CHARITY COMMISSION
FOR ENGLAND AND WALES

GUIDANCE

Charities and risk management (CC26)



Contents

1. Introduction 2

2. Understanding the basics of risk management 4

3. Knowing the requirements - the risk management statement 9

4. A risk management model 12

Annex 1. Risk register template with examples of use 19

Annex 2. Examples of potential risk areas, their impact and mitigation 20

1. Introduction

1.1 What is this guidance about?

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. Risk is an everyday part of charitable activity and managing it effectively is essential if the trustees are to achieve their key objectives and safeguard their charity's funds and assets.

This guidance outlines the basic principles and strategies that can be applied to help charities manage their risks. It should help trustees set a risk framework that allows them to:

- identify the major risks that apply to their charity
- make decisions about how to respond to the risks they face
- make an appropriate statement regarding risk management in their annual report

The risks that a charity faces depend very much on the size, nature and complexity of the activities it undertakes, and also on its finances. As a general rule, the larger and more complex or diverse a charity's activities are, the more difficult it will be for it to identify the major risks that it faces and put proper systems in place to manage them. This means that the risk management process will always need to be tailored to fit the circumstances of each individual charity, focusing on identifying the major risks. Trustees of large, complex charities may need to explore risk more fully than the outline given here.

The main body of the guidance covers:

- an overview of the reasons for and the processes involved in risk management
- the legal requirement for trustees to make a risk management statement in their annual report, and what that statement must contain
- a model of risk management to help charities work through the process. This section is intended to be of particular interest to those actually carrying out or involved in the identification and management of a charity's exposure to risk

Annex 1 contains a risk register template with examples of how it can be used and Annex 2 gives examples of the most common risk areas for charities, their potential impact and the possible steps to mitigate them.

1.2 Previous guidance

This guidance has been updated to include current thinking in models for assessing risk and to draw attention to the distinction between risks that arise from a financial situation and risks arising in other ways that can be seen as non-financial, even if ultimately they have a financial impact. There is no change to the regulatory requirements for charities (see Part 3).

1.3 'Must' and 'should': what the Charity Commission mean

The word 'must' is used where there is a specific legal or regulatory requirement that you must comply with. 'Should' is used for minimum good practice guidance you should follow unless there's a good reason not to.

The commission also offer less formal advice and recommendations that trustees may find helpful in the management of their charity.

1.4 The meaning of some terms used in this guidance

The Charities Act means the Charities Act 2011

Annual report means the trustees' annual report prepared under the Charities Act

Governing document (GD) means a legal document setting out the charity's purposes and, usually, how it is to be administered. It may be a trust deed, constitution, memorandum and articles of association, will, conveyance, Royal Charter, scheme of the commission, or other formal document.

Joint venture in this guidance means an entity formed between two or more parties to undertake some form of economic activity together. The parties involved create a new entity by all contributing equity, and they then share in the revenues, expenses, and control of the enterprise. The venture can be for one specific project only, or a continuing business relationship.

Regulations refers to the Charities (Accounts and reports) Regulations 2008 (SI 2008 No. 629) which set out the required form and content of the trustees' annual report and the scrutiny and accounting arrangements for charities. The Regulations made the SORP recommendations that the trustees' annual report should contain a risk management statement a statutory requirement for certain charities.

Risk is used in this guidance to describe the uncertainty surrounding events and their outcomes that may have a significant impact, either enhancing or inhibiting any area of a charity's operations.

Subsidiary trading company is any non-charitable trading company owned by a charity or charities to carry on a trade on behalf of the charity or charities.

Trustee means a **charity trustee**. **Charity trustees** are the people who are responsible for the general control of the management of the administration of the charity. In a charity's governing document they may be collectively called trustees, the board, managing trustees, the management committee, governors or directors, or they may be referred to by some other title.

2. Understanding the basics of risk management

This part covers:

- Why is risk management important?
- What particular types of risk do charities face?
- How can risk be managed?
- What is disaster recovery planning?

More detail on approaches to identifying and managing risk management can be found in Part 4.

2.1 Why is risk management important?

Identifying and managing the possible and probable risks that a charity may face over its working life is a key part of effective governance for charities of all sizes and complexity.

By managing risk effectively, trustees can help ensure that:

- significant risks are known and monitored, enabling trustees to make informed decisions and take timely action
- the charity makes the most of opportunities and develops them with the confidence that any risks will be managed
- forward and strategic planning are improved
- the charity's aims are achieved more successfully

Reporting in its trustees' annual report on the steps a charity has taken to manage risk helps to demonstrate the charity's accountability to its stakeholders including beneficiaries, donors, funders, employees and the general public.

2.2 What types of risk do charities face?

Charities will face some level of risk in most of the things they do. The diverse nature of the sector and its activities means that charities face different types of risk and levels of exposure.

An essential question for charities when considering risk is whether or not they can continue to meet the needs of beneficiaries now and in the future. For example, in a period of economic uncertainty, the major financial risks for a charity are likely to be:

- termination of funding from other bodies
- the future of contracts
- fundraising from the general public
- fluctuations in investments
- an unforeseen rise in demand for their services

Generally, risk will need to be considered in terms of the wider environment in which the charity operates. The financial climate, society and its attitudes, the natural environment and changes in the law, technology and knowledge will all affect the types and impact of the risks a charity is exposed to. Although the risks that a charity might face are both financial and non-financial, a part of the ultimate impact of risk is financial in most cases. This could be where a party seeks compensation for loss, or costs incurred in managing, avoiding or transferring the risk, for example by buying employers' liability insurance or buildings insurance. The law requires that some risks are insured - motor insurance and employers' liability insurance for charities that employ staff are compulsory.

A system of classification, such as the example below, is helpful for ensuring key areas of risk arising from both internal and external factors are considered and identified. Annex 2 expands on this approach and provides further illustrations of the type of risks that may fall into each category.

