Institute of Risk Management

IRM Charities Special Interest Group

An introduction to understanding and managing regulatory risk

www.theirm.org/charities

irm

Developing risk professionals

Insurance | Financial services | Infrastructure | Energy | Oil and gas | Health | Banking | Logistics

Why risk it? Get qualified

Advance your career with IRM risk management qualifications

Learn from anywhere in the world <

Study in six months <

Globally recognised <

Email: studentqueries@theirm.org

Phone: +44 (0)20 7709 4125

or visit www.theirm.org

About the Institute of Risk Management (IRM)

The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

For over 30 years our qualifications have been the global choice of qualification for risk professionals and their employers. We are a not-for-profit body, with members working in all industries, in all risk disciplines and in all sectors around the world.

About the Charities Special Interest Group

The IRM Charities 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.

To join the Charities Special Interest Group or for additional information, please take a look at our web page: www.theirm.org/charities

If you have any questions about IRM Special Interest Groups, please email membership@theirm.org.

About this guide

This guide has been designed with risk practitioners or individuals with risk management responsibilities in mind. Trustees and senior managers may also find the information useful.

We hope this guide will help you to identify relevant regulators and their requirements and help you to evidence how they are managed in your organisation.

The guide is not intended to be a comprehensive review of every regulator and their requirements. The guide focuses on regulators and managing their requirements rather than general charity law and legislative requirements. The National Council for Voluntary Organisations (NCVO) has produced a legal checklist for boards and charities which covers the legal aspects for most voluntary organisations. The Charity Commission website also contains guidance on your legal requirements.

Our authors and editors

This guidance has been produced through the input of members of the IRM Charities Special Interest Group (SIG) that formed part of the Risk & Regulation Working Group.

The main authors are:
John Greenwood, Asthma UK
Steve Brown, Alzheimer's Society
Steve Griffiths, Alzheimer's Society

With editing undertaken by:
Alyson Pepperill CFIRM, Gallagher

Contributors:
Amanda Wade, Care International UK
Charles Mitchell, Cancer Research UK
Fiona Davidge, The Wellcome Trust
Kirit Naik, ActionAid UK
Lucille Street, Help for Heroes
Marilyn Acker, VSO
Roberta Beaton, Nursing and Midwifery Council
Tracy Lumsden, Cancer Research UK

Foreword

Your charity will have a number of regulators that set the rules for how you operate and who oversee your activities. The number and range of regulators relevant to you will largely depend on your charity's activities.

The charity sector is built on a foundation of trust between charities and stakeholders. Regulations set the rules that charities are expected to follow. Transparency and the expectation that you will adhere to the highest ethical and operational standards is very important. As such, regulatory compliance is particularly important for the ongoing success of your charity.

Failure to comply with relevant regulatory requirements can have significant consequences for your charity. These include loss of trust, loss of support, reputational damage, regulatory censure, increased costs and financial penalties. Serious incidents of non-compliance can even result in the closure of your charity. There have been several incidents where charities have failed to comply with regulations. These incidents have been widely covered in social and traditional media. These incidents not only damaged the individual charities but the wider charity sector.

In short, regulatory compliance needs to be an issue high on every charity's agenda. This introductory guide has been developed to help you consider the key issues and provides a practical starting point for addressing regulatory risks in your charity.

Contents

Definitions

Item	Definition
Risk	Effect of uncertainty on objectives. The effect may be positive, negative or a deviation from the expected.
Strategic risk	These are risks that could affect or influence the delivery of your strategic aims and where the impact would be felt organisation wide.
Operational risk	These are typically internal and predictable risks and relate to day to day management. These are risks that are controlled through internal controls, policies and training.
Compliance risk	This is a risk associated with failing to meet regulatory or statutory compliance with policies or rules set by government or industry/sector regulator. This could include the Charity Commission, Fundraising Regulator, Information Commissioner's Office, Care Quality Commission, Ofsted, and Gambling Commission.
Regulation	Regulations are rules that have been made by an authority or granted to an authority in order to control an industry, a process or sector. The key difference between legislation and regulation is that legislation refers to laws that have been or are being enacted, while regulation refers to the process of monitoring and enforcing the law. For example, the Data Protection Act 2018 is the main piece of legislation and the General Data Protection Regulation (GDPR) is the main regulation that governs data protection. The ICO are responsible for enforcing these.
Regulator	A regulator is responsible for enforcing the code of conduct/ principles set out in the relevant regulation.
Enforcement	Enforcement action may be issued by regulators if organisations do not conform to the required standards. Enforcement can include financial penalties, removal of a licence to operate, and/or imprisonment.

