Grant Thornton

CFG INSPIRING FINANCIAL LEADERSHIP

Charity Risk Benchmarking Study

Paul Rao

Director and Head of Charity Internal Audit and Risk Practice at Grant Thornton UK LLP

Contents

1. Background to the Study and the Top 10 Risks identified
2. Income and financial sustainability
3. Data Protection compliance (including GDPR)
4. Safeguarding
5. People, leadership, and culture
6. Cyber Security
7. Business continuity incidents

Top 10 Risks Charities Face (in no particular order)

#	Risk area	Risk defined
1	Income and financial sustainability	Insufficient income and reserves for a charity to achieve its strategic objectives and maintain its operations.
2	Data Protection compliance (GDPR)	An event or incident such as an external data breach or inadvertent internal error resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
3	Organisational change including digital transformation	The failure to execute organisational change and transformation programmes effectively and to achieve the intended benefits of these, resulting primarily in an inefficient use of the charity's resources.
4	Safeguarding	Failure to safeguard a charity's beneficiaries or associated vulnerable individuals including children, from abuse and maltreatment.
5	People, leadership and culture	Weaknesses or failure of leadership, inability to develop and retain talent effectively and an organisational culture that is not an enabler in the pursuit of a charity's strategy and objectives.

Top 10 Risks Charities Face (in no particular order)

6	Governance	The charity does not achieve its strategic, charitable, regulatory and ethical objectives due to inadequate governance at the Board and senior management / operational levels.
7	Regulatory	The charity fails to comply with applicable regulatory requirements, leading to reputational damage and financial penalties.
8	Cyber security	Cyber incidents (typically unauthorised or inappropriate access to an organisation's network) executed by external or internal parties that negatively impact the confidentiality, integrity and availability of a charity's information systems and data
9	Business continuity incidents	The occurrence of incidents that limit an organisation's ability to operate as it normally would in business as usual situations.
10	Reputation	A range of occurrences including incidents, events and outcomes that may consequently damage a charity's reputation. **Note:** Reputation risk is largely a consequence of other risk events materialising, however the study identified that charities are including it as a specific risk and therefore it was included in the top 10.

Income and financial sustainability

The risk is there being insufficient income and reserves for a charity to achieve its strategic objectives and maintain its operations.

The impact of **environmental, social, political and economic factors** on large charities over the last few years has demonstrated that the most common sources of income can quickly be stifled.

Covid-19 has had a particularly acute impact on the **forecasted incomes** of large charities by **limiting the capacity** to fundraise.

- Scenario planning and re-forecasting should be iterative exercises to combat the events that threaten business continuity or business as usual and periods of heightened uncertainty.
- Risk assess sources of income to identify those that are either more susceptible to reductions or loss or, through the opportunity lens, may potentially be expanded. These should feed into contingency plans and future strategic and organisational planning processes as charities consider the longer term effects of Covid-19 and the risk of a further outbreak.
- Volunteers for fundraising and other income generation activities should be well communicated with.

Data Protection compliance (including GDPR)

The risk is of an incident, such as an external data breach or inadvertent internal error, resulting in the accidental or unlawful **destruction, loss, alteration, unauthorised disclosure** of or access to personal data.

The GDPR is particularly relevant to charities due to their tendency to hold substantial amounts of personal and **sensitive special category** data related to their donors, beneficiaries and volunteers, as well as often undertaking significant **marketing activity**.

The **legal obligation to report** personal data breaches under the GDPR has also increased the potential exposure of charities to **financial penalties** and **reputational damage** that could be a consequence of a data breach.

- Establish and rigorously maintain records of data processing activity and an information asset register.
- Understand and manage the sharing of data among third parties.
- Develop an effective method for identifying and reporting data breaches in order to meet the GDPR’s 72-hour timescale.
- The relevant requirements of the Fundraising Regulator’s Code of Fundraising Practice and the GDPR must be fully considered, and compliance monitoring frameworks put in place.

Safeguarding

The risk is a failure to safeguard a charity's beneficiaries, employees, volunteers or other associated vulnerable individuals including children, from abuse and maltreatment.

This risk could have significant **personal impact** and **reputational damage**.

Safeguarding has gained **media attention** recently due to a range of concerns at high profile charities and is an area of **focus of the Charity Commission**.

- Clearly define principles and rules in a safeguarding policy.
- Implement robust controls for background and DBS checks.
- Provide tailored training.
- Provide easy escalations for safeguarding concerns.
- Ensure that safeguarding is a board driven area of control.

People, leadership, and culture

The risk is weaknesses or failure of leadership, an inability to develop and retain talent effectively and an organisational culture that is not an enabler in the pursuit of a charity's strategy and objectives.

Effective leadership is an key driver with a heightened focus in charities, particularly since the onset of the Covid-19 situation as staff have considered how leaders have **responded to the crisis**.

The **tone from the top, consistency of messaging** and **role modelling of desired behaviour** is key to **retaining and attracting staff**.

- Aim to develop a culture that is aligned with the charity's strategy and objectives.
- Focus on employee performance management (people management, check-ins, appraisals etc.) to ensure wellbeing (especially during a crisis) and talent management.
- Succession plans should be kept under regular review.

Cyber security

The risk is that cyber security incidents compromise the **confidentiality, integrity and availability** of a charity’s information systems and data.

We find a **range of weaknesses** regarding the governance arrangements and technical measures in place.

It is **constantly evolving** and therefore charities cannot afford to be complacent with their awareness and investment in cyber security measures.

- A training and awareness programme is one of the most effective preventive control measures. It should raise awareness of phishing and social engineering.
- Cyber risk and assurance must be driven by the Board.
- Develop a comprehensive patch management strategy.
- Review and test (e.g. penetrating testing) network perimeter configuration on a periodic basis.
- Due to Covid-19, there is a heightened need to ensure that the “Bring Your on Device” policies are clear and adhered to, and that the risks in relation to the use of these devices/tools are regularly reviewed and managed.

Business continuity incidents

The risk is that incidents limit an organisation's ability to operate as **business as usual**.

Covid-19 has fundamentally challenged the common perceptions of events that threaten business continuity held by management and trustees. It has forced organisations of all scales to **rapidly adopt remote working practices** capable of operating over much longer and highly uncertain time horizons.

- Strengthen Business Continuity Plans (BCPs) using lessons learned from Covid-19.
- Remove the traditional 'battle boxes' and 'war rooms' and take advantage of technology to streamline approaches to business continuity and enhance operational resilience.
- Build resilience and robustness into the IT environment. Charities should ensure that their IT strategies adequately address emerging trends, such as mobile devices and the Cloud, to strengthen operational resilience.
- Revisit the charity's business impact analysis (BIA). This information is used to determine how much should be spent on countermeasures and recovery facilities.

Paul Rao

Director and Head of Charity Internal Audit and Risk Practice

For Grant Thornton UK LLP

T +44 (0)7775 548 347

E Paul.Rao@uk.gt.com

Grant Thornton

grantthornton.co.uk