Risk category	Examples
Governance risks	• inappropriate organisational structure • trustee body lacks relevant skills or commitment • conflicts of interest
Operational risks	• lack of beneficiary welfare or safety • poor contract pricing • poor staff recruitment and training • doubt about security of assets
Financial risks	• inaccurate and/or insufficient financial information • inadequate reserves and cash flow • dependency on limited income sources • inadequate investment management policies • insufficient insurance cover
External risks	• poor public perception and reputation • demographic changes such as an increase in the size of beneficiary group • turbulent economic or political environment • changing government policy
Compliance with law and regulation	• acting in breach of trust • poor knowledge of the legal responsibilities of an employer • poor knowledge of regulatory requirements of particular activities (eg fund-raising, running of care facilities, operating vehicles)

2.3 How can risk be managed?

Following identification of the risks that a charity might face, a decision will need to be made about how they can be most effectively managed. Trustees may wish to establish a risk framework to help them make decisions about the levels of risk that can be accepted on a day to day basis and what matters need to be referred to them for decision.

There are four basic strategies that can be applied to manage an identified risk:

- transferring the financial consequences to third parties or sharing it, usually through insurance or outsourcing
- avoiding the activity giving rise to the risk completely, for example by not taking up a contract or stopping a particular activity or service
- management or mitigation of risk
- accepting or assessing it as a risk that cannot be avoided if the activity is to continue. An example of this might be where trustees take out an insurance policy that carries a higher level of voluntary excess or where the trustees recognise that a core activity carries a risk but take steps to mitigate it - public use of a charity's property such as a village hall would be such a risk

Part 4 sets out a possible framework for evaluating the potential courses of actions that can be taken to manage the risks identified.

Two simple examples that illustrate different risks and how they might be managed.

Example 1: Funding of core activities

This concerns two charities that are working with disadvantaged people in a local community.

One charity is dependent on funding in the form of donations from local philanthropists, including local businesses, for the vast majority of its funds. In the event of a downturn in the economic cycle those same local businesses may no longer be in a position to contribute either because of cash flow difficulties or because they face severe financial difficulty themselves. This will lead to a sudden drop in income that may have a severe impact on the charity's ability to do its work.

The other charity depends mostly on public sector funding and, provided this funding is renewed on a timely basis, it may therefore have a more secure income stream. Uncertainty only arises at the time that the funding agreement comes up for review or renewal.

Both charities in this example may find that the impact on their local community of an economic downturn means that families in the community are struggling to manage and that both charities are dealing with a far higher number of potential beneficiaries than they had expected or planned to help.

In such a situation the trustees of both charities will need to draw up an outline of the steps that their charity should take in these circumstances. At the same time they will need to draw up a recovery plan, that could be activated when necessary, that would include alternative ways of raising funds, concentrating on core activities, reducing costs and taking advantage of any new opportunities that arise. Consideration of the risks attached to these areas would be part of the budget setting and forward planning process and also part of the ongoing monitoring of their charity's performance throughout the year.

The commission's guidance **Charity governance, finance and resilience: 15 questions trustees should ask** sets out a number of key questions that trustees can use as a basis for discussion at any planning meeting.

Example 2: Cutting costs

In this example, one charity is organising a garden fete and the other is organising a charity concert.

The organisers of the garden fete want to set out stalls and fun activities for children in a large private garden to raise funds for the village hall. They are expecting a good turnout of up to 200 people over the day. Since the event is being held on an English summer's day, they may plan to have a tented area just in case of showers and a back up plan to use the village hall if it rains heavily. This means they wouldn't need to take out insurance covering the effects of adverse weather conditions. In thinking through and planning the event, the trustees are taking account of risk in a very practical, pragmatic way.

The organisers of the charity concert may approach the weather risk differently as part of their planning. They may be hiring an outdoor venue, hiring seating, incurring costs in setting up a parking area and refreshments, and paying artists' performance fees. The fete described in the previous paragraph was comparatively small with 200 people attending over the whole day, but the concert is planned to have 600 seats for a 3 hour early evening performance. The risk from adverse weather to the charity concert is viewed as so great that the extra cost of insurance is considered worthwhile.

Note that even though facing the same risk of adverse weather, the scale and nature of the fundraising events can cause trustees to take a different approach to risk management.

2.4 What is disaster recovery planning?

As a part of an effective risk management process, a charity should consider what needs to be done if a serious event does take place. This could range from a fire or flood to a serious computer malfunction.

Charities should consider how their services to their beneficiaries would be affected as a result of a serious incident, including those with a major impact and a low likelihood, and plan to resume normal operations as far as and as soon as possible. Many charities develop disaster recovery plans (sometimes referred to as business contingency plans) and follow good practice procedures used in the public and private sector.

The scope and complexity of any disaster recovery plan will vary according to the size and activities of the charity concerned. However, the basic stages in establishing an effective disaster recovery or business contingency plan are likely to be similar to those shown in the following grid.

1 First steps	• commit to planning across the charity • develop a plan by a team representing all functional areas of the charity • plan as a project if appropriate
2 Impact/risk assessment	• identify all major risks • each risk to be given an impact and likelihood rating (see Part 4) • consider overall risk profile of charity
3 Drawing up the plan	• establish milestones to move charity from disaster to normal operations • start with immediate aftermath • outline what functions need to be resumed and in what order • plan should identify key individuals and their roles and duties
4 Testing	• plan process of testing properly • reproduce authentic conditions as far as possible • plan tested by the key individuals identified in the plan • document test procedures and record results • consider amendments to plan
5 Training	• make all charity trustees, staff and volunteers aware of plan and their own duties and responsibilities • stress the importance of planning even if the disaster appears to be a remote likelihood • get feedback from all to ensure that duties and responsibilities are understood
6 Updating and maintaining	• plan should be updated to be applicable to current activities • give someone responsibility for updating plan and communicating any changes • all changes should be fully tested • key staff informed of changes in duties and responsibilities

3. Knowing the requirements - the risk management statement

This part covers:

- Who is responsible for risk management in a charity?
- What are the legal requirements for charities in relation to risk management?
- Which charities must have a risk management statement?
- What does the risk management statement need to cover?
- Does the risk management statement need to be audited?