Introduction

Why is it important to manage regulatory risks?

Your charity has people that rely on you such as beneficiaries, clients and employees. Your charity may also deliver services to commissioning bodies. Managing regulatory risk will help you demonstrate to these groups in addition to your supporters, the public and any other stakeholders that your organisation is well run and can be trusted. This helps maintain stakeholders' support for you in the longer term.

The Charity Governance Code has integrity as one of its seven principles and states: "The board acts with integrity, adopting values and creating a culture, which help achieve the organisation's charitable purposes. The board is aware of the importance of the public's confidence and trust in charities, and trustees undertake their duties accordingly".

More broadly, effective charity regulation helps underpin trust in the charity sector as a whole. The publication 'Trust in Charities' (2018) highlighted that trust in charities has a significant impact on the overall success of the sector. A poor perception of this trust (arising from non-compliance with regulations or other action/inaction by charities) can result in lower levels of support for the sector as a whole.

Who is responsible for complying with regulations?

The charity sector is incredibly diverse. The nature, size and objectives vary significantly. Recent statistics in a briefing document produced by the NCVO 'Fast facts about the charity sector'* indicates there are approximately 163,000 charities in the UK. 50% have an income of less than £10,000 per year and 97%have an income of less than £1 million. Less than 1% of charities have an income in excess of £100 million, although these large charities receive about 18% of total charity sector income.

91% of charities have no paid workforce and rely solely on volunteers to achieve their goals. Thus, many charities that are required to comply with regulatory requirements have no paid employees to manage compliance.

Charities' arrangements and resources for the management of regulatory compliance will vary. Depending on the size of your charity, you may have a dedicated compliance function that is responsible for working with the business to ensure the organisation remains compliant with all regulatory requirements. You may also use an in-house or outsourced internal audit team to provide an additional layer of assurance to the Trustees.

