TRUSTEES' SHORT GUIDE SERIES

# Risk Management.

## Basic charity governance and accounting.

**August 2026**

pem.

**Risk is the possibility of something bad happening and according to the Oxford English Dictionary has been used in a financial context since the 1600s. Good governance requires trustees to act in their charity's best interests and central to that is managing the risk that something bad will happen.**

In 2025 the Charity Commission produced its own sector risk assessment which highlighted financial resilience and risks to public benefit as its two spotlight risks. In addition the assessment considered 8 other areas of risk. Depending on the nature and activities of the individual charity the risk landscape will be very different and it is important that trustees map out the key challenges to their charity.

Trustees and management should also remember that risk is not always of failing to respond to 'something bad' but also the failure to exploit an advantage or take an opportunity and therefore risks should be framed and considered from both aspects.

# Identifying risks

Charity Commission guidance on risk management includes templates and examples of risks and mitigations and includes the following table to direct thoughts about risk. The table below sets out some examples of risks, including some highlighted by the Charity Commission.

| Risk category | Examples |
|---|---|
| Governance risks | ▪ Inappropriate organisational structure.<br>▪ Trustee body lacks relevant skills or commitment.<br>▪ Conflicts of interest.<br>▪ Too little impact/outcome information to set strategy. |
| Operational risks | ▪ Lack of beneficiary welfare or safety.<br>▪ Poor contract pricing.<br>▪ Poor staff recruitment and training.<br>▪ Doubt about security of assets.<br>▪ Inability to meet beneficiary donor expectations of technological change. |
| Financial risks | ▪ Inaccurate and/or insufficient financial information.<br>▪ Inadequate reserves and cash flow (e.g. reserves tied up in property or other illiquid assets).<br>▪ Dependency on limited income sources.<br>▪ Poor cost recovery.<br>▪ Inadequate investment management policies.<br>▪ Insufficient insurance cover.<br>▪ Competition for grants/funding.<br>▪ Poor segregation of duties. |
| External risks | ▪ Poor public perception and reputation.<br>▪ Demographic changes such as an increase in the size of beneficiary group.<br>▪ Turbulent economic or political environment.<br>▪ Changing government policy. |
| Compliance with law & regulation | ▪ Acting in breach of trust.<br>▪ Poor knowledge of the legal responsibilities of an employer.<br>▪ Poor knowledge of regulatory requirements of particular activities (e.g. fund-raising, running of care facilities, operating vehicles).<br>▪ Breach of data protection regulations. |

These categories may not be the most natural for trustees and a more focussed set of categories, tailored to the charity may be easier to promote discussions of risk.

- Competition
- Conflicts
- Cyber security
- Fraud
- Funding
- Information availability
- Leadership
- Natural disasters (pandemic, fire, flood)
- Overseas impact
- People
- Property
- Public benefit
- Regulation
- Reputation
- Safeguarding
- Social tensions
- Strategic direction
- Technology

However, any risk management is unlikely to be effective if a charity merely calls up a list of risks, ascribes some non-specific mitigations and files the paper away for another year. Whilst some risks are generic, and this is a good starting point, how that risk manifests will depend on individual circumstances.

For example, one charity might consider the risk around a large single source of funding to be financial, with the risk being how the charity funds activities if that funding is removed. However, another charity may consider that the restrictions around the use of funds do not give the charity sufficient flexibility to meet its full objectives. It is important therefore to understand the particular consequence or most significant consequence for the charity when designing the mitigating actions.

To be effective, risk management needs to be embedded in decision making, answering the question "what will prevent the charity from achieving that objective, outcome, activity?" Focusing on these questions can help the charity identify its risks and actions it needs to take more effectively.