3.1 Who is responsible for risk management in a charity?

The responsibility for the management and control of a charity rests with the trustee body and therefore their involvement in the key aspects of the risk management process is essential, particularly in setting the parameters of the process and reviewing and considering the results.

This should not be interpreted as meaning that the trustees must undertake each aspect of the process themselves. In all but the smallest charities, the trustees are likely to delegate elements of the risk management process to staff or professional advisers. The trustees should review and consider the key aspects of the process and results. The level of involvement should be such that the trustees can make the required risk management statement with reasonable confidence.

3.2 What are the legal requirements for charities in relation to risk management?

Legal requirement: charities that are required by law to have their accounts audited must make a risk management statement in their trustees' annual report confirming that '...the charity trustees have given consideration to the major risks to which the charity is exposed and satisfied themselves that systems or procedures are established in order to manage those risks.' (Charities (Accounts and Reports) Regulations 2008)

Major risks are those risks that have a major impact and a probable or highly probable likelihood of occurring. If they occurred they would have a major impact on some or all of the following areas:

- governance
- operations
- finances
- environmental or external factors such as public opinion or relationship with funders
- a charity's compliance with law or regulation

Any of these major risks and their potential impacts could change the way trustees, supporters or beneficiaries might deal with the charity.

Charities will need to consider risk and its management in a structured way if a positive risk management statement is to be made. One method of reviewing and assessing risk through a 'risk mapping' exercise is set out in Part 4.

3.3 Which charities must have a risk management statement?(Legal requirement)

Charities that are required to be audited: All charities that are under a legal requirement to have their accounts audited must make a risk management statement in their trustees' annual report.

The statutory audit thresholds effective from 1 April 2009 are:

- an income of £500,000 or more or
- a gross income exceeding £250,000 with gross assets held exceeding £3.26 million

Further information on audit thresholds can be found on the **GOV.UK website**.

Smaller charities: Trustees of smaller charities with gross income below the statutory audit threshold (who should still be concerned about the risks their charity faces) are encouraged to make a risk management statement as a matter of good practice.

Incorporated charities (companies): Charities that are incorporated under company law (other than small companies[1] as defined by company law) must include a business review in their directors' report. The business review must contain a description of the principal risks and uncertainties facing the company.

3.4 What does a risk management statement need to cover?

The purpose of the risk management statement is to give readers of the trustees' annual report an insight into how the charity handles risk and an understanding of the major risks the charity is exposed to. It is also an opportunity for the trustees to comment on any further developments of risk management procedures being undertaken or planned.

The form and content of the statement is likely to reflect the size and complexity of an individual charity's activities and structure. The commission is not seeking 'template' reporting, or requiring a detailed analysis of the processes and results. A narrative style that addresses the key aspects of the requirements is acceptable. This means:

- an acknowledgement of the trustees' responsibility
- an overview of the risk identification process
- an indication that major risks identified have been reviewed or assessed
- confirmation that control systems have been established to manage those risks

1 To be a small company at least two of the following conditions must be met:
- annual turnover must be £6.5 million or less
- the balance sheet total must be £3.26 million or less
- the average number of employees must be 50 or fewer

Many charities, particularly larger charities or those with more complex activities, will, as a matter of best practice, expand on this basic approach in their reporting. Where this more detailed approach to reporting is adopted the following broad principles can be useful:

- a description of the major risks faced
- the links between the identification of major risk and the operational and strategic objectives of the charity
- procedures that extend beyond financial risk to encompass operational, compliance and other categories of identifiable risk
- the link between risk assessment and evaluation to the likelihood of its occurrence and impact should the event occur
- a description of the risk assessment processes and monitoring that are embedded in management and operational processes
- trustees' review of the principal results of risk identification processes and how they are evaluated and monitored

3.5 Does the risk management statement need to be audited?

Although the risk management statement forms an important part of the trustees' annual report, there is no requirement for the statement to be audited unless other requirements outside the **Charities Act 2011** or the Companies Act 2006 apply. The regulatory requirements do not extend auditors' duties but auditors who become aware of apparent misstatements or inconsistencies in the trustees' Annual Report, based on their other audit work, will seek to resolve them and will need to consider the impact on their report, if such issues cannot be resolved. In extreme cases a reporting duty may arise where charity assets are at significant risk or have already been lost, auditors should be aware of their whistle-blowing obligations and may find the commission guidance **Reporting Serious Incidents** of help.

4. A risk management model

This part sets out a model for risk management covering the typical stages in the process and will be of use to those actually carrying out or involved in the identification and management of the risks a charity faces. The model can be adapted by any charity to suit its size and activities and covers:

1. Establishing a risk policy
2. Identifying risks
3. Assessing risks
4. Evaluating what action needs to be taken on risks
5. Periodic monitoring and assessment

For most charities, risk management has been incorporated into their management processes for many years. While there is no requirement or obligation for trustees to adopt any particular model, having a rigorous process and a clear risk management policy helps ensure that:

- the identification, assessment and management of risk is linked to the achievement of the charity's objectives
- all areas of risk are covered - for example, financial, governance, operational and reputational
- a risk exposure profile can be created that reflects the trustees' views as to what levels of risk are acceptable
- the principal results of risk identification, evaluation and management are reviewed and considered
- risk management is ongoing and embedded in management and operational procedures

Stage 1: Establishing a risk policy

An effective charity regularly reviews and assesses the risks it faces in all areas of its work and plans for the management of those risks. The implementation of an effective risk management policy is a key part of ensuring that a charity is fit for purpose.