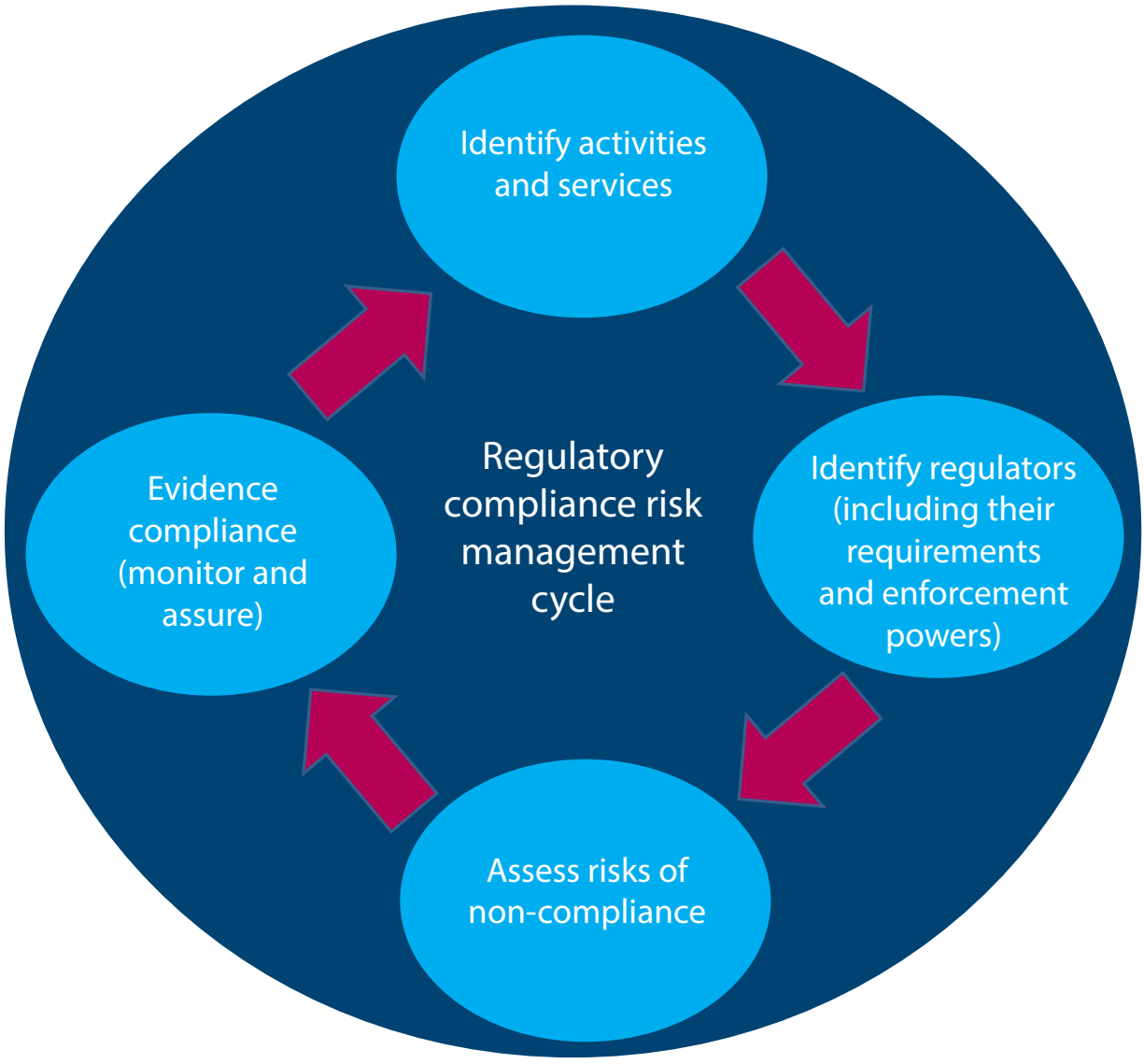
The Charity Commission is very clear that trustees are ultimately responsible for compliance with regulations.

On a practical level, all people who work for (or with) your charity will have some responsibility for their actions. This includes ensuring that they comply with relevant regulations that apply to the activities they are undertaking. Management must ensure all relevant people understand the regulations and monitor compliance.

*https://www.ncvo.org.uk/about-us/media-centre/briefings/1721-fast-facts-about-the-charity-sector

The Regulatory Risk Cycle

Our guide will follow the regulatory risk cycle set out in the diagram below:



Step One: Identify activities and services

Before you identify the regulators relevant to your charity it is necessary, as a first step, to identify the range of your activities and service provision, including any trading subsidiaries or Community Interest Companies.

Having done that you can then identify for each activity and service whether there are any relevant regulators that set the rules for that activity or service.

Remember

Even if you outsource an activity to a third-party provider you need to be confident that they are also complying with relevant regulations on your behalf. You must keep suitable records to evidence how you check this.

Step Two: Identify regulators

Who are the key regulators?

The Charity Commission

The Charity Commission for England and Wales is the non-ministerial government department that regulates registered charities in England and Wales and maintains the Central Register of Charities.

Their website gives further information on charity registration and their requirements: https://www.gov.uk/government/organisations/charity-commission

Regulators in Northern Ireland and Scotland

The equivalent body in Northern Ireland is The Charity Commission for Northern Ireland: https://www.charitycommissionni.org.uk/

The Office of the Scottish Charity Regulator (OSCR) in Scotland regulates the Charity sector in Scotland: https://www.oscr.org.uk/

Please refer to the relevant website for further information and guidance on their powers.

There are a number of other regulators that may be applicable to your organisation. Unfortunately, there is no one source of information about regulators but a useful place to start is the National Council for Voluntary Organisations website. This includes a page on Charity Law and Regulation, which has advice and signposts to other sources of information to help you identify which regulations may be relevant to you.

