Carmichael.

# *Sample Completed Risk Register*

***There are a number of approaches and frameworks for developing an organisation's Risk Management System and Risk Register. This document reflects the framework recommended by the Charities Regulator, though any non-profit may find it useful. This document is intended for guidance only and all organisations should develop their own Risk Management System and Risk Register.***

**Introduction**

The identified risks are grouped under 7 key risk areas.

**Key Risk Areas**

1. **Governance (G)**
2. **Strategic (S)**
3. **Compliance (legal & regulatory) (C)**
4. **Operational (O)**
5. **Financial (F)**
6. **Environmental or External (E)**
7. **Reputational (R)**

Each risk on the register is given a brief description of the potential risk for the organisation and the potential impact if the risk was to occur. Each risk is also assigned a Risk Owner who has oversight responsibility for monitoring the risk and the implementation/ review of the steps to be taken to mitigate the likelihood of the risk occurring or if it does occur, the impact on the organisation. The monitoring frequency is specified and the risk owner needs to ensure that this monitoring occurs.

Each of the risks are assessed in terms of (1) likelihood of the risk occurring on a scale of 1 – 5 where 1 is very unlikely and 5 is very likely; (2) the impact for the Organisation if the risk was to happen also rated on a scale of 1 -5 and (3) the controls in place or steps to be taken to mitigate the risk. The controls are rated of a scale of 1 to 3 where 1 it is felt that the controls are very effective and 3 an assessment that the controls or steps are not very strong and/or likely to be effective in preventing the risk or the mitigating its impact if it did occur. The risk score is determined by multiplying the risk impact by the risk likelihood by the effectiveness of the controls. (Likelihood X Impact) X Controls.

The following traffic light system is used on a risk register to highlight / prioritise risk:

| Risk Level | Risk Score |
|---|---|
| High | 25+ |
| Medium | 13 – 24 |
| Low | 0 – 12 |

The Risk Committee oversees the preparation and regular update of the risk register, the monitoring of risks and the regular review and assessment of the Highest Risks to determine if any new or additional steps to mitigate or control the risk should be implemented. The Risk No Column can be colour coded to reflect the Risk Score, for example:

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| F1 | Dependency on a limited number of income/funding sources | Cash flow and budget impact of loss of income source | CEO | • Identify major funding/income source dependencies<br>• Implement adequate reserves policy | Annual review of the risk by the Risk Committee reporting to the board. The review will assess;<br>• Adequacy of reserves to sustain an income shock<br>• Opportunities for income diversification or to develop additional income sources | 3 | 4 | 2 | 24 |