There are risks associated with all activities - they can arise through things that are not done, as well as through ongoing and new initiatives. Charities will have differing exposures to risk arising from their activities and will have different capacities to tolerate or absorb risk. For example, a charity with sound reserves could embark on a new project with a higher risk profile than, say, a charity facing financial difficulties. Risk tolerance may also be a factor in what activities are undertaken to achieve objectives. For example, a relief charity operating in a war zone may need to tolerate a higher level of risk to staff than might be acceptable in its UK-based activities in order to achieve its objectives. A charity will also need to look at the risk profile, ie the balance taken between higher and lower risk activities.

These considerations will inform the trustees in their decision as to the levels of risk they are willing to accept and may provide a benchmark against which the initial risk assessment is undertaken. The risk assessment and evaluation in turn will inform the trustees of the charity's overall risk profile and the steps taken to manage the major risks identified. This will help the trustees agree their policies on risk. 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.

Stage 2: Identifying risks

Although there are various tools and checklists available, the identification of risks is best done by involving those with a detailed knowledge of the way the charity operates. Whilst the risk management statement focuses on major risks identified by trustees, input into this process will extend beyond the trustee body (except perhaps in the smallest charities).

Examples of what a charity will need to consider as part of this process include:

- the charity's objectives, mission and strategy
- the nature and scale of the charity's activities
- the outcomes that need to be achieved
- external factors that might affect the charity such as legislation and regulation
- the charity's reputation with its major funders and supporters
- past mistakes and problems that the charity has faced
- the operating structure - for example using subsidiary trading companies, collaborating in a joint venture; branches or an affiliated structure where a parent body offers support to its members or affiliated bodies
- comparison with other charities working in the same area or of similar size
- examples of risk management prepared by other charities or other organisations

For this process to work, trustees and executive management need to be committed to it. All staff and volunteers will need to understand the part they should play in risk management. Trustees will need to consult widely with key managers and staff, as ideas are likely to come from all levels of the organisation. Internal workshops involving management, staff and volunteers are often used to gather information. Some workshops can involve supporters and beneficiaries where reputational risk or provision of service to beneficiaries is being considered.

Where the charity conducts some of its activities through affiliated members, branches, subsidiary companies or joint ventures which are legally separate entities, risks may arise that could directly or indirectly impact on the charity. For example, events in a subsidiary trading company may affect income streams to the charity, give rise to reputational risk or may even affect operational objectives directly if the subsidiary is used as a vehicle for service delivery. The risk identification process, whilst focusing on the risk to the charity itself, is therefore also likely to include identifying risks that may arise in branch, subsidiary company or joint venture activities. The trustees of a charity may seek to ensure that the directors of subsidiary companies also adopt similar risk management procedures, with the results being reviewed by the charity's trustees or incorporated into the overall risk management processes of the charity.

There are a number of models or frameworks that provide a classification of the type of risk to which an organisation can be exposed. Most models can be adapted to fit the charitable sector. Annex 2 sets out one possible framework, looking at risk across the following categories:

- governance
- operational risk
- finance risk
- environmental and external risk
- law and regulation compliance risk

It is important to appreciate that the process of risk identification must be charity specific reflecting the activities, structure and environment in which a particular charity operates. It follows from this that Annex 2 should not be used as a checklist, but rather to illustrate the type of risks that may be faced.

Similarly, although the process of risk identification should be undertaken with care, the analysis will contain some subjective judgements - no process is capable of identifying all possible risks that may arise. The process can only provide reasonable assurance to trustees that all relevant risks have been identified.

Stage 3 Assessing risk

Identified risks need to be put into perspective in terms of the potential severity of their impact and likelihood of their occurrence. Assessing and categorising risks helps in prioritising and filtering them, and in establishing whether any further action is required. One method is to look at each identified risk and decide how likely it is to occur and how severe its impact would be on the charity if it did occur.

This approach attempts to map risk as a product of the likelihood of an undesirable outcome and the impact that an undesirable outcome will have on the charity's ability to achieve its operational objectives. It enables the trustees to identify those risks that fall into the major risk category identified by the risk management statement.

In previous guidance the commission set out a risk management methodology that focused on considering both the impact of a risk and the likelihood of it occurring, giving them equal importance. Using this method, the impact score is usually multiplied by the score for likelihood and the product of the scores used to rank those risks that the trustees regard as major risks.

In recent years, methodologies for measuring risk impact and likelihood have developed further. Many organisations now take account of events that are rare or unprecedented, where the rules are unknown or rapidly changing or where risks are driven by external factors beyond their control. These risks which have very high impact and very low likelihood of occurrence are now accepted by many as having greater importance than those with a very high likelihood of occurrence and an insignificant impact. In these cases, the concept of impact and the likelihood of risks occurring and their interaction should be given prominence in both the risk assessment and risk management processes. Using the method outlined in the previous paragraph, they would have scored the same.

If an organisation is vulnerable to a risk that potentially might have an extremely high impact on its operations, it should be considered and evaluated regardless of how remote the likelihood of its happening appears to be. Charities need to find a balance and they will need to weigh the nature of the risk and its impact alongside its likelihood of occurrence. With limited resources, the risks and the benefits or rewards from the activity concerned will need to be considered. It is important to bear in mind that on rare occasions improbable events do occur with devastating effect, at other times probable events do not happen.

A focus on high-impact risk is important, but trustees should not forget that what may be a lower impact risk can change to very high impact risk because of the possible connection between it happening and triggering the occurrence of other risks. One low impact risk may lead to another and another so that the cumulative impact becomes extreme or catastrophic. Many studies have shown that most business failures are the result of a series of small, linked events having too great a cumulative impact to deal with rather than a single large event. If organisations only look at the big risks they can often end up ill-prepared to face the interaction of separate adverse events interacting together.

The following tables can be used to provide some guidance on the 1-5 scoring illustrated in this section.

