Paper for Board November 17th/18th.

From Jon Davies.

Towards an effective risk management strategy.

Recommendations

That the Board delegate staff to assess our risks, create a strategy to deal with them and report back to the next board meeting.

Specifically:

1. We formulate a general statement about risk culture.
2. Agree a format for staff and Board to oversee and manage risks.
3. That a set of risks is identified and put through the impact/likelihood formula so that for 2012/13 they become the risks that are monitored/managed.
4. We agree a frequency of CEO and Board oversight of risks.

Introduction

It is important for any organisation to think about what risks it could face and how it would deal with them.

To quote the National Council for Voluntary Organisations (NCVO)

> For charities, a risk can be defined as "any event or action that may harm an organisation's ability to achieve its charitable objectives and execute its strategies". This definition means that risk is not confined just to the financial affairs of the organisation, but to all areas of the charity's operations

Risk management does not have to be seen as a threatening or negative activity. Instead risk can be seen as an opportunity.

Grading risk is crucial. The risk of running out of pens would be accommodated within day to day practices. The risk of being hit by an extra-terrestrial meteorite on the other hand may be too extreme to contemplate. We can also be too risk averse and miss out on possibilities.

NCVO sees risk as having three components:

- **Hazard**: risk of bad things happening
- **Uncertain outcomes** : not meeting expectations
- **Opportunity**: exploiting the upside (for example, the possibilities of increasing investment returns with the *Trustee Act 2000* which gives wider powers of investment but also a statutory duty of care)

And coming from inside or outside:

> Risks are either 'external' or 'internal' to the organisation. An example of external risk would be changes in economic conditions or public perceptions. The HIV / AIDS charities found in the middle of the 1990s that their income from government and public fundraising was in decline. An 'internal' risk could be a failure in operational or financial controls, for example, fraud.

Risk affects all parts of the organisation:

- **Strategic**: the risk of not meeting strategic objectives
- **Operational**: failure in operation, which may in turn impact on charitable objectives, for example a fundraising campaign that fails to meet its target
- **Financial**: not maximising returns or losing money for example leaving excess funds in a current

bank account instead of a high return account

- **Regulatory**: failure to meet regulatory requirements
- **People**: failure to maximise performance or minimise loss

Wikimedia UK needs to be realistic and think about the sort of risks that we hope we won't be subject to but need to be ready for.

The whole board is responsible

Trustees are responsible for setting the climate regarding risk and assessing and managing risks in all aspects of their organisation. The work may well be delegated to the staff but oversight will remain a board responsibility.

How do we create a risk management strategy?

Risk management process has three aspects

- **Risk assessment**:identify all the factors, events and situations that could present a risk to the organisation
- **Risk analysis**: sort, score and rank risks as the basis for making decisions about how to handle them
- **Risk management**: develop strategies and methods to avert or minimise risk

A lot of the heavy lifting on this will be down to staff but the board has a crucial role to play in setting the tone and regular monitoring.

- Some key questions:

- **What do *we* mean by Risk Culture?**
- **How much risk do we feel we can accept?**
- **Why is risk culture important? How does culture affect risk management?**
- **What are the advantages of having a risk strategy**?
  What can the board do about risk culture?
- **How can the board support this strategy?**

Levels of acceptable risk may well be different on different topics - for example a new project may be high risk in terms of its success but be in line with strategy, and totally normal. A financial risk would always have to be kept very low - so we need to distinguish between activities/project development and compliance issues of law, finance etc.

In practical terms:

•Are we providing consistent, coherent, sustained and visible leadership in terms of how we expect our people to behave and respond when dealing with risk?

•How do we establish sufficiently clear accountabilities for those managing risks and hold them to their accountabilities?

•Can people talk openly without fear of consequences or being ignored?

•How do we acknowledge and live our stated values when addressing and resolving risk dilemmas?

•How do the organisation’s structure, processes and reward systems support or detract from the development of our desired risk culture?

•Do we have sufficient organisational humility to look at ourselves from the perspective of stakeholders and not just assume we’re getting it right?

•How do we satisfy ourselves that new joiners will quickly absorb our desired cultural values?

•How do we support learning and development associated with raising awareness and competence in managing risk at all levels?

•What training have we as a board have had in risk?

What success might look like

•Distinct and consistent tone throughout the charity.

•Commitment to ethical principles

•Common acceptance of the importance of continuous management of risk

•Transparent and timely risk information

•Encouragement of risk event reporting and whistle blowing, actively seeking to learn

•Risk management skills and knowledge valued, encouraged and developed,

•Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged

•Alignment with employee policies.

Some practical examples:

> ***Example: Board concerned about its overall risk strategy and compliance with the SORP***
>
> Undertake potential full reviews of methods and processes organisation uses, and recognise, manage and harness the power of risk to ensure compliance.
>
> ***Example: Board concerned with potential level of fraud***
>
> Idenitfy potential areas of fraud and establish effective fraud prevention and detection function.
>
> ***Example: Board of a children's charity concerned about confidentiality and security of data***
>
> Undertake comprehensive review of IT security policy including compliance with relevant legislation, that is Data Protection Act.

Our currently identified risks.

In our case we have identified the following risks and actions, (some updated from UK wiki others, more sensitive are on the office wiki):

Fundraiser risks (out of date given recent events but for illustration).

The WMF changes the arrangements for sharing funds from the WMF fundraiser.

> Action:
> Maintain a reserve fund so WMUK has time to downsize to a size appropriate to our new resource base after this change.