Some regulators are sector-wide and potentially relevant to your charity. Here are some examples:

- Information Commissioner's Office (ICO) - The ICO is responsible for enforcing data protection and freedom of information rights. The ICO is responsible for enforcing GDPR and Privacy and Electronic Communications Regulations (PECR) in the UK.
- Fundraising Regulator - Independent regulator for charitable fundraising in England, Wales and Northern Ireland.
- Health and Safety Executive (HSE) - Independent regulator for work-related health, safety and illness in the UK
- Advertising Standards Authority (ASA) - The ASA is the independent regulator for advertising across all media (broadcast, print and media).
- The Pension Regulator - The body responsible for protecting workplace pensions in the UK.
- HM Revenue and Customs (HMRC) - The HMRC are responsible for tax, payments and customs in the UK.

Other regulators

There are also regulators that are sector or activity specific. To help you identify these types of regulators, you could consider the following questions about your activities and services (this is not an exhaustive list):

- Does your charity run a society lottery or raffle? If yes, you may need a licence for the Gambling Commission and to comply with the Gambling Commission's Licence Conditions and Code of Practice (LCCP).
- Does your charity use a fundraising agency to conduct any of your activities? If yes, you will have to comply with the Fundraising Regulator's Code of Fundraising Practice. You must also have systems in place to monitor that the fundraising agency also complies. For example, the Fundraising Regulator is responsible for regulating charitable fundraising in England, Wales and Norther Ireland. You should also be aware of the Institute of Fundraising, a membership body for fundraisers, who have produced their own Code of Conduct.
- Do you provide education or training to children or young people? If yes, you may need to be registered with Ofsted. Check their website for further details on registration.
- Do you produce advertising or media campaigns? If yes, the adverts must comply with the Advertising Standards Authority's (ASA) advertising code.
- Do you provide regulated health or social care, such as residential or nursing care or domiciliary care? If yes, and you operate in England and Wales you must be registered with the Care Quality Commission. Northern Ireland and Scotland have equivalent regulators.
- Do you transfer funds overseas? If yes, you may need to refer to local and international sanctions requirements and undertake additional checking on local partners.

You will need to think more deeply about this to identify the full list of regulators that apply to your charity, all within the context of your charity's activities and the services you provide.

Don't forget to engage widely across the organisation when you are identifying regulators.

There are a number of other organisations that are not regulators but who will promote best practice; for example, the Charity Finance Group (CFG) champions best practice in financial management: https://cfg.org.uk/about

Identify regulatory requirements

Once you have identified the regulators that are relevant to your charity, you then need to identify their requirements that you need to comply with. This can be complex, but the regulator's website is a good starting point. You may also wish to refer to the NCVO's webpage on 'Charity Law and Regulation'*.

Regulators work in a variety of ways and it is important that you are aware of their expectations and any incident reporting requirements e.g. the HSE requires Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) reporting and the ICO for data breaches.

Some regulators, for example the Charity Commission, Gambling Commission and Companies House , require you to complete regular returns. The NCVO suggests it is helpful if you create an organisational calendar of key dates to ensure you have oversight over your responsibilities during the year.

Some regulators may conduct audits and spot checks to review your compliance and others may not routinely engage with you unless there has been an identified issue, for example a serious complaint, a media report, or a whistleblowing event.

Many regulators use principles rather than fixed rules and explicit directions. Principle based regulation is often open to interpretation, so if in doubt you should seek further guidance and clarification.

* https://www.ncvo.org.uk/policy-and-research/charity-law-and-regulation

Example: The Fundraising Regulator

The Fundraising Regulator was introduced in 2016 and replaced the Fundraising Standards Board. It has published its Code of Fundraising Practice which sets out the standards that all charities and third party agencies that engage in fundraising activities are expected to adopt and comply with. The Fundraising Regulator will investigate complaints where charities have failed to meet the expected standard and may refer the charity to other regulators as appropriate.