Impact

Descriptor	Score	Impact on service and reputation
Insignificant	1	• no impact on service • no impact on reputation • complaint unlikely • litigation risk remote
Minor	2	• slight impact on service • slight impact on reputation • complaint possible • litigation possible
Moderate	3	• some service disruption • potential for adverse publicity - avoidable with careful handling • complaint probable • litigation probable
Major	4	• service disrupted • adverse publicity not avoidable (local media) • complaint probable • litigation probable
Extreme/ Catastrophic	5	• service interrupted for significant time • major adverse publicity not avoidable (national media) • major litigation expected • resignation of senior management and board • loss of beneficiary confidence

Likelihood

Descriptor	Score	Example
Remote	1	may only occur in exceptional circumstances
Unlikely	2	expected to occur in a few circumstances
Possible	3	expected to occur in some circumstances
Probable	4	expected to occur in many circumstances
Highly probable	5	expected to occur frequently and in most circumstances

The 'heat map' below shows a different way of assessing risk by increasing the weighting of impact. This works on a scoring of xy+y where x is likelihood and y is impact. This formula multiplies impact with likelihood then adds a weighting again for impact. The effect is to give extra emphasis to impact when assessing risk. It should be remembered that risk scoring often involves a degree of judgement or subjectivity. Where data or information on past events or patterns is available, it will be helpful in enabling more evidence-based judgements.

In interpreting the risk heat map below, likelihood is x and impact is y. The colour codes are:

Red - major or extreme/catastrophic risks that score 15 or more

Yellow - moderate or major risks that score between 8 and 14

Blue or green - minor or insignificant risks scoring 7 or less

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 Remote	2 Unlikely	3 Possible	4 Probable	5 Highly Probable

Likelihood

Some suggest an even greater weighting for impact and use a formula of xy+2y.

Stage 4 Evaluating what action needs to be taken on the risks

Where major risks are identified, the trustees will need to make sure that appropriate action is being taken to manage them. This review should include assessing how effective existing controls are.

For each of the major risks identified, trustees will need to consider any additional action that needs to be taken to manage the risk, either by lessening the likelihood of the event occurring, or lessening its impact if it does. The following are examples of possible actions:

- the risk may need to be avoided by ending that activity (eg stopping work in a particular country)
- the risk could be transferred to a third party (eg use of a trading subsidiary, outsourcing or other contractual arrangements with third parties)
- the risk could be shared with others (eg a joint venture project)
- the charity's exposure to the risk can be limited (eg establishment of reserves against loss of income, foreign exchange forward contracts, phased commitment to projects)
- the risk can be reduced or eliminated by establishing or improving control procedures (eg internal financial controls, controls on recruitment, personnel policies)
- the risk may need to be insured against (this often happens for residual risk, eg employers liability, third party liability, theft, fire)
- the risk may be accepted as being unlikely to occur and/or of low impact and therefore will just be reviewed annually (eg a low stock of publications may be held with the risk of temporarily running out of stock or loss of a petty cash float of £25 held on site overnight)

Once each risk has been evaluated, the trustees can draw up a plan for any steps that need to be taken to address or mitigate significant or major risks. This action plan and the implementation of appropriate systems or procedures allows the trustees to make a risk management statement in accordance with the regulatory requirements.

Risk management is aimed at reducing the 'gross level' of risk identified to a 'net level' of risk, in other words, the risk that remains after appropriate action is taken. Annex 1 gives two examples of how gross and net risk can be recorded in a risk register. Trustees need to form a view as to the acceptability of the net risk that remains after management.

In assessing additional action to be taken, the costs of management or control will generally be considered in the context of the potential impact or likely cost that the control seeks to prevent or mitigate. It is possible that the process may identify areas where the current or proposed control processes are disproportionately costly or onerous compared to the risk they are there to manage. A balance will need to be struck between the cost of further action to manage the risk and the potential impact of the residual risk.

Good risk management is also about enabling organisations to take opportunities and to meet urgent need, as well as preventing disasters. For example, a charity may not be able to take advantage of technological change in the absence of a reserves policy that ensures there are adequate funds, or perhaps could not organise a successful emergency relief programme without adequately trained staff and organisational structures. Annex 2 sets out some illustrative examples of the type of systems and procedures that can be put into place to mitigate an identified risk.

Stage 5 Periodic monitoring and assessment

Risk management is a dynamic process ensuring that new risks are addressed as they arise. It should also be cyclical to establish how previously identified risks may have changed. Risk management is not a one-off event and should be seen as a process that will require monitoring and assessment. Staff will need to take responsibility for implementation. There needs to be communication with staff at all levels to ensure that individual and group responsibilities are understood and embedded into the culture of the charity. A successful process will involve ensuring that:

- new risks are properly reported and evaluated
- risk aspects of significant new projects are considered as part of project appraisals
- any significant failures of control systems are properly reported and actioned
- there is an adequate level of understanding of individual responsibilities for both implementation and monitoring of the control systems
- any further actions required are identified
- trustees consider and review the annual process
- trustees are provided with relevant and timely interim reports

One method of codifying such an approach is through the use of a risk register (see Annex 1). The register seeks to pull together the key aspects of the risk management process. It schedules gross risks and their assessment, the controls in place and the net risks, and can identify responsibilities, monitoring procedures and follow up action required.

The trustees can monitor risk by:

- ensuring that the identification, assessment and mitigation of risk is linked to the achievement of the charity's operational objectives
- ensuring that the assessment process reflects the trustees' view of acceptable risk
- reviewing and considering the results of risk identification, evaluation and management
- receiving interim reports where there is an area needing further action
- considering the risks attached to significant new activities or opportunities
- regularly considering external factors such as new legislation or new requirements from funders
- considering the financial impact of risk as part of operational budget planning and monitoring

Annual monitoring by trustees supplemented by interim reports is likely to be sufficient for most charities where operating conditions are stable. Depending on a charity's risk profile, more frequent monitoring might be advisable.

Thanks to contributors

The commission are grateful to Pesh Framjee, Head of Not for Profits at Howarth Clark Whitehill for his contribution to the updated guidance on assessing risk (Part 4, stage 4).