Infrastructure Issues

- **Debit integration needs sorting**

  Actions:
  - Work with key developer to ensure implementation within timescale.
  - Contingency planning to manage without integration, but with improved donation workflow and manual data imports to ensure good stewardship

- **Payment processor problems**

  Actions:
  - Meet with our supplier to discuss any likely service disruption and contingencies should such occur
  - Fundraising Manager to work with WMF to negotiate issues around any PayPal service disruption
  - Fundraising Manager to oversee a checking/testing schedule when fundraiser is live to identify problems when they occur, avoiding prolonged outage without notice
  - Fundraising Manager to work with WMF contractor to ensure through infrastructure testing prior to launch of fundraiser to identify any errors

Data storage and access

- **The CRM 'workload' issues**

  Actions:
  - Extensive testing pre-November of data import and export mechanisms and processes
  - Preparation for time-heavy processing of large data sets
  - Have considered option of increasing time-out length of server in extreme circumstances on advisement

- **Data protection issues**

  Actions:
  - Have valid data protection insurance
  - Have valid and sufficient SSL certification in place
  - Fundraising Manager to have oversight of those with differing access to different areas of managing the fundraiser, and ensure appropriate agreements are signed and access in line with | Calidicott principles

- **Freedom of Information issues**

  Actions
  - Fundraising Manager to draw up process to responding to Subject access or freedom of information requests.
  - Fundraising Manager work with Chief Exec to manage responses to any FoI or Subject Access requests to ensure compliance.
  - Fundraising Manager to seek to pre-empt requests by timely sharing of anonymised data and results through public wiki whenever appropriate and in a planned fashion.

- **Advertising Standards Agency compliance**

  Actions:
  - Fundraising Manager to working with ASA's Copy Advice service to check appeals text for banners and landing pages, and linked pages with further info.

- **Poor donor stewardship**

  Actions:
  - Fundraising Manager to plan how staff and volunteer resources to manage queries
  - Fundraising Manager to organise refreshed templates for thanking donors and trial bulk mailings
  - Fundraising Manager to schedule communications are timely and relevant to avoid 'spamming' audiences

Other financial risks

Financial risk - we run out of the funds needed to support our plans.

Action:

Create and adhere to good practice financial systems and protocols.

Build in contingency planning to budget

Create reserves to ensure at least one year of continuing activities.

Financial risk - we are subject to fraudulent activity from within or outside.

Action: Maintain exemplary financial systems and ensure they are adhered to through regular monitoring and professional external audit.

Have regular external overview of our activities and practices.

Organisational risk

The UK community fractures with disagreements between its members and constituent parts

Action:

Continue open and transparent systems to allow open debate whilst encouraging a presumption of good faith

Develop membership meetings as per 3 and five year plans.

Offer feedback to comments from community in a timely and honest fashion.

The WMF takes actions which WMUK opposes

Action:

Encourage all WMUKs members to participate in WMFs consultations to minimise the risk of such a breach.

Develop WMUK's independent fundraising alongside our joint fundraising with WMF so we can act independently if needed.

WMUK takes actions which WMF opposes

Action:

Be open about our decision making processes, consult with our partners before decisions are made, if practical.

Develop WMUK's independent fundraising alongside our joint fundraising with WMF so we can act independently if needed.

Risks related to WMF projects

Scandal related to pornography or politics or other issue on some corner of the WMF sites

Action:

Continue outreach to new readers and editors so we already have a reputation in peoples mind before the 'scandal' hits.

Training of Trustees in media interview techniques.

Work with public relations volunteers to make sure our response is available

Collapsing editor base means a decrease in quality

Action:

Build WMUK programme with editor retention and development a core objective.

Monitor effectiveness of activities.

Develop Train the Trainers to build new capacity.

Wikipedia and sister sites become unpopular and usage declines

Action:

Outreach and partnership work to improve the quality of Wikipedia and other WM projects.

Tailor programme of activities to re-build confidence and usage.

Decrease in diversity of editor and volunteer base Action:

Build programmes to address these concerns.

Pay especial attention to developing, supporting and retaining volunteer base.

Target hitherto underrepresented groups.

Monitor effectiveness of activities.

Others that we will need to consider:

- **Reputational risks**
- **Organising events**
- **Financial systems**
- **HR risks.IntroductionBullying**
- **Staff turnover**
- **IT security**
- **Other security risks.**

How to rate the risks

NCVO offers a rating grid against which we could score our risks and come up with a prioritised list:

Matrix of risk probability against impact

Impact	**Very low probability (1)**	**Low probability (2)**	**Medium probability (3)**	**High probability (4)**	**Very high probability (5)**
Very high (5)	Low score	Low score	Medium score	High score	High score
High (4)	Low score	Low score	Medium score	Medium score	High score
Medium (3)	Low score	Low score	Low score	Medium score	Medium score
Low (2)	Low score	Low score	Low score	Low score	Medium score
Very low (1)	Low score	Low score	Low score	Low score	Low score

In the NCVO and Institute for Risk management model staff are delegated to assess the risks and report back in this sort of fashion
The staff then take discuss with their colleagues and either agree or score them differently.

The staff feedback to the Board and then plot these onto a 'risk register' identify what safeguards are in place, monitor how effective they are and report regularly to the board.

Sample risk register

Area covered: ________________________

Date: ______________________

Source: _______________________

Risk register

Risk reference number	Identified risk	Priority	Safeguard reference number	Adequacy of safeguard
R-00001	Risk X could happen if Y with Z consequences	Low impact, high probability	S-00001	Adequate, accept risk
R-00002	If A occurs, risk B will mean C	High impact, very high probability	S-00002	Inadequate, act

This would then lead to a register of safeguards:

Register of safeguards

Safeguard reference number	Safeguard identified	In place?	Implemented /evaluated	Reviewed
S-00001	Description of safeguard...	Yes	29/11/02 by DN	01/04/03 by GH
S-00002	Description of safeguard...	No	08/02/03 by GH	10/07/03 by GH

Reported to Trustees' meeting on: __________________