**Risk Register**

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| Risk Category: **Governance** | | | | | | | | | |
| G1 | Board lacks relevant skills or commitment to meet its responsibilities and duties | • The Organisation becomes moribund or fails to achieve its purpose<br>• Oversight and guidance of the organisation is inadequate<br>• Key decisions are made that bypass the Board<br>• Attendance by board meetings is poor and difficulties in getting | Chairperson | • Conduct regular board skills audits and agree skills required<br>• Develop and review annually a board succession plan<br>• Provide induction for new board members This is done for all new members<br>• Review board training needs and provide relevant training to board | Annual review of the risk by the Risk Committee reporting to the board. The review will assess;<br>• Skill needs/gaps of the board<br>• Actions/updates needed to the succession plan | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | a quorum for board meetings<br>• Board sub committees meet irregularly and are not focused<br>• Poor decision making reflected in poor service delivery and dissatisfied clients, members and funders<br>• Resentment or apathy amongst staff | | members Item for discussion by Risk Committee and to make recommendations to board | | | | | |
| G2 | Loss of key staff/ staff retention | • Experience or skills lost<br>• Operational impact of key projects and priorities<br>• Loss of contact base and corporate knowledge | Risk Committee and the CEO | • Succession planning On-going<br>• Document systems, activities and projects<br>• Implement training programme On-going<br>• Agree notice periods and handovers<br>• Ensure adequate terms and conditions for all staff, in line with industry norms<br>• Ensure a vibrant and supportive working environment<br>• Put in place effective performance management structures to stimulate and support excellent | Annual review of the risk by the Risk Committee reporting to the board of adequacy/effectiveness of the mitigation steps to manage/minimise this risk. The review will assess the positions considered to be most at risk and if any additional measures need to be put in place. | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | work performance and motivation | | | | | |
| G3 | Quality of reporting to Board (accuracy, timeliness & relevance) | • Inadequate information resulting in poor quality decision making<br>• Failure of board to fulfil its control functions<br>• Board becomes remote and ill informed | Chair | • Assessed as part of annual board evaluation process. Positive responses from board members on quality | Annual review of the risk by the Risk Committee reporting to the board of adequacy/effectiveness of the information provided to the board. | | | | |
| Risk Category: **Strategic** | | | | | | | | | |
| S1 | The Organisation lacks an appropriate strategic direction or focus that is in tune with the evolving needs and business /operating environment | • The organisation drifts with no clear objectives, priorities or plans<br>• Issues are addressed piecemeal with no strategic reference / context<br>• Difficult decisions are avoided or put on the long finger<br>• Needs of beneficiaries not fully addressed<br>• Financial management difficulties<br>• Loss of reputation | Board | • Develop and monitor 3-year strategic plan which sets out the key aims, objectives and targets of the Organisation<br>• Regularly review (at least every 5 years) the Organisation's vision and constitution Review of Constitution<br>• Develop and monitor annual operational/ business plans<br>• CEO's report to the Board mapped against strategic aims and objectives | Annual review of this risk by the Strategy, Committee reporting to the board of adequacy/ effectiveness of the mitigation steps to manage/minimise this risk | | | | |
| S2 | The Organisation does not have the flexibility or the sustainability to survive a major | • Dramatic loss of income up to closure of some parts of all operations of the Organisation | Board | • Review the experience of the Covid-19 pandemic and assess what worked well and what should be done | Annual review of the risk by the Risk Committee reporting to the board of adequacy/effectiveness of the mitigation steps to manage/minimise this risk. | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | catastrophic event such as global pandemic | | | differently if a similar catastrophic event were to reoccur<br>• Review and update the Disaster Recovery and Business Continuity Plan in light of the Covid-19 experience.<br>• Build/Maintain strong reserves to provide emergency funding to keep operations going while responses to the loss of income are being developed.<br>• Maintain good relations with funders and national bodies | | | | | |
| S3 | Ineffective or inappropriate organisational structure | • Lack of information flow and poor decision-making procedures<br>• Certain activities may not get appropriate management direction and oversight<br>• Certain activities may get too much time given their relative importance or contribution | CEO | • Use organisation chart and job roles & responsibilities to provide a clear understanding of roles and duties<br>• Develop a scheme of delegated authority to the CEO<br>• Delegation and monitoring should be consistent with good practice<br>• Conduct regular reviews of the | Review of the risk by the Strategy Committee at least once every 3 years as part of the strategic development process reporting to the board of adequacy/ effectiveness of the mitigation steps to manage/minimise this risk | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | • Remoteness of senior managers /staff from operational activities<br>• Uncertainly or lack of clarity as to roles and duties<br>• Decisions made at an inappropriate level of excessive bureaucracy<br>• Decision bottlenecks due to too many decisions being taken by one or two individuals<br>• Uneven workloads | | organisation structure, and the allocation of responsibilities and time | | | | | |
| Risk Category: **Compliance (Legal or Regulatory)** | | | | | | | | | |
| C1 | Compliance with legislation and regulations appropriate to the activities, size and structure of the charity | • Fines, penalties or censure from licensing or activity regulators<br>• Loss of licence to undertake a particular activity<br>• Employee or beneficiary take action for negligence<br>• Suffer damage to our reputation | CEO | • Identify key legal and regulatory requirements that apply to the Organisation<br>• CEO submits a compliance report annual to the board<br>• Allocate responsibility for key compliance procedures<br>• Put in place a process for compliance monitoring and reporting to the board overseen by the Risk Committee | CEO to submit a legal & regulatory compliance report to the board annually.<br><br>Risk Committee to regularly review and assess the risk register & mitigation steps to report to the board<br><br>All compliance reports/ concerns received from the CRA, funders or regulators to be brought to the attention of the board. | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | • Maintenance and regular review of the Organisation's risk register overseen by the Risk Committee<br>• Prepare for compliance visits<br>• Review compliance reports /concerns from regulators, inspectors, auditors and staff when received take appropriate action to address issues/ concerns | | | | | |
