Proceedings of IRM Charities Special Interest Group

EMBEDDING RISK MANAGEMENT AT A TIME OF NEED 2009

Event held: 1 September 2009
Output notes issued: 21 December 2009

The Institute of Risk Management

Description

Proceedings from the Institute of Risk Management Charities Special Interest Group (SIG) Risk Management Event, hosted by Lloyd's Register, 71 Fenchurch Street, London, EC3M 4BS, on 1 September 2009.

Contents

1 Introduction

The real economic damage caused by the financial sector is still unfolding. Charities are among the most vulnerable and many are now realising that they need to urgently rethink their business strategies if they are to weather the storm. Risk management is all about managing a business successfully, whatever the weather. It's all about achieving goals and overcoming business threats through implementing a process that is capable of navigating obstacles as they arise.

The aim of the seminar was to focus on real situations and examine practical solutions. To set the scene, William Hotopf, Senior Head of Risk & Audit, The Prince's Trust outlined the methods and approach adopted at the Trust. This was followed by a workshop. Keith Povey, Group Corporate Secretary, Lloyd's Register opened the workshop to present the practical aspects of risk management with small charities in mind and a team of expert panellists chaired tables to promote discussion among delegates on specific topics.

The seminar closed with a wrap up session in which the panellists summarised the points that emerged from the smaller workshop discussion groups (some aspects of which require further development).

Speaker Biographies

William Hotopf

William is Senior Head of Risk and Audit for The Prince's Trust. His role involves reporting to the Executive Board of the Trust, Chief Executive and Audit Committee throughout the year on Risk Management and Internal Audit issues. The Prince's Trust helps change young lives by giving practical and financial support to young people who need it most. William is also a volunteer for Crusaid, a charity helping people living with HIV and AIDS in the UK and South Africa, and attends the Finance and General Purposes Committee on a monthly basis.

Keith Povey

Keith is Group Corporate Secretary for Lloyd's Register and acts as a Trustee for Lloyd's Register Educational Trust. His role involves him in Lloyd's Register's Investment and Audit Committees and he is also a Pension Fund Trustee. Lloyd's Register is a charitable Community Benefit Society with a large number of subsidiaries and over 200 offices worldwide. Keith runs the insurance programme for this large and complex group, a task which has given him first hand experience of the necessity of risk management in charities.

2 Embedding Risk Management in the Prince's Trust

By William Hotopf

What is Risk Management?

Risk Management is a management style based on assessing the potential likelihood and impact that could be caused to a business if key (strategic) risks are not controlled and mitigated.

This is summarised in the Risk List prepared every three months by the Risk Management Group. New risk factors are also recorded in one-page paper produced alongside the Risk List – Recent Changes to the Risk Environment.

At the Trust we have adopted a broader definition of Risk Management:

> "Making sure that people are equipped to understand the potential risks that their actions may expose the Trust to, and helping them take a look at the design of what they are planning to do to reduce both the likelihood of an incident occurring and its potential impact. The central Programme Quality and Safety team provides advice and on occasion (few and far between) may halt an activity altogether".

This definition places embedding Risk Management centrally in our definition – if it's not embedded it's not happening.

The Challenges the Trust faced

The Trust in its current form was created by the merger of a group of charities in 1999, all of which offered services to young people and had the Prince of Wales as its patron.

This caused tensions because of distinctly different cultures for staff and volunteers in each charity. Matters further complicated by each charity working with different age-groups and in different ways (also inconsistencies in legislation on the definition of "children").

The new Prince's Trust then divided itself into geographic areas comprising the nine English regions and three Celtic countries. Each region had its own management structure and variants of the core programmes developed.

This contributed to a number of problems:

- Financial: erosion of unrestricted reserves in the period 1999-2000 to 2002-03
- Programme delivery: too many avoidable Health and Safety incidents on Trust programmes

By 2003-04 it was clear that we needed to take a new approach to managing our risks.

How we embedded Risk Management

Key appointments; new Chair of Trustees (2003), new Finance Director, Chief Executive and Heads of Quality and Risk Management (2004), then appointment of Internal Auditor (2005).

We reviewed programme design and published a series of toolkits telling staff members (and volunteers) how (with reasons) we run our programmes.

