Institute of Risk Management - Charities Special Interest Group

Winter 2016/17 Newsletter

Produced in association with Ansvar Insurance

irm

ansvar
Insuring the heart of your community

Alyson Pepperill
Chair, IRM Charity Special Interest Group

Introduction

Happy New Year! Ok I know we're slightly late to be saying that so instead welcome to our first newsletter of 2017!

I just thought it would be useful to provide a reminder to you all about what the SIG is here to do:

The IRM Risk Special Interest Group was established over 10 years ago to provide practical guidance for charities about managing risk and opportunities for sharing knowledge, tips and best practice amongst sector professionals. Our overall aim is to increase the sector's knowledge of risk management best practice, explore practical solutions for managing sector challenges (such as new regulation requirements), and provide a forum where risk professionals can meet to learn from one another and share up-to-date risk management practice.

This newsletter kicks off with a review of 2016 and looking forward to the work we will undertake in 2017, as well as recapping on our final seminar of 2016 on the topic of Fundraising Risk & Regulation.

Our Risk Expert this edition is Fiona Davidge who is an established risk management expert of world renown following her significant involvement in the drafting and the work underway to redraft ISO31000 everyone's favourite guide to risk management.

And our Risk Practitioner is Rowenna Fielding who is absolutely brilliant at translating the very dry topic of Data Protection and Information Governance into something interesting and what's more fun – as we experienced at our last seminar of 2016. Pirate games and all!

Lina Munro of NSPCC provides a valuable insight into how that charity is managing the colossal changes experienced in the fundraising arena in 2016, which of course continues to change through 2017.

My final point is to sincerely thank the 100 and more of you who completed our short and simple Risk Survey. More will follow on this topic in the next newsletter.

I hope you enjoy the newsletter and find it useful in your day job as we continue to concentrate on being practical rather than theoretical.

Charities Special Interest Group (CIG) Committee Members

Alyson Pepperill (Chair)
alyson_pepperill@ajg.com

Guy Biggin
guy.biggin@crowecw.co.uk

Jan Cadby
jan.cadby@btinternet.com

Lisa Reilly
eisfcoordinator@eisf.eu

Kevin Thomas
kevin.thomas@ecclesiastical.com

Roberta Beaton
roberta.beaton@rnib.rg.uk

Lina Sleath
lina.munro@nspcc.org.uk

Perry Marshall
perry.marshall@alzheimers.org.uk

Steve Griffiths
steve.griffiths@alzheimers.org.uk

Rhiannon Sullivan
rhiannon.sullivan@mariecurie.org.uk

Alyson Pepperill
Chair, IRM Charities Special Interest Group

2016 in review and looking forward to 2017

At the end of 2016 and moving into 2017 the SIG team sat back and reflected on what we have achieved in 2016. We thought 2015 was a pretty good year but, if anything, 2016 has been even better in terms of our activity and how the SIG cohort has expanded.

One of our key aims is to make risk management more accessible to charities. So much of the guidance out there is geared towards the finance sector and big corporates and just isn't relevant to most of us - added to which it's usually full of jargon and way too long! In 2015 we launched our 'Getting Started' campaign and this year we've followed it up with not one, but two pieces of guidance - 'Getting better' and 'Setting your risk appetite'. Getting better sets out a simple framework to help you develop a plan for improving your risk management. Risk appetite is a hot topic at the moment but can be a complex subject to grasp. Our recently published guidance aims to help charities understand how much risk they are prepared to take in different areas of their work – take a look if you haven't seen it yet at **https://www.theirm.org/events/special-interest-groups/charities/**

All of this guidance is written by members of the Charities SIG committee with input from those who attend our meetings and seminars. In 2016 we held four very well attended round table meetings and seminars to launch the guidance and to discuss topics ranging from techniques we're using to embed risk management to developing risk appetite.

But as we know there will be some of you who can't attend our events which are usually held in London, we reach out further through this newsletter – kindly sponsored by Ansvar Insurance – we hope this goes some way to filling the gap there! We try to give a round-up of the key issues discussed at the events as well as articles from our guest speakers and other experts. As you can imagine it takes a lot of effort to produce three newsletters each year so we'd love to know what you think of them. What are the burning issues you'd like to hear more about? Contact Alyson Pepperill with any thoughts.

