Risk Management Policy

Charity Commission Guidance

The Charity Commission strongly recommends that charities have a clear risk management policy and process to identify and manage all types of risks, and embed risk management into the charity's work. CC26 provides guidance.
If any staff notice an element of risk whilst at work, whether it be a risk to themselves, their clients, or the public, it is that staff member's duty to report the risk.

Responsibilities

The Board has overall responsibility for ensuring that there is an appropriate system of controls, financial and otherwise in place and working effectively. The systems of financial control are designed to provide reasonable, but not absolute, assurance against material mis-statement or loss. These include:

- a strategic plan and an annual business plan and budget approved by the Board.
- regular consideration by the Board of financial results and variance from budgets.
- delegation of authority and segregation of duties.
- management of risk.

The overall risk framework is managed by the Executive. The Board exercises oversight and scrutiny through the Committee.

1. *Reporting risks*

1.1. Reducing risk must take priority. Any risk that would pose an immediate threat must be acted upon instantly in order to reduce risk.

1.2. Through the Sanctuary Management Console Software (SMC Software©2006) on the General Office computer click the 'Open Risk Assessments' button.

1.3. Click the Add New Risk Assessment button. This will have the current date automatically entered.

1.4. Complete all sections of the form.

1.4.1. If any member of staff is uncertain as to what to type into the form he/she must seek the help of the Health & Safety Officer.

1.5. Close the form.

1.6. Team Leaders will complete risks forms from information in the SMC on Ellis Whittam WorkNest Portal.

2. *Monitoring and Responding to Risk Assessments*

2.1. The risk assessment form is a permanent addition to the minutes of the Staff Meetings.

2.2. The Chair of the meeting will read out recent risk assessments so that all staff are aware of them and the action required can be delegated accordingly.

2.3. All staff have a personal responsibility for their safety and a corporate responsibility for the safety of others. Therefore, all staff must regularly view risk assessments through the Management Console in order to be aware of the risks around them.

2.4. All paper risk assessments pre Management Console are available to view in a file kept in the General Office.

2.5. The Health & Safety Officer will monitor risk assessments according to his professional agenda and will delegate action required to the most appropriate person(s) or organisation(s).

2.6. Policies, procedures and working protocols will be changed, reviewed and modified whenever necessary in order to reduce risks.

2.7. Notices and posters will be displayed wherever necessary to inform of identified risks so that they can be avoided or appropriately managed.

3. *Managing Organisational Risk*

3.1. Strategic Risk. Longer-term risk is assessed in the Strategic Plan using techniques such as SWOT and PESTLE. These are covered in the strategy module.

3.2. In-year. Risk is managed using the risk management cycle and framework, which are outlined below.

3.3. Continuity Planning. There is also a separate Business Continuity Plan to manage unforeseen events requiring either temporary or permanent relocation.

3.4. Cyber Security. Most cyber-attacks are composed of four stages: Survey, Delivery, Breach and Affect. This National Cyber Security Centre (NCSC) infographic outlines security controls, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber-attack.

4. *Risk Management Cycle*

4.1. Risk is managed by means of a cycle of identification, quantification, management and review.

4.1.1. Identification. Identify the various risks that may materialise.

4.1.2. Quantifying. Assess and quantify these risks.

4.1.3. Managing. Take appropriate action to manage these risks. This is usually the weakest area in a risk management framework. Risks can be managed as follows:

4.1.3.1. Avoidance. Action that can be taken to avoid a risk occurring.

4.1.3.2. Mitigation. Action that can be taken to reduce the impact a risk may have, if it occurs.

4.1.3.3. Buying Out. Generally, this is done using insurance.

4.1.3.4. Accepting. Risk cannot be eliminated entirely and any steps taken to manage risk must be reasonable, as resources are not unlimited in terms of money and time. Equally, adopting a purely risk averse approach limits opportunity.

4.1.3.5. Reviewing. Risks should be reviewed as regularly as is necessary, depending on their likely probability and impact in the light of changing circumstances. This may be done on an ongoing basis, at appropriate points in projects or at regular meetings.

5. *Risk Framework*

5.1. Identification. The list of individual risks by category is in the Master Risk and Scoring Totals Spreadsheet. There are 50+ risks in 11 categories; compliance, external, governance, facilities, finance, income, IT, people, PR/Brand, strategy and upside.

5.2. Quantifying. A risk scoring exercise is carried out with each risk assessed in terms of its potential impact and likelihood on a scale of 1 to 10. If upside risks are included, the impact score should be negative, as these reduce overall risk. The average of the responses for each risk is used as the gross risk score for that risk.

5.3. Management.

5.3.1. Traffic Lights. Many organisations use a traffic light system to simplify managing risk. One way of doing this might be to objectively assess gross risk scores as follows:

Risk level acceptable, does not pose substantive threat to objectives	**Risk level high** and poses potential threat to achieving objectives	**Key Risk - too high** and poses serious threat to achieving objectives.
Less than?	More than?	More than?
Reported To		
Risk lead (CEO)	Executive Team	Board
Managed By		
Staff team	Risk lead (Buildings H&S manager)	Executive

5.3.2. Key Risks.

- Key risks (and possible amber risks) should be included in the Risk Management Plan spreadsheet with their likelihood and impact scores and the appointment of whoever leads on each risk.
- Risk leads should then identify what action will be taken and include this in the relevant section:
  - Avoidance – will help prevent the risk occurring.
  - Mitigation – will reduce the impact if it did occur.
- Then estimate how much this will reduce the risk and insert a percentage in the relevant column for each risk.
  - For example, if it would halve the likelihood of the risk occurring insert 50% in the avoidance % column and, if it would reduce the impact by three quarters, insert 75% in the mitigation column.
- Once the plan has been completed, it should be reviewed by the CEO/Executive Team to ensure that the:
  - Various actions are realistic and will be delivered.
  - Estimates are prudent.
  - Net risk for all risks is acceptable – within the charity's risk appetite.
- The Risk Management Plan should be reviewed by the Finance (or other) Committee and approved by the Board annually with updates presented to each meeting.
  - Where risk management action isn't working as planned, the action being taken and expected outcome should be reported in the CEO/director's reports.
- Management of key risks should be reflected in appraisal objectives.

5.3.3. Other Risks.

- Responsibility for action to manage other risks should be delegated down and may be managed in several ways, including:
- Having risk as a standing agenda item at executive or other meetings.
- Setting specific risk responsibilities as appraisal objectives.
- Including risk responsibilities in job descriptions.
    - This could include appointing an individual with specialist expertise to coordinate managing a risk across the charity.
    - For example, for safeguarding or H&SW.
- Automatically including as part of the planning process for projects and programmes.
- Posters and information in newsletters – eg H&SW, safeguarding, environmental.

Training