## Assessing the risks

Risk is subjective, often based on an individual's experience or personal judgments. Therefore it is important that charity's trustees come together to understand their risk appetite for the charity, and the impact of that when prioritising and responding to risks. A too conservative or risk adverse attitude might mean that opportunities are lost, or mitigations are excessive and costly in time or expense in comparison to the risk. Whereas a relaxed attitude may jeopardise the charity's finances or reputation.

Risks are often assessed against a scale of likelihood and impact to help prioritise and create a visualisation of the significant risks impacting the charity. This assessment should consider both where the risk is currently and what the trustees consider to be an acceptable level for that risk, not all risks will be able to be completely negated. The task is then to design mitigating actions to move the risk to an acceptable level and maintain the risk at that level.

Charity Commission guidance gives an example of a heat map (page 16) that can be used to assess risk which has descriptors for impact and likelihood. Many charities ascribe a value to the impact to further help analyse the risk. The meaning of the rankings should be agreed by management and the charity trustees and used consistently for all risks.

Trustees should identify their favoured presentation, be it a heat map or other visual presentation of risks to create a summary, or a more simple table with highlights.

Each risk presented on the summary will need a detailed description plan and owner.

## Mitigating the risks

The risk appetite and assessment of risk highlights the principal risks which may stop the charity from achieving its objectives, and helps the charity identify strategies.

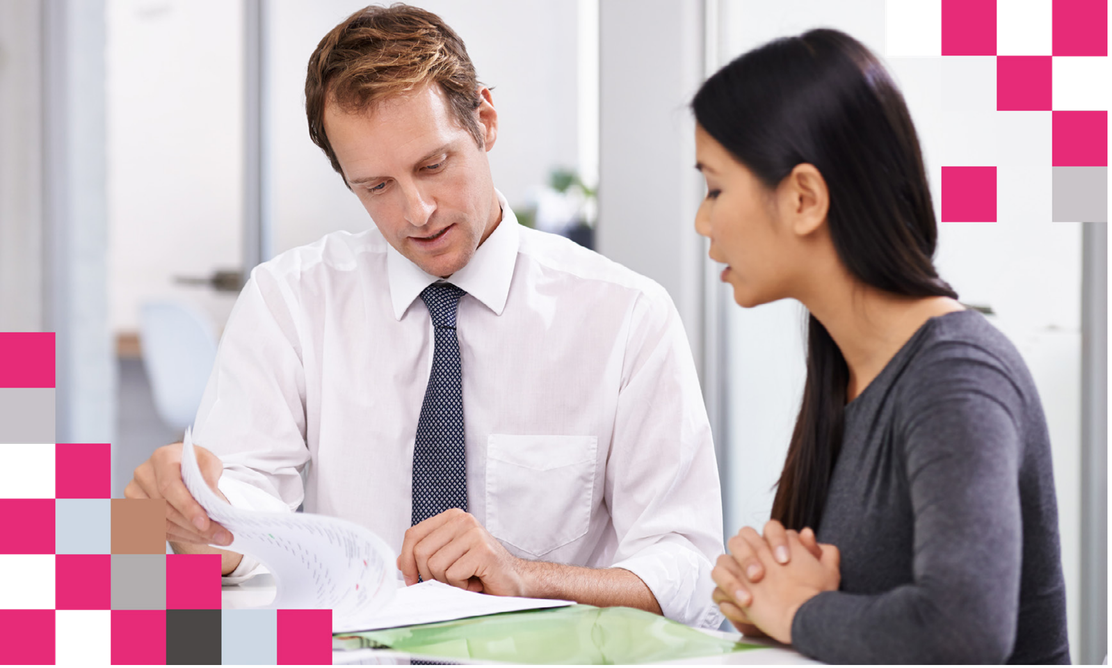
The following examples reflect the Charity Commission's guidance as ways to mitigate risk:

- The risk may need to be avoided by ending (or not starting) that activity (e.g. stopping work in a particular country).
- The risk could be transferred to a third party (e.g. use of a trading subsidiary, outsourcing or other contractual arrangements with third parties).
- The risk could be shared with others (e.g. a joint venture project).
- The charity's exposure to the risk can be limited (e.g. 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 (e.g. internal financial controls, controls on recruitment, personnel policies).
- The risk may need to be insured against (this often happens for residual risk, e.g. employers liability, third party liability, theft, fire, cyber).
- The risk may be accepted as being unlikely to occur and/or of low impact and therefore will just be reviewed annually.