Remember

Regulators, their powers and their responsibilities will change over time and it is important to keep up with any changes and the impact this will have on your charity. For example at the time of publishing this guidance the Fundraising Regulator is consulting on a review of the fundraising standards.

Understand the powers of the regulators

The next step is to identify the powers of each Regulator and the potential impact if you fail to comply. These powers can have significant consequences for your charity.

Regulators are responsible for monitoring, guiding and promoting best practice. If a charity fails to comply, regulators have the power and authority to impose a range of sanctions. The powers of regulators differ but can include imposing fines, removal of licences, removing Trustees, freezing assets and referral to other regulators.

Regulators usually publish their findings and the actions they take on their websites which may result in media interest.

Understand the potential consequences of non-compliance

The following table highlights potential impacts of non-compliance on your organisation:

Who is affected?	Potential consequences of non-compliance
Beneficiaries	• Loss of trust from beneficiaries • Reduction in services provided
Donors	• Loss of trust from donors • Support withdrawn
Partners	• Loss of financial support • Loss of corporate sponsorship
Organisation	• Reputation damaged • Poor morale and resignations from leadership team, trustees etc. • Management time and resources • Loss of staff • Fines imposed • Adverse media stories • Inability to achieve strategic objectives

To have a better understanding of the expectations of your regulators it can be helpful to record the following details (see Appendix 1 for an example template):

- Name and overview of their regulatory role and purpose
- Their powers
- Maximum fines/penalties for non-compliance
- What do you need to comply with e.g. code of conduct, fundamental standards, licences etc.
- Identification of responsibility in your organisation for compliance with regulator's requirements - there may be more than one person within an organisation and may be best undertaken by someone close to the relevant business area rather than by someone at the centre of the organisation.

International charities will also have to consider:

- How the requirements vary for each country in which your organisation operates.

Summary

- Identify and list your activities and services
- Engage widely across your organisation to understand the full scope of regulation relevant to you and review the NCVO website
- Bear in mind there may be other organisations that are not regulators as such but which promote best practice that stakeholders may expect you to follow
- Next identify the regulatory requirements and the potential consequences of non-compliance by consulting the regulator's individual website
- Consider whether to use a table to record the expectations of your regulators (see Appendix)
- Develop a process to ensure changes to regulations are monitored and action taken when changes are made
- Keep a log of regulators, their powers, your responsibilities, and internal owners

Step Three: Assess risks of non-compliance

You are now ready to assess the risks of your organisation not complying with the relevant regulatory requirements. You could take a workshop approach to this assessment and involve relevant people with expertise of the business area in your organisation. This will ensure that you capture all of the regulators that are relevant to your organisation.

You should use your organisation's existing risk management process and risk assessment criteria to help ensure risks are assessed consistently across the organisation. Record the likelihood of a regulatory risk occurring and the impact if it were to occur and record your assessment

If you do not have an existing risk management process please refer to the IRM's Getting Started guidance and the *Charity Commission's guide Charities and Risk Management* (CC26).

Summary

- Assess regulatory risk across the organisation
- Integrate the findings into your existing Corporate Risk Register or other risk management process

Step Four: Evidence compliance

It is very important that your organisation can demonstrate that it complies with regulatory requirements – to comply and to be seen to comply. The evidence you gather needs to be up-to-date, tangible and robust.

It may be helpful to refer to a requirements list for each regulator and then identify how you can evidence compliance.

This process will help to identify any gaps, for example, a lack of training, policies or internal controls that can be improved etc.

See an example below (taken from the Fundraising Regulator's Code of Fundraising Practice) for how a documentated record could work in practice:

Rule	Evidence and status	Location of evidence	Actions/Owner/ Date
Fundraising code Complaints: Organisations MUST have a clear and publicly available complaints procedure which MUST also apply to any Third Parties fundraising on their behalf	Published complaints policy and procedure. Status: current	Website	
	Minutes of annual review of policy by Fundraising Committee with sign off by Director and Trustee approval Status: current	Committee records folder	
	Contract with third party fundraisers outlines their requirements to comply with the complaints procedure. Status: Under review	Contracts folder	Complete contract review. Fundraising manager by Q3

Summary

- Develop a demonstrable process to evidence compliance
- Undertake a gap analysis to identify where you may have insufficient evidence to demonstrate compliance
- Take action to close any gaps and agree ownership of actions and due dates
- Make the actions as clear as possible

Key messages

The sector is so diverse that it is difficult to create a resource that covers all regulators and their requirements. Each charity needs to identify and assess its regulatory risk exposures to ensure that these risks are managed and there is supporting evidence to confirm compliance.