We set up Quality Groups to bring together regional and national managers to discuss the development of our procedures.

We produced a Governance Handbook to describe roles and responsibilities for our Trustee Board, Senior Management Team and Regional Management Teams.

We developed a media strategy to define the first steps taken after a major incident, including controlling responses to questions from the media.

We restated our Reserves Policy and started to ensure that we spent less than our current income, this enabled us to build our reserves and save for the future.

We reviewed all our other policies to ensure that they were fit for purpose, and developed a house-style for drafting policy documents.

Embedding changes to the risk management process

We identified the barriers to embedding risk management, and thought about the appropriate sales technique for each:

- Over-familiarity– we are continually managing risks from cradle to grave (tie up your shoe-laces, brush your teeth, no you cannot scatter your mother's ashes here)
- Deterministic model in a chaotic world and differential perception of risk – problem that risk management can oversimplify and often overplay risks.
- Sometimes wrongly cited as a reason for introducing an unpopular change - never, ever let this happen
- Inner child arguments – "but we've always done it like this", and "every other charity is doing it this way" – *it's so unfair!* Proper response: explain in plain English why we are making the change, remain calm, patient and firm
- Personal dynamics – some people will simply look at you, grit their teeth and refuse to take on board what you are saying. Identify someone they will listen to preferably one of their team, wherever possible do *not* go above their head in the line management structure.

We have found it useful to use analogies to motoring to describe, redesign and sell our key controls:

- Speed-bump controls – found in finance systems such as sign-off for invoices or the transaction limit on credit cards. Can only be overridden by a deliberate act, such as sharing passwords or making multiple payments on a credit card for the same transaction.
- Traffic light controls – also found in finance system such as purchase orders, differs from speed-bump controls (built into computer system) because a management control instead. Can also be overridden by a deliberate act.
- Zebra crossing controls – these are a sort of optional traffic light control, typically whether or not the control applies depends on factors that might make the action

higher risk, such as running extra checks on expense claims above a certain value threshold, or taking special precautionary health and safety measures when dealing with a particular group of clients.

- Roundabouts – "culturally specific" traffic light controls. Example of our Drugs and Alcohol policy – we cannot write a policy that does not agree with the letter of the law so the instructions are intentionally open to interpretation. In these cases we try to ensure that the adjudication of the policy lies with a named member of our senior management team.
- Speed-limit controls – "do this action until we tell you to stop", the least satisfactory of controls because people instinctively disobey and enforcement requires constant management surveillance and prompt, possibly response (think of speed cameras).

As we refine and develop risk management we have tried to revise our controls to make them clearer and easier to monitor. This has involved moving away from 40 page policy documents (and establishing a process for annual review of all policies), reviewing the structure and content of our intranet, and wherever possible replacing speed-limit controls with traffic lights.

We found out what people were doing and compared this to what people should be doing. We have now introduced standard job titles throughout the Trust.

We started using our Risk Register as a bridge between job roles, key policies and the risks addressed by the policies.

We reviewed our expectations of what embedded risk management would look like and brought our insurance programme under risk management.

We developed a template for operational risk management for use by the staff responsible for delivering our programmes round the country. Sections of these risk lists are reviewed each month and their content is reviewed by the central risk management group to pick up on emerging issues.

Future challenges for Risk Management in the Trust

- Volunteers
- Managing innovation
- Changing nature of government spending
- Electronic filing systems and document control

3 The Small Charity Guide to Managing Risk

By Keith Povey

Introduction

Risk is often described as danger or something going wrong. Most people have some idea of what risk management is about because risk is a commonly used term and widely experienced in aspects of our lives. Large organisations employ professional Risk Managers who manage risk through a constant cycle of identifying, monitoring and reporting risk, and instigating actions to mitigate, accept, transfer or avoid risk in line with business or cost justification; but for a charity with a small turn-over it is difficult to employ specialist knowledge.

Risk management is one of the most important responsibilities of a trustee and a risk management programme is important in meeting the mission of your charity, enabling you to prevent disasters. The Charity Commission recommends that it is good practice for all charities to carry out a proportionate annual risk assessment and to commit to reporting on the findings. Charities subject to statutory audit, the trustees' annual report is required to contain "a statement confirming that the major risks to which the charity is exposed, as identified by the trustees, have been reviewed and systems or procedures have been established to manage those risks".