This assessment can help direct the response as can understanding the risk appetite. The chart below, allocating the risks to the difference quarter, can provide visual impact and help focus attention on the most significant risks.

| Impact | | |
|---|---|---|
| | **High impact, *low* likelihood** - Mitigate effects/transfer | **High impact, *high* likelihood** - Avoid/ minimise likelihood |
| | **Low impact, *low* likelihood** - Accept | **Low impact, *high* likelihood** - Minimise likelihood/accept |

Likelihood



# Building your risk register

This risk register relies on having sufficient disaggregation of the risks to enable management and trustees to have understanding of the impact of the controls in place and how they mitigate the risk. For example a risk described as 'fraud risk' – with the response 'good internal controls' is unlikely to give trustees sufficient comfort that the risks are being managed. However a 'risk of unauthorised payments' is more likely to be successfully mitigated by a control around 'delegated authorities being set and reviewed and dual authorisations of payments'.

The level of detail in the risk register reviewed by trustees must be balanced as too detailed may be overwhelming such that the trustees cannot provide successful strategic oversight and insufficient detail may not give a clear indication of the tailored risk and response.

Each charity will need to consider what is right for that organisation. It may be that department risk registers are held separately, with only the most significant currently unmitigated risks and strategic risks being considered by the trustees.

**Risk code** - Give each risk a code. This makes it easy to refer to it with others (e.g. in a meeting).

**Risk** - Identify your risks with a basic description.

**Potential impact** - Understand the impact with a basic description of the consequences of that risk.

**Impact (1–5)** - Rate the initial impact based on your agreed scale.

**Likelihood (1–5)** - Rate the initial likelihood score based on your agreed scale.

**Initial risk score** - Calculate your initial risk score.

**Target risk score** - Think about your appetite for these risks. Give each one a target risk score that reflects the level of risk you'd be happy to accept.

**Current controls** - List the controls that you currently have in place to reduce and control each risk.

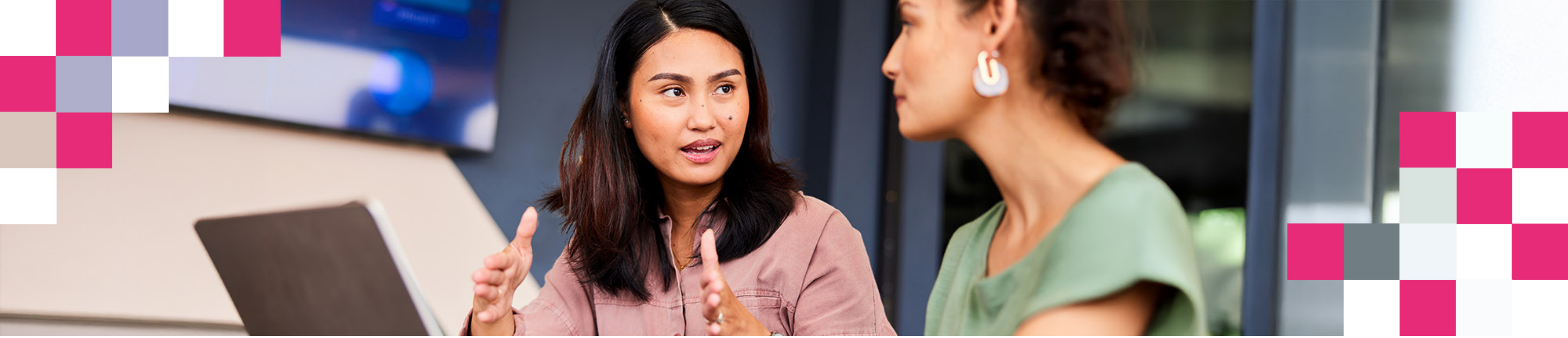
**Impact of current controls** - Assess the impact of the controls that you currently have in place to reduce and control each risk.

