

# Charity and Non-Profit Organisations Risk Taxonomy

Risk Name	Risk Description	Potential Impact	How it Could Materialise	Potential Control and Remediation
<b>Financial Risk</b>	The risk of financial loss due to inadequate funding, mismanagement of funds, or unexpected expenses.	<ul style="list-style-type: none"> <li>- Loss of funds</li> <li>- Inability to continue operations</li> <li>- Damage to reputation</li> </ul>	<ul style="list-style-type: none"> <li>- Misallocation of budget</li> <li>- Reduction in donor contributions</li> <li>- Unforeseen expenses</li> </ul>	<ul style="list-style-type: none"> <li>- Regular financial audits</li> <li>- Maintaining a reserve fund</li> <li>- Diversifying income streams</li> <li>- Stringent budget controls</li> </ul>
<b>Operational Risk</b>	The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.	<ul style="list-style-type: none"> <li>- Service disruption</li> <li>- Increased costs</li> <li>- Inefficiencies.</li> </ul>	<ul style="list-style-type: none"> <li>- Staff errors</li> <li>- System failures</li> <li>- Process inefficiencies</li> </ul>	<ul style="list-style-type: none"> <li>- Implementing standard operating procedures</li> <li>- Regular training for staff</li> <li>- Investing in reliable systems</li> <li>- Continuous monitoring and evaluation</li> <li>- Business Continuity Planning</li> <li>- Crisis Management Framework</li> <li>- Disaster Recovery Planning</li> </ul>
<b>Compliance Risk</b>	The risk of legal or regulatory sanctions, financial loss, or damage to reputation due to non-compliance with laws, regulations, or internal policies.	<ul style="list-style-type: none"> <li>- Legal penalties</li> <li>- Fines</li> <li>- Reputational damage</li> </ul>	<ul style="list-style-type: none"> <li>- Failure to adhere to legal requirements</li> <li>- Lack of knowledge about regulatory changes or new regulations</li> </ul>	<ul style="list-style-type: none"> <li>- Regular compliance audits</li> <li>- Staying updated with regulatory changes including horizon scanning</li> <li>- Implementing robust compliance policies</li> </ul>
<b>Reputational Risk</b>	The risk of damage to the organisation's reputation due to negative public perception.	<ul style="list-style-type: none"> <li>- Loss of donor trust</li> <li>- Reduced donations</li> <li>- Loss of partnerships</li> </ul>	<ul style="list-style-type: none"> <li>- Negative media coverage</li> <li>- Public scandals</li> <li>- Service delivery failures</li> </ul>	<ul style="list-style-type: none"> <li>- Effective communication strategies</li> <li>- Transparency in operations</li> <li>- Swift response to negative events</li> <li>- Maintaining high ethical standards</li> </ul>
<b>Strategic Risk</b>	The risk arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.	<ul style="list-style-type: none"> <li>- Failure to achieve objectives</li> <li>- Loss of competitive edge.</li> </ul>	<ul style="list-style-type: none"> <li>- Poor strategic planning</li> <li>- Failure to adapt to changes in the external environment</li> </ul>	<ul style="list-style-type: none"> <li>- Regular strategic reviews</li> <li>- Stakeholder engagement</li> <li>- Flexible and adaptive planning processes</li> </ul>
<b>Cybersecurity Risk</b>	The risk of financial loss, disruption, or damage to the reputation of an organisation due to failure of its information technology systems.	<ul style="list-style-type: none"> <li>- Data breaches</li> <li>- Loss of sensitive information</li> <li>- Operational disruption.</li> </ul>	<ul style="list-style-type: none"> <li>- Hacking</li> <li>- Phishing attacks</li> <li>- Inadequate IT security measures</li> </ul>	<ul style="list-style-type: none"> <li>- Implementing robust cybersecurity measures</li> <li>- Regular IT audits</li> <li>- Staff training on cybersecurity awareness</li> <li>- Having a response plan for data breaches</li> </ul>
<b>Fraud Risk</b>	The risk of financial or reputational loss due to fraudulent activities within the organisation.	<ul style="list-style-type: none"> <li>- Financial loss</li> <li>- Legal consequences</li> <li>- Reputational damage</li> </ul>	<ul style="list-style-type: none"> <li>- Embezzlement of funds</li> <li>- False reporting</li> <li>- Misuse of assets</li> </ul>	<ul style="list-style-type: none"> <li>- Regular financial audits</li> <li>- Whistleblower policies</li> <li>- Strong internal controls</li> </ul>
<b>Safeguarding Risk</b>	The risk of harm or abuse to individuals within the organisation's care or service.	<ul style="list-style-type: none"> <li>- Harm to individuals</li> <li>- Legal consequences</li> <li>- Reputational damage</li> </ul>	<ul style="list-style-type: none"> <li>- Inadequate supervision</li> <li>- Lack of safeguarding policies</li> <li>- Failure to report incidents</li> </ul>	<ul style="list-style-type: none"> <li>- Comprehensive safeguarding policies</li> <li>- Regular training</li> <li>- Clear reporting procedures</li> </ul>
<b>Conflicts of Interest Risk</b>	The risk of decisions being influenced by personal interests rather than the best interests of the organisation.	<ul style="list-style-type: none"> <li>- Biased decision-making</li> <li>- Loss of trust</li> <li>- Legal consequences</li> </ul>	<ul style="list-style-type: none"> <li>- Personal relationships influencing decisions</li> <li>- Lack of transparency</li> <li>- Undisclosed interests</li> </ul>	<ul style="list-style-type: none"> <li>- Conflict of interest policies</li> <li>- Regular disclosures</li> <li>- Independent decision-making processes</li> </ul>
<b>People Risk including Key People Dependency</b>	The risk arising from dependency on key personnel and issues related to staffing.	<ul style="list-style-type: none"> <li>- Disruption in operations</li> <li>- Loss of key skills and knowledge</li> <li>- Decreased morale</li> </ul>	<ul style="list-style-type: none"> <li>- High turnover of key staff</li> <li>- Insufficient staff training</li> <li>- Lack of succession planning</li> </ul>	<ul style="list-style-type: none"> <li>- Succession planning</li> <li>- Staff development programs</li> <li>- Adequate staffing levels</li> </ul>
<b>Governance Effectiveness Risk</b>	The risk of ineffective governance impacting the organisation's performance and compliance.	<ul style="list-style-type: none"> <li>- Non-compliance</li> <li>- Inefficient operations</li> <li>- Reputational damage</li> </ul>	<ul style="list-style-type: none"> <li>- Lack of board oversight</li> <li>- Poor leadership</li> <li>- Inadequate policies</li> </ul>	<ul style="list-style-type: none"> <li>- Regular board evaluations</li> <li>- Clear governance structures</li> <li>- Effective leadership training</li> </ul>
<b>Access Control and Data-Security Risk</b>	The risk of unauthorised access to systems and data, leading to data breaches or loss.	<ul style="list-style-type: none"> <li>- Data breaches</li> <li>- Loss of sensitive information</li> <li>- Operational disruption</li> </ul>	<ul style="list-style-type: none"> <li>- Weak password policies</li> <li>- Lack of access controls</li> <li>- Phishing attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Strong access control policies</li> <li>- Regular security audits</li> <li>- Staff training on data security</li> </ul>