One thing we didn't expect to be doing at the start of 2016 was responding to the House of Lords Select Committee's inquiry into charity sector sustainability. Members of the SIG helped to draft a comprehensive response on behalf of the IRM which we hope will help the Committee understand how critical risk management is to improving the sector's capability. Watch out for their report in March 2017!

So that's it for 2016 but as you may well have noticed we're already on the case for 2017 with our first event taking place on 21st February. There will be 3-4 more and further information on these will follow so keep any eye on our website for details of our upcoming events.

We're also hoping to tackle Risk Governance and separately Regulatory and Compliance Risk Management during 2017 with a view to adding new publications to our suite.

All of the work committee members do is on top of our day jobs so a big thank you to everyone who has helped to draft and publish our guidance, our newsletters and to host and arrange our events. We're a small (but I like to think select!) band of people and we're always looking for others to join us so we can do even more to help charities implement and embed risk management. If you'd be interested in attending our events or receiving our newsletter just let me know.

Alyson Pepperill
Chair of SIG

Fundraising Risk & Regulation Event – 2nd November 2016

Our final SIG event of 2016 saw 20 representatives from the sector come together at Crowe Clark Whitehill's (CCW) London office to learn about and discuss the very rapidly changing landscape of fundraising and information governance, as well as to learn about Event Risk Management.

Following a welcome by Naziar Hashemi of CCW and Alyson Pepperill (SIG Chair) we moved quickly onto the meat of the afternoon session, Lina Munro of NSPCC talking about how NSPCC have tackled fundraising risk and regulation. This was clearly an all-encompassing piece of work that Lina dedicated herself to in 2016.

NSPCC have around 200 employed fundraisers and of course, thousands of volunteers raising funds as well. The way Lina and her team have tackled this subject is through training and in particular through inductions (as we all know there is a regular turnover of staff within most charity fundraising departments), as well as by drawing up and publishing guidance and reference materials that are straightforward and easy to follow. Publications include:

Data consent wording: This page will contain the most up-to-date recommended opt-in/opt-out wording.

RASCI sign off process: This page explains the process for approving new fundraising creatives for public use.

Introduction to Fundraising Events: This eLearning module provides an overview of what needs to be considered to run an event in a safe and compliant way.

Data Protection guidance for Fundraisers: An overview of what fundraisers need to know about data protection.

Involving children or young people in fundraising events: Basic information and a risk assessment template covering safeguarding risks.

How to request a fundraising contract: As it says!

Mandatory guidance for fundraising materials: Overview of what must or could be included on fundraising materials.

Fundraising complaints guidance: How to manage these in conjunction with the NSPCC's Complaints Policy.

Clearly there are a lot of different angles that need to be covered off. At the end of the day though Lina and her small team are ready and waiting to help at the end of a phone.

And there was no evidence that Lina would be resting on her laurels having achieved so much! She outlined the following as the next steps for her team and sought ideas back from the audience too.

1. Crisis management plan (clear PR, communication tree, testing)
2. Compliance dashboard (clear line of sight for trustees)
3. Training for comms and marketing on ASA/ Ofcom/BCAP
4. Learning from mature risk sectors (Aviva on sign-off, Credit Suisse on crisis management)

Lina passed on to Rowenna Fielding of RNIB to introduce the subject of Information Governance to the audience. Her presentation to the SIG started out with some of the lessons about Information Governance (IG) that RNIB has learned during the past year. Key among those was the realisation that information risks are actually business risks which affect, depend or are caused by the ways in which information assets are managed. As such ownership of information risks should not sit with the Information Governance lead but with the business stakeholders.

The difference between awareness of information risk and understanding of how to manage information risk was also highlighted. The true goal of IG training is to drive desired behaviours and shape organisational culture – to be effective, it must not be boring! Culture also plays a significant role in embedding good practice, especially in getting people to adopt the approach of "baking in" IG all the way through planning, change and design processes, rather than attempting to "bolt on" IG requirements at the last minute.

The session concluded with a demonstration of some of the training material used within RNIB – a fun data protection treasure hunt which used pirate-themed scenarios to bring the 8 data protection principles and key risks to life.

The 8 data protection principles include:

1. Data is processed fairly and lawfully;
2. Data is only obtained for a specified purpose;
3. Data shall be adequate, relevant and not excessive;
4. Data is accurate and kept up to date;
5. Data is not kept longer than necessary;
6. Is processed in accordance with the rights of the data subjects;
7. Is protected and defended against unauthorised or unlawful processing or accidential loss or destruction;
8. Is not transferred to a country or territory that doesn't ensure adequate protection for the rights of data subjects.