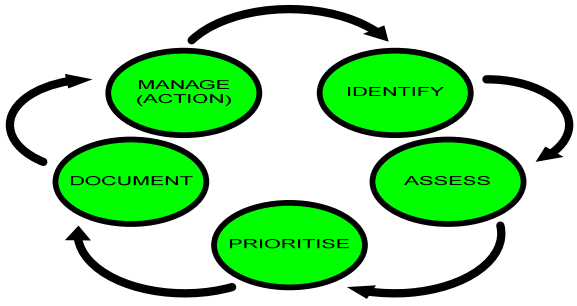
(Charity Commission publication *Charity reporting and accounting: the essentials* (CC15) Crown Copyright).

In practice this means identifying risks and describing the procedures and plans your charity has put in place to safeguard or reduce likely problems as well as indicating how you monitor those risks and what contingencies you have in place.

To help small charities we have put together a simple method to manage risk but the complexity of your risk review will very much depend on the nature and size of your charity's operation.

The Constant Cycle of Risk Management

1. Identify risk
2. Assess risk
3. Prioritise risk
4. Document risk
5. Manage risk



Identify risk

Look at all the elements of your charity's work and consider a wide range of things that might happen. The Charity Commission's Charities and Risk Management online guidance gives the following examples of areas you may need to consider:

- **Governance Risk;** trustee board lacks relevant skills, trustee board dominated by one or two individuals or an out of date governing document.
- **Operational Risk;** IT and communications system failure, high staff turnover, key member of staff leaving, lack of business continuity plan, a change in government policy or negative publicity.
- **Regulatory Risk;** failure to comply with reporting requirements, compliance risks or a breach of data protection.
- **Financial Risk;** low level of reserves or a dependence on a single source of funding.

Assess risk

Once a risk has been identified assess the likelihood of the risk happening and the impact of the risk, on the charity, if it is realised.

A simple method is to assign a numerical value between 1 and 8 for:

- likelihood of the risk happening (Frequency)
- A score of 1 represents low frequency, not very likely to occur.
- A score of 8 represents high frequency, a regular occurrence.

and

- Impact of the risk on the charity if it is realised (Consequence)
- A score of 1 represents no consequence
- A score of 8 represents a major consequence.

Prioritise risk

Multiply the factors (Frequency X Consequence = Priority)

Higher the value - higher the priority

Example:

Risk **A** has a Frequency of 5 and a consequence of 7 (5 X 7 = 35).

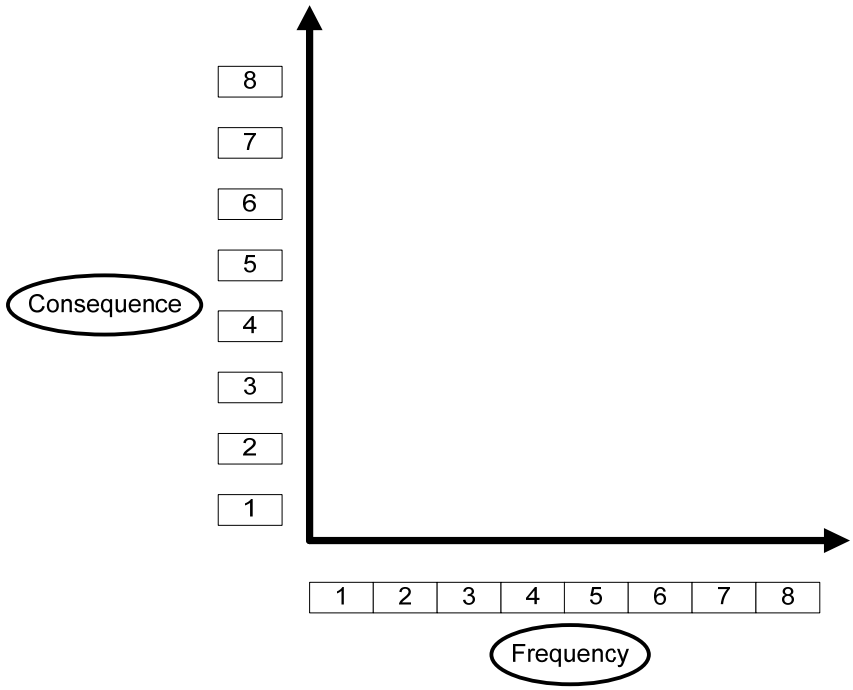
Risk **B** has a frequency of 3 and a consequence of 8 (3 X 8 = 24).
Therefore - Risk **A** (35) is a higher priority than risk **B** (24).