Annex 1. Risk register template with examples of use

Risk management is aimed at reducing the 'gross level' of risk identified to a 'net level' of risk, in other words, the risk that remains after appropriate action is taken. This template has been created to illustrate a practical way of recording in a risk register how this reduction in level might be achieved by the charity. In example 1, the gross risk is identified as the lack of return/diversity of investment portfolio and rated as high. After identifying the procedures for managing this risk, the net risk has been rated as medium. Trustees need to form a view as to the acceptability of the net risk that remains after management.

Example 1

Risk area/risk identified	lack of return/diversity of investment portfolio
Likelihood of occurrence (score)	probable (4)
Severity of impact (score)	major (4)
Overall or 'gross' risk	high (20)
Control procedure	• investment policy set by trustees • written instructions to FSA authorised investment advisor • quarterly reviews by trustees
Retained or 'net' risk	medium
Monitoring process	performance reports reviewed quarterly by trustees
Responsibility	trustees and treasurer
Further action required	quarterly agenda item for trustee meetings
Date of review	quarterly

Example 2

Risk area/risk identified	unsatisfactory fundraising
Likelihood of occurrence (score)	probable (4)
Severity of impact (score)	major (4)
Overall or 'gross' risk	high (20)
Control procedure	• financial appraisal of new projects • benchmarking of returns achieved • budget reporting by fundraising activity
Retained or 'net' risk	medium
Monitoring process	• financial reporting by fundraising activity • quarterly reporting by fundraising manager to trustees/CEO
Responsibility	fundraising manager/CEO
Further action required	• new initiatives to be approved by trustees unless included in current business plan • review of regulatory compliance of current methods
Date of review	• when appropriate • next trustee meeting

Annex 2. Examples of potential risk areas, their impact and mitigation

The charitable sector is by its nature diverse. The nature of activities, funding base, reserves and structures will expose charities to differing areas of risk and levels of exposure. While the areas of risk identified below will deserve consideration by most charities, it is not an exhaustive list of all potential areas of risk and should not be a substitute for a charity undertaking its own processes for risk identification.

This list is intended to be an indication of some of the main areas of risk that may need to be considered by trustees. Illustrative examples of potential impact are given, as well as some illustrative examples of controls or action that might be taken to mitigate the risk or impact. Some risks will fall into more than one category. Although the list may be long, it is not exhaustive and there will be other risks that apply to a particular charity because of its own circumstances and activities.

The risks are classified as follows:

- governance
- operational
- financial
- environmental or external
- compliance (law or regulation)

Governance risks

Potential risk	Potential impact	Steps to mitigate risk
The charity lacks direction, strategy and forward planning	• the charity drifts with no clear objectives, priorities or plans • issues are addressed piecemeal with no strategic reference • needs of beneficiaries not fully addressed • financial management difficulties • loss of reputation	• create a strategic plan which sets out the key aims, objectives and policies • create financial plans and budgets • use job plans and targets • monitor financial and operational performance • get feedback from beneficiaries and funders
Trustee body lacks relevant skills or commitment	• charity becomes moribund or fails to achieve its purpose • decisions are made bypassing the trustees • resentment or apathy amongst staff • poor decision making reflected in poor value for money on service delivery	• review and agree skills required • draw up competence framework and job descriptions • implement trustee training and induction • review and agree recruitment processes

Potential risk	Potential impact	Steps to mitigate risk
Trustee body dominated by one or two individuals, or by connected individuals	• trustee body cannot operate effectively as strategic body • decisions made outside of trustee body • conflicts of interest • pursuit of personal agenda • culture of secrecy or deference • arbitrary over-riding of control mechanisms	• consider the structure of the trustee body and its independence • agree mechanisms to manage potential conflicts of interest • review and agree recruitment and appointment processes in line with governing document • agree procedural framework for meetings and recording decisions
Trustees are benefiting from charity (eg remuneration)	• poor reputation, morale and ethos • adverse impact on overall control environment • conflicts of interest • possibility of regulatory action	• ensure legal authority for payment or benefit • consider alternative staffing arrangements • implement terms and procedures to authorise/approve expenses and payments • agree procedures and methods to establish fair remuneration conducted separately from 'interested' trustee (remuneration committee/benchmarking exercise etc)
Conflicts of interest	• charity unable to pursue its own interests and agenda • decisions may not be based on relevant considerations • impact on reputation • private benefit	• agree protocol for disclosure of potential conflicts of interest • put in place procedures for standing down on certain decisions • review recruitment and selection processes
Ineffective organisational structure	• lack of information flow and poor decision making procedures • remoteness from operational activities • uncertainty as to roles and duties • decisions made at inappropriate level or excessive bureaucracy	• use organisation chart to create a clear understanding of roles and duties • delegation and monitoring should be consistent with good practice and constitutional or legal requirements • review structure and the need for constitutional change

Potential risk	Potential impact	Steps to mitigate risk
Activities potentially outside objects, powers or terms of gift (restricted funds)	• loss of funds available for beneficiary class • liabilities to repay funders • loss of funder confidence • potential breach of trust and regulatory action • loss of beneficiary confidence • taxation implications (if non-qualifying expenditure)	• agree protocol for reviewing new projects to ensure consistency with objects, powers and terms of funding • create financial systems to identify restricted funds and their application
Loss of key staff	• experience or skills lost • operational impact on key projects and priorities • loss of contact base and corporate knowledge	• succession planning • document systems, plans and projects • implement training programmes • agree notice periods and handovers • review and agree recruitment processes
Reporting to trustees (accuracy, timeliness and relevance)	• inadequate information resulting in poor quality decision making • failure of trustees to fulfil their control functions • trustee body becomes remote and ill informed	• put in place proper strategic planning, objective setting and budgeting processes • timely and accurate project reporting • timely and accurate financial reporting • assess and review projects and authorisation procedures • have regular contact between trustees and senior staff and managers