With the recent concerns highlighted in the media about the uses of people's personal data by fundraisers, the never-ending reports of information security breaches in all sectors and the prospect of the EU General Data Protection Regulation - a more stringent data protection law which comes into force in 2018, it's definitely time for charities to consider Information Governance risk as a strategic matter.

Our final speaker was Barry Ifould of Arthur J. Gallagher who has worked with a number of Gallagher charity clients to help them consider and improve their approach to Event Risk Management. Barry clearly laid out that what drives Health & Safety generally is legislation and of particular importance is the need for charity fundraising teams to include or have access to a competent person as per the Health & Safety at Work Act.

In fact Competent Person is defined as "A person shall be regarded as competent for the purposes of paragraphs (1) and (8) where he has **sufficient training** and **experience or knowledge** and other qualities to enable him properly to assist in undertaking the measures referred to in paragraph (1)."

Barry went into detail on how to undertake an Event Risk Management and provided really useful advice based on his experience of working with charities around the areas likely to be overlooked or not done in sufficient detail.

It was certainly true that the initial feedback from the attendees was very positive and afterwards receiving emails thanking the SIG and saying 'a very helpful afternoon' certainly inspire us to continue bringing excellent speakers to our events. The truly scrumptious afternoon tea also went down very well – thank you CCW!!

Fiona Davidge
Risk Expert
Wellcome Trust

What is your background and how did you get into risk management?

I came into the risk world as a second career after studying for a law degree in my early thirties. This followed an earlier career as a registered nurse and then Royal Air Force nursing officer.

After graduating I joined Thames Water in an emergency planning role. My manager really encouraged me to develop expertise in the field and then added business continuity to my workload. Two years later the company asked our team to develop a corporate risk management framework and at that point I commenced studying for the Diploma of Risk Management with the IRM to support our knowledge in that area.

My next role was Senior Corporate Risk Manager at London Underground where my focus was integrating corporate, asset and project risk management which had traditionally operated as separate frameworks with limited interaction.

A desire to broaden my interaction beyond the corporate risk process brought me to the Wellcome Trust, a global charitable foundation which funds and supports scientific research in human and animal health. Here I have responsibility not only for the risk management process but also the insurance programme and more recently the business continuity process. Variety is good; it broadens my interaction with differing teams and levels of personnel and helps me to get under the skin of Wellcome.

What's a typical day like?

I am normally based at our London headquarters on the Euston Road, so I suppose you could say I follow a typical office based daily routine, working at my computer, attending meetings and interacting with people, following the necessary meeting and reporting cycles of Wellcome.

I also provide risk management expertise for our scientific research facility, the Wellcome Genome Campus near Cambridge. Every month I spend a few days there. It makes a refreshing contrast to London, working with people who manage the large academic campus which is set in the Cambridgeshire countryside and the scientists themselves who are busy working in leading edge research into the human genome.

What do you enjoy most about your job?

The fact that, as the risk manager, I have a broad visibility of most initiatives and challenges that Wellcome gets involved with! This can range from supporting the development of a public exhibition in India, providing risk management training to operations staff from some of our overseas funded scientific initiatives, working with IT staff at the Genome Campus who run one of the largest data centres in the UK and facilitating discussions with our Executive in respect of the strategic risks facing the organisation. It is a varied job and brings me into contact with a broad spectrum of staff and contractors.

What are the challenges?

The biggest challenge is getting people to view risk management as an enabler rather than a hindrance; that it is here to support the delivery of objectives not to say 'No' to everything! All too often people are so busy dealing with the known panics of today that they fail to look ahead and anticipate potential uncertainties and manage them.

Wellcome has recently decided to integrate many of the operational risk management activities into one team, so not only has Business Continuity been added to our remit, but the Health & Safety team will also shortly be working with us as one unit. I think for all of us that will add value, share knowledge and improve connectivity, all of which can only benefit Wellcome.

What advice can you give to others trying to implement risk management?