Document risk

A document can help communicate your plan and will clearly identify roles and responsibilities. All considered risks should be documented; it is useful to display your data in a risk register similar to the example below.

Risk	Priority	Frequency	Consequence	Control	Monitoring process	Responsibility	Further action required	Date of review
IT system is old. All charity data is held on the system	1	5	7	Back-up all data at the end of each working day	Log to be kept of system failure	Trustees / treasurer	Obtain funds for new IT system	01/11/09
Un-satisfactory fundraising returns	2	3	8	Financial appraisal of new projects. Budget reporting by fundraising activity.	Financial reporting by fundraising activity. Quarterly reporting by fundraising manager to the Board.	Fundraising manager	All new initiatives to be approved by the Board unless included in the current business plan.	Next Board Meeting

To help prioritise risk plot your data onto an axis as in the diagram below.



2-3

Manage risk

Managing risk means devising ways to either prevent the risk, minimise the impact, transfer the risk to a third party or avoid the risk entirely.

Options are:

Risk Mitigation: This is the response to risk that typically comes to mind first. It includes all the countermeasures that the charity can take against threats.

Risk Acceptance: If the cost of addressing a risk is greater than the risk itself or if addressing the risk would pull resources away from a far more serious risk, the rational course of action may be to simply accept the risk.

Risk Transfer: In some cases, it is more prudent to transfer the risk to a third party such as an insurance company than to allocate limited resources toward mitigation efforts that are unlikely to make a difference.

Risk Avoidance: There will be situations when the level of risk and the cost of addressing that risk are simply not tolerable. In these cases, it is best to avoid the risk entirely.

Conclusion

Be prepared, formulate a Contingency plan, time spent now will enable a faster response and minimise impact to your charity should a risk be realised.

Managing all unknowns with a single approach can enable a charity to be better prepared for what might happen. Focus on positive and negative outcomes to events which will be more effective than focusing on negative points only.

Consider how your risk management plan can benefit your charity. Example; people may have more faith in your services if they are aware of your risk management policies and potential funders will be reassured that there money is in good hands.

4 Introduction to break-out sessions

Following the presentations the meeting divided into 5 discussion groups hosted by an expert. Discussion Group 1 talked about investment risk management, Discussion Group 2 talked about Information Security, Discussion Group 3 talked about Human Resources and Discussion Group 4 talked about Event Risk Management and Discussion Group 5 talked about Fundraising Risk Management.

Discussion Group 1

Investment Risk Management

Expert: Oliver Boyle MIRM**,** Chairman, IRM Charities Special Interest Group and Investment Director, Thomas Miller Investment Ltd

The effects of the recession are far from over and the price of the taxpayer's rescue will be felt by us all. Charity finances will be severely stretched and trustees will have a hard time balancing reserve assets against risk assets in a low return environment. Recent research from the Charity Commission suggested that trusts and foundations are weathering the economic downturn relatively well. However, their investment income has been impacted and they will be forced to exercise more caution in how they manage the risks associated with grant-making. As a consequence the effectiveness of charities will come under intense scrutiny. Trustees will need to show how they govern their finances and demonstrate what level of reserves their charity needs. Delegation of investment management duties to professionals does not delegate the duty of care – overall responsibility lies with the board of trustees.

Topics discussed:

- Investment decision risk
- Formulating an investment policy
- Balancing investment advice against value for money
- The pressure to invest ethically
- Measuring investment performance and the use of the total return approach
- Safe-keeping of financial assets

Discussion Group 2

Information Security

Expert: David Funnell CIRM, previously Risk Advisor, Guide Dogs

Recent research suggests that the biggest threat to information security and data loss is posed by "insiders". The exposure of confidential information is now viewed as the single greatest threat to enterprise network security. Over the past 12 months organisations surveyed reported an average of 14.4 incidents of unintentional data loss through employee negligence. The report stated that contractors and temporary staff represented the greatest insider risk to organisations, a by-product of the recession and slow recovery?

