased over time.

You might have to stop the risky activity

Insurance isn't available for everything and can be an expensive option, but there are some risks you can transfer in this way. You may also find you can use contracts to transfer certain risks to a third party.

Don't forget contingency plans

For the risks that are highly likely to happen you will also need a contingency plan. This will help you to formulate how you are going to minimise disruption if the risk occurs.

Appoint an owner for each action

Make sure that each action you decide to take has an 'owner' who will be responsible for ensuring the action is implemented and for reporting on progress. Make sure everyone in the organisation knows who the 'owner' is to avoid any misunderstanding.

Record agreed actions on the risk register

Your risk register will probably be seen by a number of people across the charity and they will want to know about the action planned to reduce risk. Risk owners will also need to consider progress of the actions as part of their regular risk reviews.

The importance of monitoring and reviewing risks

A common mistake people make is to identify their risks, come up with some actions to address them, record it all carefully on a risk register and then file it away, never to see the light of day again.

Risks change – consider them regularly

Once a year just isn't enough, but is often what happens. But think back twelve months; has everything you planned for the year turned out exactly as you thought it would?

For fast moving projects you might need to review risks as often as weekly in a 5-15 minute teleconference, but for more strategic risks quarterly might be enough. Think about how often you need to review risks as you develop your risk management framework.

Risks do change. Sometimes external factors can mean that a risk increases, reduces or goes away altogether. And the action you're taking should be reducing risk as well, of course.

Remember too to consider whether there are any new risks. As the external landscape changes or as a new project progresses, it's quite likely you will identify new risks. Add these to your risk register, assess them and decide how to manage them in the same way as before.

Check the action you're taking – is it effective?

Is the action you've decided to take having the desired effect? If you're doing everything you planned but the risk is still as severe as it was before then you need to take stock. Do you need to stop and do something else instead? Or do you just need to do more of what you're doing? Or perhaps faster?

It can be helpful to think about when you expect risks to reduce as a result of action taken. For example if you are training staff in response to a risk, then the risk probably won't reduce until they have had the training and have operated the system for a few weeks. But if the risk hasn't reduced at that point you'll need to have a rethink.

Update your risk register

Remember to update the risk register after every review. Record the reason for any changes you make. This is something that is often overlooked – it's seen as yet another form to fill in. But it actually provides a useful audit trail, an important thing in a sector where staff turnover can be high and stakeholders are many.

Learn the lessons!

Even with the best risk management processes, risks will sometimes occur. This may be due to external events beyond your control or simply because you under-estimated the likelihood of it happening. If this is a risk you had identified you will hopefully have had a contingency plan, but make sure you learn from the experience. Why did it happen? Could it happen again? What could you do differently another time?

It's a good idea to communicate the learning to key people across the charity as although it might be too late this time, others may be able to prevent similar issues in their work.

This could also assist in managing the internal and external communications to demonstrate to stakeholders that you are an organisation that learns from historical lessons.

Communication and consultation

The most serious risks can have catastrophic consequences so it's important to make sure that the right people know about the risks you've identified and how you are managing them.

Tell relevant stakeholders about your progress

Risks are usually managed at different levels within an organisation. There might be project and business unit risk registers, as well as a corporate risk register. Different people will be interested in each and you will need to agree with management who needs to see what. For risks that could have a severe impact on organisational objectives it's likely that the senior management or the Trustees will make decisions about what action is taken. It's a good idea to agree some criteria so that everyone knows exactly when they need to 'escalate' a risk. You can link this to your assessment criteria (see page 7) – see the example below.

RAG assessment	Who should manage the risk?
🟥	Executive Team/Director – urgent remedial action required
🟧	Head of function – remedial action and senior level monitoring required
🟩	Line manager – low level monitoring required

Speak up!

Concerns can arise about what is happening at work and usually they are easily resolved. However, it can be difficult to know what you should do if your concerns are about ethical or legally questionable practices in the workplace.

It is important that people have an opportunity to speak out so we advocate your organisation developing an effective Whistle Blowing policy alongside the Risk Policy and communicates both amongst staff and other stakeholders.

Produce a regular risk report

The risk register alone might not tell the full story. Management and Trustees will want to know how effective risk actions are, whether risk scores have changed and why and whether any risks have been closed or new risks identified. They may also identify new risks based on the information provided.

As part of your risk management framework you will need to decide how frequently you will report to the Trustees and in what format. Some organisations use a one or two page dashboard that focuses on key risks, new risks and how these are being managed, as well as detailing future risk management strategies. Some charities will also have an Audit and Risk Committee which oversees risk management on behalf of the Trustees and may look at the charity's risks more frequently.

Support informed decision making

By providing accurate and concise information about risks and how they are managed, your charity will be able to make informed decisions about the present and future strategy and this in turn will support the organisation to achieve its objectives.

Include a risk management statement in your annual report

By law, the Charity Commission for England and Wales requires trustees of charities over the audit threshold to report on the major risks to which the charity is exposed, confirming that they are satisfied systems are in place to manage those risks.

Further information

The IRM has produced guidance specially tailored for charities

This guidance supplements our short leaflet which you can download from the Institute of Risk Management's charity pages at www.theirm.org. You may also find out more about IRM's Charities Special Interest Group at www.theirm.org/events/special-interest-groups/charities/
and our other publications:

- Getting Better (with risk management) – a risk maturity matrix
- Setting Risk Appetite
- Risk Management Governance: Structures and Accountabilities

More information is available on the website

www.theirm.org has a wide range of information available free of charge. You can also sign up for webinars to hear live discussions about a range of risk topics. And if you join the IRM you can access an even wider range of resources.

The Charity Commission has produced a guide for trustees

CC26 Charities and Risk Management is available at www.charity-commission.gov.uk

irm

Institute of Risk Management
2nd Floor, Sackville House,
143-149 Fenchurch Street,
London, EC3M 6BN

Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org