- First and foremost, risk management is not a standalone activity. It MUST be integrated into the day job for all staff and be everyone's responsibility. So do not design a parallel management process, integrate it into existing management and reporting frameworks
- It must support and underpin your organisation, its mission and objectives; risk and risk management is only relevant in that context and spoken in that language
- It should be seen as a facilitator of change, options and solutions; not just a paper based due diligence chore

Rowenna Fielding
Information Governance Officer at RNIB

IG article for Risk SIG

I first got interested in the subjects of information security and privacy while I was working in IT, as a systems administrator for a small training company. Unfortunately, due to the Sales Director's exotic Internet browsing habits, some malicious software had made its way onto the company's IT network and it was my job to clear it up. Once the panic was over, I realised that the investigation had actually been the most fun I'd had since starting my IT career, so I decided to get more into the security side of it.

At one point during my information security career, I was handed a copy of the Data Protection Act and informed that this, too was to be my responsibility. The more I learned about privacy rights and law, the more I could see that managing information well is not just a legal obligation but actually brings many benefits to organisations, individuals and society as a whole.

I'm now at the Royal National Institute for the Blind (RNIB) and my role is "Information Governance Officer" – which probably sounds a lot less fun than it actually is.

What is Information Governance?

"Information Governance" is just the formal way of saying "the systems, standards and culture an organisation needs, to manage information". Although many people think of Information Governance (IG for short) as a compliance issue, doing it well brings many more benefits than merely ticking a 'compliance' box.

Ultimately, the aim of IG is to make sure:

- there is reliable, accurate, useful information
- which is used effectively, lawfully and responsibly
- that is stored, found and used efficiently
- to enable, inform and protect the organisation
- so that the organisation can do what it does as well as it can.

Top tips for managing IG risk

Data inventory

In order to assess and manage the risks associated with information assets, the first step must be to find out what – and where – they are. The most effective way to do this is to map out the organisation's business processes and activities then to identify the points at which data is collected, generated, stored and used. Not only does this help to provide a start-to-finish view of the 'journeys' that data takes through the organisation, the activity itself also helps to develop a data-aware culture that treats information as a core business asset.

Hearts and minds

Treating IG as a compliance requirement can lead to a perception of IG as "red tape" or "barriers" which creates an environment in which IG is seen as a necessary evil to be avoided or evaded, rather than a core aspect of quality assurance. Simply telling people "you must do this" or "you can't do that" doesn't work – in order to engage people, there needs to be a clear explanation of why something is done in a certain way. Training material needs to be fun, accessible, relevant and continually refreshed otherwise it will be quickly forgotten (or even ignored) by people who are just trying to get their jobs done.

Don't confuse measures with goals

Although there are compliance standards for data protection, records management, confidentiality and information security, the ultimate purpose can be lost in a flurry of box-ticking and cosmetic solutions that keep auditors happy, rather than putting in good accountability structures and a culture of information awareness which form the foundations for more sustainable IG management. Approaching IG as a "compliance exercise" in which a framework or standard becomes a checklist is likely to lead to an extended session of Whack-A-Mole as standards change and the organisation evolves. A top-down approach is much more likely to be effective and starts with the question "how can we manage our information more effectively?"

What achievement am I most proud of?

So far in my information governance journey, my greatest achievement has been to make real changes in how people view data protection, both at work and in my personal life - that rather than being about boring paperwork and preventing people from getting their jobs done, it's really about making sure people's rights are protected and helping an organisation run smoothly. Raising enthusiasm for data protection is half the battle!

What is the strangest risk I have ever encountered?

I was once conducting a records management audit when I noticed that all of the paper archiving boxes in the storage cupboard had been wrapped around with silver gaffer tape. The boxes looked strong enough to me, so I asked why the tape had been added. The answer was "because of the mice". Apparently, the office building – being quite old – had a large resident mouse population who were constantly in search of materials for their nests. By trial and error, the staff had discovered that they wouldn't chew through the silver tape (although I didn't ask whether they'd tried other, tastier colours) and so to prevent their paper records being damaged or destroyed, they'd covered the boxes with tape. Soon after, we made arrangements to have the files moved to a purpose-built document storage facility!

Lina (Munro) Sleath
Business continuity, risk and compliance manager, NSPCC

How we tackled fundraising risk

I started my first week as a fundraising compliance manager by watching our CEO being questioned on live TV about our fundraising compliance. This is a summary of what has worked and hasn't worked for me in managing fundraising risks the past two years. I will also share a few ideas for managing fundraising risk in 2017.

What is fundraising risk?