As charities come to terms with reduced income, and cutbacks in spending on non core operations, key business decisions are being made to determine how best to protect their information assets, and reputation as a consequence of data loss.

Topics discussed:

- How do charities manage the governance, risk management and compliance (GRC) of information security, is it an holistic systems view?
- What are the biggest challenges to information security that charities face?
- Which information security framework?
- How do you measure performance of your information security framework?
- How is assurance provided?

Discussion Group 3

Human Resources

Expert: Mike Heath, Peninsula Business Services Ltd

Topics discussed:

- Trustee responsibilities: Employment law / Health & Safety Considerations
- Discrimination in the workplace: Voluntary staff, pay as you earn staff, self employed
- The new ACAS code of practice as of April 2009: Disciplinary and grievance procedures
- Pension contributions: What are the implications for the charitable sectors?

Discussion Group 4

Event Risk Management

Expert: Alyson Pepperill FIRM, IRM Director and Client Projects Director, Oval Insurance Broking Ltd

Topics discussed:

- Embedding event risk management
- Communication
- The process
- Types of events
- Is it worth it?
- Run events in-house or outsource

Discussion Group 5

Fundraising Risk Management

Expert: Peter Heap, Consultant, Ark Risk Consulting

Topics discussed:

- Importance of analysing different revenue streams to assess vulnerability of each and hence overall potential revenue gap for the charity

- Look at potential new revenue sources and cost effectiveness of each. Risk is opportunity as well as threat. Diversification is also important to prevent reliance on single sources
- Apply standard risk management process to analyse new opportunities i.e. impact and likelihood. Determine how threats can be minimised
- Examples of risks of different revenue streams:
  - Voluntary income
  - Trading
  - Investment income
  - Legacies
  - Public funding
  - Corporate funding
  - Membership income

5 Comments from the break-out sessions

Immediately following the discussion groups delegates provided feedback to the other delegates in the meeting; their comments are listed below. Two larger pieces of work were received after the event from Alyson Pepperill offering advice on event risk management and from Chris O'Keeffe offering advice on information security and these can be found in Appendix A and Appendix B respectively.

5.1 Investment Risk Management

Investment Managers need to help charities understand the investment risks contained in their portfolio. Likewise, charities need to ensure that their financial requirements are more accurately reflected in their investment policy so as to provide a measured and meaningful investment objective. All too often trustees find themselves adopting investment performance benchmarks that they do not fully understand and that are not linked directly to the financial needs of the charity.

Having trustees with investment expertise can help a board ask the right questions, but should not be relied on for investment solutions. Time should be set aside to educate the entire board so that an assessment of their collective understanding of investment issues can be formulated. This will make it easier for the board to gauge what advice they need and govern the arrangements put in place.

Using more than one investment manager or investing in a range of investment products does not automatically provide the benefits of diversification. Prior thought should be given to the underlying risk profile of the entire portfolio. Trustees should first evaluate their financial strength and their tolerance for the financial risk that arises from investing in different asset classes, i.e. cash, bonds, equities etc.

In summary the formulation of a risk based investment policy should be a more frequent process than is often the case with most charities.

6 Summary

The management of risk and the balance between risk and reward is vital. To be effective, risk management must be linked to business objectives and cover the complete range of risk your charity is exposed to.

To make changes to effectively manage risk the key issues for management are:

- Realisation of benefits must be owned by the Trustees
- Become active as soon as possible and identify the risks facing your charity
- Factors other than clear benefits can take priority, organisational politics need to treated pragmatically
- Common acceptance of business objectives is crucial for change management

It is the intention of the Institute of Risk Management Charities SIG to hold further discussion groups. Details of future discussion groups and events will be advertised on the website.

Appendix A

Event Risk Management: What to consider when planning an event

By Alyson Pepperill FIRM, IRM Director

Why do you hold events?

This is the first question to consider. Is it the case that you have always held such events and therefore you continue to do so? With the advent of new media and digital applications many businesses and charities are turning away from face to face meetings and events – have you considered this?