| C2 | Regulatory and funder reporting requirements are not adequately met | • Regulatory action taken against the Organisation<br>• Suffer damage to our reputation<br>• Negative impact on future funding | CEO | • Review and agree compliance procedures and allocation of staff responsibilities | CEO to confirm to the board annually that all regulatory and funder reporting requirements have been met<br><br>All compliance reports/ concerns received from the CRA, and any other funders or regulators to be brought to the attention of the board. | | | | |
| Risk Category: **Operational** | | | | | | | | | |
| O1 | Inadequate Disaster Recovery & Business Continuity planning | • Computer systems failures or loss of data<br>• Destruction of property, equipment, records through fire, floods or similar damage | CEO | • Review and update the Disaster Recovery and Business Continuity Plan in light of the covid-19 experience.<br>• Review & update the IT back-up & recovery plan | Annual review of the risk and assessment of the mitigation steps by the Risk Committee reporting to the board | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | • Implement and periodically test the data back-up procedures and security measures<br>• Review insurance cover at least once every 3 years<br>• Review/update disaster recovery plan at least once every 3 years | | | | | |
| O2 | Poor Health & Safety | • Staff injury<br>• Service liability<br>• Ability to operate all or some of our services curtailed or suspended<br>• Injury to Resident Member staff, visitors and the public | CEO | • Comply with the law and regulations<br>• Get our external safety advisors to review and update our safety plan<br>• Train staff and safety officer<br>• Put in place monitoring and reporting procedures | Annual review of the risk and assessment of the mitigation steps by the Risk Committee reporting to the board | | | | |
| O3 | Poor staff performance, morale or attitude | • Employment disputes<br>• High staff turnover rates<br>• Health & Safety issues<br>• Claims for injury, stress, harassment, unfair dismissal<br>• Equal opportunity & diversity issues<br>• Adequacy of staff training<br>• Low morale | CEO | • Review regularly the effectiveness and quality of our recruitment process<br>• Ensure that all new staff receive a structured induction training<br>• Adhere to the Organisation's policies for checking references, job descriptions, contracts of employment, | Annual review of the risk and assessment of the mitigation steps by the Risk Committee reporting to the board | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | • Abuse of vulnerable staff or clients | | appraisals & feedback procedures<br>• Create a positive working environment and culture where staff feel safe in raising concerns<br>• Implement job training and development<br>• Assess regularly the on-going training needs of staff<br>• Implement health & safety training and monitoring<br>• Communicate the Organisation's protected disclosure (whistle-blowing) policy | | | | | |
| Risk Category: **Financial** | | | | | | | | | |
| F1 | Dependency on a limited number of income/funding sources | Cash flow and budget impact of loss of income source | CEO | • Identify major funding/income source dependencies<br>• Implement adequate reserves policy | Annual review of the risk by the Risk Committee reporting to the board. The review will assess;<br>• Adequacy of reserves to sustain an income shock<br>• Opportunities for income diversification or to develop additional income sources | | | | |
| F2 | Danger of Fraud or error | • Financial loss<br>• Reputational risk<br>• Loss of staff morale<br>• Regulatory action | Finance Manager | • Review financial control procedures<br>• Segregate duties<br>• Set & review authorisation limits | Risk monitored by the Audit & Finance Committee reporting to the board. The monitoring will include following reviews/ | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | • Impact on existing and future funding | | • Review security of assets<br>• Identify insurable risks | assessments of the following areas (undertaken at least once every 3 years);<br>• Adherence to and adequacy of financial control procedures<br>• Confirmation that key risk duties are segregated<br>• Adherence to and adequacy of the set authorisation limits<br>• Adequacy of the insurable risks cover | | | | |
| F3 | Cyber breach | • Loss of funds (phishing)<br>• Loss of important data (personal, account, passwords)<br>• Reputational damage | CEO & Finance Manager | • Identify and assess main vulnerability areas and implement appropriate control measures<br>• Develop a cyber-security guidance document for staff<br>• Maintain staff awareness and alertness to cyber fraud to regular reminders and communication<br>• Obtain and implement prevention advice and measures from experts, insurers and financial service providers<br>• Keep firewall and anti-virus software up to date | Annual review of the risk and assessment of the mitigation steps by the Risk Committee reporting to the board | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | • Advise staff working remotely of the need to adhere our cyber risk controls and procedures<br>• Avail of relevant training and guidance | | | | | |
| Risk Category: **Environmental or External** | | | | | | | | | |
| E1 | Loss of statutory funding, Lack of available staff/ skills in the sector or a limitations on available funds or staffing and as a result we are unable to fully meet the needs of our service users | • Inability to provide services | CEO | • Ensure regular contact and briefings to major funders<br>• Report fully on projects<br>• Meet funders' terms and conditions<br>• Ensure maintenance of existing good relationships with all stakeholders | Annual review of the risk by the Risk Committee reporting to the board | | | | |
| E2 | Competition from similar not-for-profit and for profit organisations providing similar services and supports to us | • Loss of income<br>• Reduced public profile<br>• Profitability of trading activity – services run at a loss or require subsidisation from other activities | CEO | • Monitor and assess performance and quality of our services<br>• Enhance and innovate<br>• Review market assessments and methods of service delivery<br>• Ensure regular contact with funders and service users<br>• Monitor public awareness and profile | Annual review of the risk by the Risk Committee reporting to the board | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | • Strategic selection of markets segments that we wish to target and serve.<br>• Explore, assess and regularly opportunities for collaboration, partnership, joint ventures or mergers | | | | | |
| Risk Category: **Reputational** | | | | | | | | | |
| R1 | Adverse publicity generated by the Organisation | • Loss of funder confidence or funding<br>• Loss of influence<br>• Impact on staff morale<br>• Loss of confidence by service users | Risk Committee | • Monitor complaints received (both internal and external)<br>• Agree and regularly review a crisis management strategy for handling adverse publicity including consistency of key messages and nominated spokesperson | Annual review of the risk by the Risk Committee reporting to the board | | | | |
| R2 | Poor service provision leading to poor customer satisfaction | • Customer/Beneficiary complaints<br>• Loss of fee income<br>• Loss of new business<br>• Suffer damage to our reputation | CEO | • Agree quality control procedures<br>• Monitor complaints and service user feedback<br>• Enhance and innovate services and systems<br>• Conduct regular service satisfaction surveys | Annual review of the risk by the Risk Committee reporting to the board | | | | |
| R3 | Changes to Government policy that have | • Availability of contract and grant funding | Risk Committee | • Monitor proposed legal and regulatory | Annual review of the risk by the Risk Committee reporting to the board | | | | |