**Residual risk score** - Re-score your risk (impact and likelihood) after considering the controls that are in place and effective.

**Actions required** - If your residual risk score is higher than your target risk score (i.e., current controls don't reduce the risk to an acceptable level), list the additional actions needed to reduce the risk further.

**Risk owner** - Allocate someone to take oversight of the risk and implementation of the actions.

**Review timeframe** - For ongoing assurance that risks are being controlled effectively, record who is responsible for each risk and when/how they should review it.



## Reporting on risk

Trustees need to agree with management the processes around risk and the level of detail that they require of management and as part of board oversight. For risk management to be successful, considerations of risk and understanding the impact of mitigating actions need to be embedded in the organisation decision-making and actions and controls.

Risks may change frequently or may be relatively static depending on the nature of the charity and whilst an annual review is required for all, trustees will need to decide whether that is appropriate in their context or whether a more frequent review is required. Alongside the assessment of risk is the assessment of actions and controls: trustees are required to maintain sound internal financial controls, and must review those at least annually. It is likely to be most effective to undertake this review in conjunction with the review of risks.

## Next steps

We recommend that trustees review their risk management processes to ensure that:

- The risks being managed are those most likely to stop the charity from achieving its objectives.
- The mitigating actions are specific to the risk.
- All risks and actions have owners.
- Information and review cycles should be at least annual but also reflect the changing nature of the organisation.

## Resources

- Charity Sector Risk Assessment 2025
- Charities and risk management (CC26)
- Charity governance, finance and resilience: 15 questions trustees should ask
- Internal financial controls for charities

# Your Charities & Not-for-Profit team

## Audit and accounts

**Kelly Bretherick**
Partner, Audit
kbretherick@pem.co.uk

**Michael Hewett**
Partner, Audit
mhewett@pem.co.uk

**Nikki Loan**
Partner, Audit
nloan@pem.co.uk

**Grace Quist-Therson**
Director, Audit
gquist-therson@pem.co.uk

**Gemma Baratte**
Senior Manager, Audit
gbaratte@pem.co.uk

**James Rayson**
Senior Manager, Audit
jrayson@pem.co.uk

## Tax and VAT

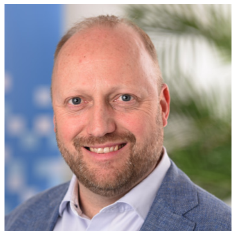
**Kate Millard**
Director, Employment Tax
kmillard@pem.co.uk

**Judith Pederzolli**
Director, Business Tax & SDLT
jpederzolli@pem.co.uk

**Robert Plumbly**
Director, VAT
rplumbly@pem.co.uk

**Michelle Harris**
Assistant Director, VAT
mharris@pem.co.uk

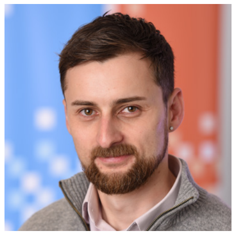
## Outsourcing: Virtual Finance Office (VFO)



**Andrew Turpin**
Partner, VFO
aturpin@pem.co.uk

**Melissa Guenigault**
Manager, VFO
mguenigault@pem.co.uk

## Independent examination



**Edward Spanner**
Manager, Accounts
espanner@pem.co.uk

**David Widdowson**
Assistant Manager, Accounts
dwiddowson@pem.co.uk

pem.co.uk

**PEM**
Salisbury House
Station Road
Cambridge CB1 2LA

**t.** 01223 728222
**e.** pem@pem.co.uk