When you have mapped out your regulatory landscape, the management of regulatory compliance will come down to four main areas:

- People – who is directly responsible for each risk?
- Process – how the risk of non-compliance is managed?
- Evidence – how can you prove you are compliant
- Actions – to improve/continue compliance

Remember

The regulatory framework and requirements will change over time, monitoring and review is essential to ensure you understand and respond to changing regulatory requirements.

Our next guide will tackle how a charity can achieve assurance that they are complying with all relevant regulatory requirements throughout their organisation.

We hope you find this of interest. You can find our other publications on our web page: www.theirm.org/charities

These include:

- Getting Started with Risk Management
- Risk Management for Charities: Getting Better
- Risk Maturity Framework
- Setting Risk Appetite
- Risk Governance for Charities: Risk Management Structures and
- Accountabilities
- Stakeholder Mapping for charities

Appendix

Regulator	Overview	Powers	What are their key requirements?	Maximum fines/ penalties for non-compliance
Charity Commission	The Charity Commission is the independent Government department which registers and regulates charities in England and Wales.	• Conduct statutory notifications • Freeze a charity's bank accounts • Appoint additional Trustees • Suspend or remove a Trustee • Appoint an interim manager • Restrict the transactions a charity may enter into	The Charity Commission have produced a range of guidance documents that outlines their expectations.	Significant reputational damage for non-compliance which may lead to loss of donors, corporate partnerships, media scrutiny, long term damage to the brand and potentially closure.
Information Commissioners Office (ICO)	The Information Commissioners Office is responsible for upholding information rights in the UK including the Data Protection Act 2018, Privacy and Electronic Communication Regulations and Freedom of Information.	• Conduct audits to ensure the organisation is complying with their obligations • Serve enforcement notices if there has been a breach and prosecute if the organisation fails to comply with the enforcement notice.	The ICO cover a range of legislation and regulation including GDPR, Data Protection Act, Privacy and Electronic Communication Regulations, Freedom of Information Act.	The ICO has the power to serve a fine up to €20 million or 4% of an organisation's annual global turnover where a breach of the Act has caused substantial damage or distress and the data controller failed to take responsibility.

Regulator	Overview	Powers	What are their key requirements?	Maximum fines/ penalties for non-compliance
Fundraising Regulator	The Fundraising Regulator is the independent regulator for charitable fundraising in the UK which was launched on 7th July 2016.	• Set and promote the standards for fundraising practice • Investigate cases where fundraising has led to public concern • Adjudicate complaints from the public • Recommend best practice • Take proportionate remedial action.	Fundraising Regulator's Code of Fundraising Practice.	The Fundraising Regulator can refer incidents of non-compliance to other regulators.
Health and Safety Executive (HSE)	The HSE is GB's independent regulator for work-related health, safety and illness. Their goal is to prevent workplace death, injury or ill health.	The HSE can serve improvement and prohibition notices, withdraw approvals, vary licence conditions or exemptions, issue formal cautions and they may also prosecute.	The HSE provides guidance and tools to help businesses understand what they need to do to assess and control risks in the workplace and comply with health and safety law.	For offences committed on or after 12/3/15 the maximum penalty in the magistrates' court is an unlimited fine or imprisonment for a term not exceeding 6 months or both. In the Crown Court, the maximum penalty is an unlimited fine or imprisonment not exceeding two years or both.

Institute of Risk Management

Institute of Risk Management
2nd Floor, Sackville House
143–149 Fenchurch Street
London
EC3M 6BN

www.theirm.org

irm

Developing risk professionals