Operational risks

Potential risk	Potential impact	Steps to mitigate risk
Contract risk	• onerous terms and conditions • liabilities for non performance • non-compliance with charity's objects • unplanned subsidy of public provision	• create cost/project appraisal procedures • agree authorisation procedures • get professional advice on terms and conditions • put in place performance monitoring arrangements • consider insurable risks cover

Potential risk	Potential impact	Steps to mitigate risk
Service provision - customer satisfaction	• beneficiary complaints • loss of fee income • loss of significant contracts or claims under contract • negligence claims • reputational risks	• agree quality control procedures • implement complaints procedures • benchmark services and implement complaints review procedures
Project or service development	• compatibility with objects, plans and priorities • funding and financial viability • project viability • skills availability	• appraise project, budgeting and costing procedures • review authorisation procedures • review monitoring and reporting procedures
Competition from similar organisations	• loss of contract income • reduced fund-raising potential • reduced public profile • profitability of trading activities	• monitor and assess performance and quality of service • review market and methods of service delivery • agree fund-raising strategy • ensure regular contact with funders • monitor public awareness and profile of charity
Suppliers, dependency, bargaining power	• dependency on key supplier • lack of supplier to meet key operational objectives • non-competitive pricing/ quotes • insufficient buying power	• use competitive tendering for larger contracts • put in place procedures for obtaining quotations • authorised suppliers listing • monitor quality/timeliness of provision • use service level agreements • consider use of buying consortia

Potential risk	Potential impact	Steps to mitigate risk
Capacity and use of resources including tangible fixed assets	• under-utilised or lack of building/office space • plant and equipment obsolescence impacting on operational performance • mismatch between staff allocations and key objectives • spare capacity not being utilised or turned to account	• agree building and plant inspection programme • agree repair and maintenance programme • agree capital expenditure budgets • undertake efficiency review
Security of assets	• loss or damage • theft of assets • infringements of intellectual property rights	• review security arrangements • create asset register and inspection programme • agree facility management arrangements • have safe custody arrangements for title documents and land registration • manage use of patent and intellectual property • review insurance cover
Fund-raising	• unsatisfactory returns • reputational risks of campaign or methods used • actions of agents and commercial fund-raisers • compliance with law and regulation	• implement appraisal, budgeting and authorisation procedures • review regulatory compliance • monitor the adequacy of financial returns achieved (benchmarking comparisons) • stewardship reporting in annual report

Potential risk	Potential impact	Steps to mitigate risk
Employment issues	• employment disputes • health and safety issues • claims for injury, stress, harassment, unfair dismissal • equal opportunity and diversity issues • adequacy of staff training • child protection issues • low morale • abuse of vulnerable beneficiaries	• review recruitment processes • agree reference and qualification checking procedures, job descriptions, contracts of employment, appraisals and feedback procedures • implement job training and development • implement health and safety training and monitoring • be aware of employment law requirements • implement staff vetting and legal requirements (eg DBS checks) • agree a whistle-blowing policy
High staff turnover	• loss of experience or key technical skills • recruitment costs and lead time • training costs • operational impact on staff morale and service delivery	• review interview and assessment processes • agree fair and open competition appointment for key posts • agree job descriptions and performance appraisal and feedback systems • conduct 'exit' interviews • review rates of pay, training, working conditions, job satisfaction
Volunteers	• lack of competences, training and support • poor service for beneficiaries • inadequate vetting and reference procedures • recruitment and dependency	• review and agree role, competencies • review and agree vetting procedures • review and agree training and supervision procedures • agree development and motivation initiatives
Health, safety and environment	• staff injury • product or service liability • ability to operate (see Compliance risks) • injury to beneficiaries and the public	• comply with law and regulation • train staff and compliance officer • put in place monitoring and reporting procedures

Potential risk	Potential impact	Steps to mitigate risk
Disaster recovery and planning	• computer system failures or loss of data • destruction of property, equipment, records through fire, flood or similar damage	• agree IT recovery plan • implement data back up procedures and security measures • review insurance cover • create disaster recovery plan including alternative accommodation
Procedural and systems documentation	• lack of awareness of procedures and policies • actions taken without proper authority	• properly document policies and procedures • audit and review of systems
Information technology	• systems fail to meet operational need • failure to innovate or update systems • loss/corruption of data eg donor base • lack of technical support • breach of data protection law	• appraise system needs and options • appraise security and authorisation procedures • implement measures to secure and protect data • agree implementation and development procedures • use service and support contracts • create disaster recovery procedures • consider outsourcing • review insurance cover for any insurable loss

Financial risks

Potential risk	Potential impact	Steps to mitigate risk
Budgetary control and financial reporting	• budget does not match key objectives and priorities • decisions made on inaccurate financial projections or reporting • decisions made based on unreliable costing data or income projections • inability to meet commitments or key objectives • poor credit control • poor cash flow and treasury management • ability to function as going concern	• link budgets to business planning and objectives • monitor and report in a timely and accurate way • use proper costing procedures for product or service delivery • ensure adequate skills base to produce and interpret budgetary and financial reports • agree procedures to review and action budget/cash flow variances and monitor and control costs • regularly review reserves and investments
Reserves policies	• lack of funds or liquidity to respond to new needs or requirements • inability to meet commitments or planned objectives • reputational risks if policy cannot be justified	• link reserves policy to business plans, activities and identified financial and operating risk • regularly review reserves policy and reserve levels
Cash flow sensitivities	• inability to meet commitments • lack of liquidity to cover variance in costs • impact on operational activities	• ensure adequate cash flow projections (prudence of assumptions) • identify major sensitivities • ensure adequate information flow from operational managers • monitor arrangements and reporting
Dependency on income sources	• cash flow and budget impact of loss of income source	• identify major dependencies • implement adequate reserves policy • consider diversification plans