This has led to at least one major charity moving away from an event a week to fewer and smaller events.

Whatever you decide it's important to have a plan – a vision of what you want the events to achieve, how many you want to hold in a year, and why you want to hold these events.

What do you want to achieve?

This is probably such an important part of the decision making it is worth concentrating a little on areas to examine in your thinking:

Why have you held events in the past?

Often this comes down to brand awareness, publicity, building an affinity with people who may provide donations, and attracting volunteers to name a few.

Income generation may come up but the question is – did the income that you generated from the event offset the costs in terms of financial and people's time and effort (that they have not spent on other charitable work for you)?

Or perhaps it is a fear of letting down people that have enjoyed the event in the past? A difficult one to turn down if these are the very people that your charity has been set up to please and protect.

Does the event proposed actually match your objects? Does it make sense to do this?

Or is it that the event has always been held? Whether or not it has made you any money or just caused an inordinate amount of work for your staff.

Consider a past event in detail – how much did it cost to plan, develop and hold the event? How much profit or income did the event generate? What were the non financial or possibly future financial benefits (future donations or sponsorship) that can be tracked back to the event?

It could be that an event only broke even but by raising your profile new volunteers joined the organisation and a number of people started to regularly donate. It is difficult to assess this but worth including in your deliberations.

Setting a target

Probably the most effective way to consider events is to look to the future and set yourself a target. For example, I want to hold 4 events during the year and earn a minimum of £10,000 profit from each event.

Your staff can then come to you with short format business cases (hopefully using data as evidence and citing best practice) to justify the potential of an event being one of the four. This can be undertaken following the set (and simple) format shown at the end of this Appendix or a more free hand proposal could be required.

Who can approve an event?

The organisation needs to decide who can approve events and up to what expenditure that person can authorise. They can then be the central, regional or local gate keepers depending on the size of the organisation.

How can you risk manage an event?

The usual risk management process works well as a template.

Identification of risk – think about what could go wrong as well as what could go right

Assessment of risk – how seriously could the event go wrong? And what costs or penalties could the organisation be hit with?

Control the risks – think about how the risks that you identified could be controlled through transferring the risk (perhaps to outsourced events managers), reducing the exposure (e.g. excluding an event from a local fete that could lead to children being injured), or potentially avoiding the risk entirely by deciding that the event is too 'risky' and the potential costs outweigh the potential benefits.

Transferring the risk to someone else

On the face of it a tempting proposition to any Risk Manager BUT how much of a risk can you truly transfer and how much will it cost?

You cannot entirely pass on legal liabilities that rest with your organisation even if you have a contract in place. If you are deemed in a court of law to be legally liable you will have to pay any fines, costs, or awards.

However, there are many risks that can be successfully transferred to third parties through contract – but even then a vicarious liability remains which means that if your name is the 'brand' of the event despite using a bona fide event management company, the participant may still decide to sue you jointly or severally. Then it's up to the courts to decide which party(ies) is legally liable.

Vetting Third Parties

So just be aware that this is not your ticket to avoid risk – rather a way of managing it. In these circumstances you need to undertake more up front due diligence work on any outsourced agency that you use. Demonstrating that you have vetted their financial position, approach to health & safety and to risk management more generally, as well as their insurance arrangements, will help you to defend any case brought against you.

And once this up front work has been undertaken and signed off as acceptable by the authorised party then your workload reduces over and above if you had organised the event yourself. But don't forget to add the cost of the event manager's fees to your tracking spreadsheet – this replaces the costs and time/costs/opportunity costs of your staff holding the event.

Contract risk management

When signing a contract it is useful to have undertaken your risk identification and quantification first. This way you have an understanding of what could go wrong in the performance of the event and can build appropriate safeguards into the contract – or at least try to negotiate these into the contract.

Whatever is outsourced obviously still requires some management from the charity – the extent depends on the extent the event has been outsourced – all, part or a very small part. How much should depend on who is best placed to do the work to make the event a success.

How do you embed event risk management into an organisation?

Communication is the key. Below are 5 top tips on how this could be moved forward.