| Risk No | Description of Potential Risk | Description of Potential Impact | Risk Owner | Steps to Mitigate | Monitoring Frequency | Likelihood (1-5) | Impact (1-5) | Controls (1-3) | Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | an adverse impact on the Organisation or the wider sector | • Impact of general legislation or regulation on activities undertaken by the Organisation<br>• Role of the C&V sector undermined/ unvalued | | changes (e.g. Charities Act)<br>• Participate in relevant umbrella /membership bodies<br>• Lobby government in relation to relevant issues that impact on the sector | | | | | |

**List of High Rated Risks**

| | |
|---|---|
| Risk No | Copy risk from above |

| | |
|---|---|
| Risk No | Copy risk from above |

**The matrix for assessing impact, likelihood and effectiveness of existing controls**

Each risk is scored in terms of:
* **likelihood** i.e. the probability of future occurrence, how likely the risk it is that the risk will occur and how frequently it has occurred in the past.
* **impact** i.e. the impact on the organisation and external stakeholders if the risk occurs.
* **effectiveness of existing controls** i.e. given the controls which are currently in place, how effective are they at mitigating the risk.

A scale of **1** to **5** is used for **Likelihood** and **Impact**, and **1** to **3** is used for the effectiveness of existing **Controls**, according to the following matrix:

| **Likelihood**<br>Scale of 1 - 5 | **Impact**<br>Scale of 1 – 5 | **Controls**<br>Scale of 1 - 3 |
|---|---|---|
| 1 = Rarely, if ever | 1 = No significant impact | 1 = Controls highly effective |
| 2 = Possible | 2 = Minor impact | 2 = Controls effective, but could be improved |
| 3 = Likely | 3 = Significant but containable impact | 3 = No controls / controls are ineffective |
| 4 = Very Likely | 4 = High impact | |
| 5 = Unavoidable / already occurring | 5 = Extremely detrimental impact | |

The risk score is determined **by multiplying the risk impact by the risk likelihood by the effectiveness of the controls**.