Potential risk	Potential impact	Steps to mitigate risk
Pricing policy	• reliance on subsidy funding • unplanned loss from pricing errors • cash flow impact on other activities • loss of contracts if uncompetitive • affordability of services to beneficiary class	• ensure accurate costing of services and contracts • compare with other service providers • notify and agree price variations with funders • monitor funder satisfaction • develop pricing policy for activities including terms of settlement and discounts
Borrowing	• interest rate movements • ability to meet repayment schedule • security given over assets • regulatory requirements	• appraise future income streams to service the debt • appraise terms (rates available fixed, capped, variable etc) • appraise return on borrowing • use appropriate professional advice
Guarantees to third parties	• call made under guarantee • lack of reserves or liquidity to meet call • consistency with objects and priorities	• review approval and authority procedures • agree procedures to ensure consistency with objects, plans and priorities • ensure financial reporting of contingency and amendment to reserves policy
Foreign currency	• currency exchange losses • uncertainty over project costs • cash flow impact on operational activities	• ensure proper cash flow management and reserves policy • use currency matching (cost to charity in home currency) • consider forward contracts for operational needs (hedging)
Pension commitments	• under-funded defined benefit scheme • impact on future cash flows • failure to meet due dates of payment • regulatory action or fines	• use actuarial valuations • review pension scheme arrangements (eg money purchase schemes) • review procedures for admission to scheme and controls over pension administration

Potential risk	Potential impact	Steps to mitigate risk
Inappropriate or loss-making non-charitable trading activities	• resources withdrawn from key objectives • resources and energy diverted from profitable fund-raising or core activities • regulatory action, and accountability • reputational risk if publicised	• monitor and review business performance and return • ensure adequacy of budgeting and financial reporting within the subsidiary or activity budget • review and agree adequate authorisation procedures for any funding provided by charity (prudence, proper advice, investment criteria) • report funding and performance as part of charity's own financial reporting system • appraise viability • consider transfer of undertakings to separate subsidiary
Investment policies	• financial loss through inappropriate or speculative investment • unforeseen severe adverse investment conditions • financial loss through lack of investment advice, lack of diversity • cash flow difficulties arising from lack of liquidity	• review and agree investment policy • obtain proper investment advice or management • consider diversity, prudence and liquidity criteria • implement adequate reserves policy • use regular performance monitoring
Protection of permanent endowment	• loss of future income stream or capital values • buildings unfit for purpose • income streams inappropriate to meet beneficiary needs	• review and agree investment policy • obtain proper investment advice or management • consider diversity, prudence and liquidity criteria • use regular performance monitoring • ensure maintenance and surveyor inspection of buildings • review insurance needs
Compliance with donor imposed restrictions	• funds applied outside restriction • repayment of grant • future relationship with donor and beneficiaries • regulatory action	• implement systems to identify restricted receipts • agree budget control, monitoring and reporting arrangements

Potential risk	Potential impact	Steps to mitigate risk
Fraud or error	• financial loss • reputational risk • loss of staff morale • regulatory action • impact on funding	• review financial control procedures • segregate duties • set authorisation limits • agree whistle-blowing anti fraud policy • review security of assets • identify insurable risks
Counter party risk	• financial loss • disruption to activities or operations	• research counter party's financial sustainability • contractual agreement • consider staged payments • agree performance measures • monitor and review investments • establish monitoring and review arrangements where counter party is the charity's agent ('conduit funding' arrangements

Environmental or external factors

Potential risk	Potential impact	Steps to mitigate risk
Public perception	• impact on voluntary income • impact on use of services by beneficiaries • ability to access grants or contract funding	• communicate with supporters and beneficiaries • ensure good quality reporting of the charity's activities and financial situation • implement public relations training/procedures
Adverse publicity	• loss of donor confidence or funding • loss of influence • impact on morale of staff • loss of beneficiary confidence	• implement complaints procedures (both internal and external) • agree proper review procedures for complaints • agree a crisis management strategy for handling - including consistency of key messages and a nominated spokesperson
Relationship with funders	• deterioration in relationship may impact on funding and support available	• ensure regular contact and briefings to major funders • report fully on projects • meet funders' terms and conditions

Potential risk	Potential impact	Steps to mitigate risk
Demographic consideration	• impact of demographic distribution of donors or beneficiaries • increasing or decreasing beneficiary class • increasing or decreasing donor class	• profile donor base • profile and understand beneficiary needs • use actuarial analysis to establish future funding requirements
Government policy	• availability of contract and grant funding • impact of tax regime on voluntary giving • impact of general legislation or regulation on activities undertaken • role of voluntary sector	• monitor proposed legal and regulatory changes • consider membership of appropriate umbrella bodies

Compliance risk (law and regulation)

Potential risk	Potential impact	Steps to mitigate risk
Compliance with legislation and regulations appropriate to the activities, size and structure of the charity	• fines, penalties or censure from licensing or activity regulators • loss of licence to undertake particular activity (see operational risks) • employee or consumer action for negligence • reputational risks	• identify key legal and regulatory requirements • allocate responsibility for key compliance procedures • put in place compliance monitoring and reporting • prepare for compliance visits • obtain compliance reports from regulators (where appropriate) - auditors and staff to consider and action at appropriate level

Potential risk	Potential impact	Steps to mitigate risk
Regulatory reporting requirements: Financial and other reporting requirements will be dependent on how the charity is constituted and may also vary according to funding arrangements	• regulatory action • reputational risks • impact on funding	• review and agree compliance procedures and allocation of staff responsibilities
Taxation	• penalties, interest and 'back duty' assessments • loss of income eg failure to utilise gift aid arrangements • loss of mandatory or discretionary rate relief • failure to utilise tax exemptions and reliefs	• review PAYE compliance procedures • review VAT procedures • file timely tax returns • understand exemptions and reliefs available (direct tax and VAT) • take advice on employment status and contract terms and tax • implement budget and financial reporting identifying trading receipts, and tax recoveries
Professional advice	• lack of investment strategy or management • failure to optimise fiscal position • contract risks • failure to address compliance risks	• identify and ensure access to professional advice • identify issues where advice is required • conduct compliance reviews