- You need to make sure that the staff and volunteers understand why you hold events and what must be achieved from an event. Consider using sales techniques to gain buy-in – most effective when you think about the type of people or groups within your organisation and who is most likely to object to a change in events strategy, and what their gripe will come down to. For example, does a person have a vested interest in an event? Does a group of people see the event as 'theirs' and almost as part of the benefits of working for the charity?
- Next you need to make sure that staff understand who can authorise an event and the process that they will need to undertake to gain approval. This is obviously linked to what the event must achieve.
- Be careful that you don't become a scapegoat for other departments that no longer want to hold an event e.g. 'Oh we wanted to do it but XX wouldn't let us'. Risk management increasingly bears the brunt of blame. Instead try to offer a more enabling approach – what about doing this event instead or this sounds fine but could we have another think about this part of the event.
- The role of the trustees and their support is important. They have the ultimate responsibility so need to understand and buy into the events strategy and what events must achieve. A briefing note on this highlighting the protection of the charity whilst enabling the staff and volunteers could be one approach to achieve this.
- Don't forget to then monitor your strategy – what works well and what can be improved? With specific events you may like to track what went right or wrong – without utilising a blame culture and with a clear focus on getting it right in the future rather than dwelling on what went wrong in the past.

EVENT PROPOSAL CASE

Name of Event	
Event Manager	
Objective of event ▪ Financial ▪ Non Financial	
Estimated Costs of event ▪ Set up/planning ▪ Hiring and third party costs ▪ Any other costs Note also any mitigations of cost e.g. sponsorship or designated funds	
Resources required ▪ Staff ▪ Volunteers ▪ Third parties	
Estimated revenue to be generated	
Potential non financial benefits	

Appendix B

Information Security

By Chris O'Keeffe, Business Analyst, Lloyds Register

Introduction

Information is one of the most important assets enabling charities to achieve their objectives. IT based systems and processes that handle data allow information to be stored and transferred easily, but growing dependence on IT based information has increased risk. Information security seeks to reduce the risk.

The ICT environment

Information Communication Technology (ICT) costs money and cannot always be viewed in strict terms of return on investment. A Successful ICT project depends on spending what is necessary and not the least possible. Decision makers should be aware of the benefits change can bring and ensure they purchase popular tried and tested products that will have ongoing support at a reasonable price.

Software

A Software application has similarities to a biological entity it grows to meet the challenges that are forced upon it by internal business pressures and external attack. Most people are familiar with receiving regular application updates for their home computer and use anti virus software to stop unwanted changes happening through inadvertently uploading malicious code.

A management process should be put in place which allows modifications and upgrades to be managed and installed on a regular and timely basis that will reduce the risk to your charity.

Data

Always make a copy, back-up your data and store it in a separate physically secure location.

Obligation

The Data Protection Act;

Gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the individual

- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Should an individual or organisation feel they're being denied access to personal information they're entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioners Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

Basic ICT Risk Management

To help you manage ICT risk you should know the answers to the following questions:

What measures do you have in place to protect your information from unauthorised people who may try to steal or misuse it?

Do you have firewalls to limit outside access, do you have antivirus software, do you limit the use of your information to your premises? Do you encrypt data so that no one outside your organisation can read it? Do you limit staff and volunteers' use of the internet? Are they able to install their own programmes? Do you audit your back-up systems to check all the information you thought was secure actually is?

Do you have signed contracts so that essential maintenance can be carried out on both hardware and software?

Do you have a service level agreement that specifies the level of service you will receive and how fast the service will be provided?

If you operate 24 hours a day, 365 days a year do your maintenance contracts cover you adequately?

Insurance; do you have insurance for your ICT? What does the policy cover?

Business Recovery; do you have a business continuity plan appropriate to the size of your organisation that will enable you to be back in business with minimum disruption? Do you review and test your plan regularly?

Service Provider; what happens if your service provider ceases to support your business?

Conclusion

This guidance is intended to provide small charities with an introduction to information management, further information can be found at:

Information Commissioners Office
Telephone 08456 306060
The Information Commissioner's Office (ICO) is the United Kingdom's Independent authority set up to promote access to official information and to protect personal information. The ICO website includes guides to data protection and good practice notes, www.ico.gov.uk/

ICT Development Services; points voluntary and community organisations to resources that can help them to make the most of technology www.icthub.org.uk