Fundraising became a serious reputational risk in 2015 and it is also an increasing regulatory risk. From October 2014 regional media had been trailing a few stories about a pensioner called Mrs Olive Cooke receiving excessive charity mail. A few months after, Mrs Cooke committed suicide. This brought about national media headlines challenging fundraising practices, with parliament debating about an 'Olive's Law[1] ' to regulate fundraising. Two years on, charities have emerged from several investigations[2] to a regulatory regime that is still self-regulatory, but now answerable to an independent Fundraising Regulator and to a steady drip of changes to regulations and frameworks[3] . As media coverage shifts to Brexit and Trump, I have been supporting the NSPCC to navigate the after effects of 2015.

Practical steps we have taken

We tackle fundraising risk by taking corporate responsibility, with fundraisers acting as the first line that owns and manages the risks of its activities. Compliance acts as the second line that equips and supports the first line's decision making, occasionally challenging it too. As Alyson pointed out to me, this only works when the second line is genuinely supportive of the first. This is why our compliance team has worked really hard to build relationships with fundraisers.

6 things that worked well in managing fundraising risk at the NSPCC

- **Regular inductions.**
  We host a quick induction for new fundraisers. We do this every month to account for the staff turnover. We encourage this to be face-to-face, and we tell them about the compliance guidance available and the key requirements they should be aware of.
- **Compliance helpdesk.**
  This is an inbox that any staff member can email or call with a question. Kate, our compliance officer, manages this inbox and we try to resolve queries on the day or next day. She escalates complex ones to me and I review our advice given weekly. We get about 100 questions each month, and we add value by having a clear line of sight to senior management and their decision-making on areas that external guidance may not be clear on.
- **'Consent' surgery dial-ins.**
  We promote a weekly 30 minutes 'surgery' that executive board members co-chair and any fundraiser can dial in with a question about data protection compliance. Whilst we can advise on the risks, senior management are able to make the risk-based decisions. Questions are resolved quickly and within the session.
- **Internal policy update.**
  In addition, we send a monthly round-up email to all fundraisers which summarise policy and regulatory changes that may affect their fundraising activities. This sets a base level of 'must know' compliance knowledge among fundraisers who we may not see face to face.
- **Technical peer training.**
  Within the compliance team, we test and teach each other on new regulatory guidance with a weekly 'Peer to Peer' training session.
- **Incident Log.**
  When things do go wrong, we have developed a constructive culture where the person who discovers a compliance issue voluntarily asks to record this on our restricted access Incident Log. This is based on the Bank of England's model, which focusses on identifying impact and the mitigating actions to resolve the incident.

What hasn't worked so well?

- **Just signposting to guidance.**
  We trialled this in our team email's auto-reply to help reduce frequently asked questions. We realised that people still wanted a conversation, specific to their situation.
- **Mandatory e-training.**
  I would be keen to measure its effectiveness, as the questions fundraisers ask us after completing our mandatory compliance training are often covered by the e-module.
- **Compliance drop-in session.**
  We trialled this before the now successful Consent Surgery – turn out was low and the main difference was that this was not sponsored at senior management level.

[1] https://hansard.parliament.uk/Lords/2015-06-29/debates/1506293000158/Charities(ProtectionAndSocialInvestment)Bill(HL)

[2] For example, the Fundraising Standard Board (FRSB) investigations into. The ICO investigations into charities' data protection practices. The Public Administration and Constitutional Affairs Parliamentary Committee (PACAC) inquiry into charity fundraising practices.

[3] For example, CC20, Charity Act 2016, Code of Fundraising Practice, Fundraising Preference Service and ICO direct marketing guidance, as well as the merger of the Institute of Fundraising with the Public Fundraising Regulatory Association.

Ideas for 2017

One thing I know for sure is that the charity landscape will only become more complex. We need a resilient risk framework that can adapt to changes within a charity and outside it. Internally, my next focus is to look beyond our Fundraising teams.

The same ‘fundraising’ risks also apply to many of our teams who ask the public for their support - whether it’s their money, time or skills. This means extending risk management to our ‘non-fundraising’ activities such as our marketing campaigns, our petitions and our event invitations.

Externally, I am also really learning a lot from fellow charity risk & compliance professionals. I highly recommend corporate organisations as a source of free, expert advice. I have modelled our marketing sign-off process based on talking to Aviva’s marketing compliance team, and Credit Suisse has given us an invaluable gift in kind by regularly sharing their expertise on Crisis Management and Business Continuity Management.