

IRM Charities Special Interest Group

Tools for providing assurance on regulatory compliance



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 is a companion to our guide: [*An introduction to understanding and managing regulatory risk*](#) and is designed with risk practitioners or individuals with risk management and compliance responsibilities in mind. Trustees and senior managers may also find the information useful.

The guide is based on the assumption that you understand the legal and regulatory framework in which your charity operates and that based on your charity's activities – you understand the legal and regulatory requirements that you are subject to.

If you are not clear on the regulatory framework for your charity, we advise you to start by reading our introductory guide, which is available here:

https://www.theirm.org/media/4053855/Managing-regulatory-risk_final.pdf

Our authors and editors

Produced through input of members of the IRM Charities Special Interest Group (SIG) detailed below who formed part of the Risk & Regulatory Assurance Working Group.

The main authors are:

Steve Brown, Alzheimer's Society
Steve Griffiths, Alzheimer's Society

With contributions and editing undertaken by:

Alyson Pepperill CFIRM, Gallagher
John Greenwood, Asthma UK

Working Group Contributors:

Alex Paterson, British Heart Foundation
Amanda Wade, Oxfam
Charles Mitchell, Cancer Research UK
Greg Salter, retired
Jane Bettany, Historic Royal Palaces
Kim Spiers, Prince's Trust
Lucille Street, Help for Heroes
Sanna Lindstrom, Plan International
Tracey Lumsden, Cancer Research UK

Foreword

Your charity will have a legal and regulatory framework in which it operates. It is likely that there are a number of regulators that set the rules for how you operate and who oversee your activities. If your charity operates internationally, you also need to take account of the relevant law and regulations of the countries in which you operate.

Charities need to comply with all relevant laws and regulations and be seen to comply. Actual non-compliance and a failure to evidence compliance can have significant consequences for your charity and its stakeholders. These include loss of trust, loss of support, reputational damage, regulatory censure, increased costs and financial penalties. The [Charity Commission](#) recently stated that:

When it comes to trust and confidence, the challenges facing charity are considerable. The Charity Commission has been tracking public trust in the charitable sector for more than a decade and [public trust] has drifted lower in recent years to where it now stands: at the lowest level since our monitoring began.

In short, legal and regulatory compliance needs to be high on every charity's agenda. In the worst case, an inability to evidence compliance can result in legal action against individuals and the closure of your charity. This guide provides practical tools to help you provide assurance on your charity's compliance with relevant laws and regulations.

A key challenge in the provision of assurance is to ensure that it is reasonable and proportionate to the size and needs of the charity and its legal and regulatory framework. You can adapt the tools in this guide to the size and complexity of your charity.

These tools are not limited to evidencing compliance with legal and regulatory requirements. You can also use them for providing assurance over any risk or demonstrating compliance with any policy or procedure in your charity.

This guide will be of most benefit to you when your charity has a risk management process and a system for identifying and understanding the laws, regulators and regulations relevant to your charity. If you do not have these in place yet, please refer to our guides [Getting started with Risk Management](#) and [An introduction to understanding and managing regulatory risk](#).

Contents

Definitions	6
Introduction	7
Assurance and Compliance in Overview	8
1. What is assurance?	8
2. Why do you need assurance around compliance with laws and regulations?	8
3. What is compliance?	9
Tool 1: Developing an assurance framework	9
4. What is an assurance framework?	9
5. How to develop an assurance framework for legal and regulatory risk	10
6. Sources of assurance - the three lines of defence	10
Tool 2: Business Compliance Self-Assessment	12
7. What is a business compliance self-assessment and where does it fit in the three lines of defence model?	12
8. What areas of activity does the business compliance self-assessment cover in relation to compliance with laws and regulations?	14
9. What are compliance statements and how are they developed?	14
10. Completing, checking and reporting of business compliance self-assessment returns	17
11. How to use the outcomes of the business compliance self-assessment	18
Tool 3: Assurance map	19
12. Using an assurance map	19
13. Key messages from this guide	23
Annex 1: Three lines of defence - Compliance assurance models by charity size	24

Definitions

Item	Definition
Assurance	An examination of evidence for providing an assessment of governance, risk management, and control processes for the organisation.
Compliance	Making sure that any activity conducted by an organisation is within the legal parameters and that reasonable actions are taken in order to prevent incidents of non-compliance with relevant laws and regulations.
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 an organisation's 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 risks are controlled through internal controls, policies and training.
Compliance risk	This is a risk associated with failing to meet legal or regulatory compliance with policies or rules set by government or industry/sector regulators. This could include, in the UK, the Charity Commissions (England and Wales, Northern Ireland, and Scotland) Fundraising Regulator, Information Commissioner's Office, Care Quality Commission, Ofsted, and Gambling Commission. It could also include failing to comply with the Bribery Act 2010 and the Modern Slavery Act 2015. If your charity operates internationally, you would need to be aware of the relevant laws and regulations of the countries in which your organisation operates.
Laws and Regulations	<p>Laws are the written rules made by parliament, which state the principles of what a person can and cannot do. They are enforced by government officials such as police officers, agents and judges. To become enacted, laws go through the process of checks, balances and votes in order for them to become a law.</p> <p>Regulations set out how a law will be implemented and enforced. They are added by government departments and bodies to put laws into practice. Parliament delegates power to certain bodies to make such regulations. The purpose of a regulation is to ensure that a particular law is put fully into effect. A regulation is always secondary to the law it implements.</p> <p>For example the Data Protection Act 2018 is law, the Information Commissioners Office is the regulator that interprets the law by setting out regulations of how to implement the law and regulates through enforcement action.</p>
Regulator	A regulator ensures a law is put fully into effect by making regulations and enforcing these.

Introduction

Trustees, management, donors, governments, regulators and other stakeholders need to rely on the successful conduct of business activities, sound internal processes and the production of credible information.

These operational and reporting processes enable users to make decisions and develop policies. Confidence diminishes when there are uncertainties around the integrity of information or of underlying operational processes.

This guide provides practical tools to help charities assess their level of compliance with relevant laws and regulations and thereby better manage their compliance risks. These tools can help the your organisation provide assurance to its trustees and senior manager(s) that existing controls to manage legal and regulatory compliance risks are fit for purpose and working effectively.

If the controls fail or are not fit-for purpose, the effectiveness of the charity's risk management will be compromised and the organisation could fail to comply with the relevant laws and regulations. The consequences of such a failure could be severe.

This guide considers three main tools to help provide reasonable and proportionate assurance:

1. Developing an **assurance framework** for the organisation
2. A **business compliance self-assessment** (BCSA) to provide regular evidence from your front-line staff on the level of their compliance with existing controls
3. An **assurance map** to map out and assess the coverage and quality of current sources of assurance in managing legal and regulatory risks.

Larger charities often use these tools to provide assurance to their trustees. The examples in this guide can be adapted to be relevant to legal and regulatory compliance risks of a charity of any size. Our companion guide: [An introduction to understanding and managing regulatory risk](#), explains how to determine the regulations, which are relevant to a charity's activities.

These tools are universally applicable and organisations can use them for providing assurance on controls relating to other types of risks, although this is not covered within this guide.

In this guide the use of the term 'trustees' includes trustees of incorporated charities who are also 'directors' under Company Law.

Assurance and Compliance in Overview

1. What is assurance?

Trustees are legally responsible for ensuring their charity complies with relevant laws and regulation. Trustees and senior manager(s) require assurance of the organisation's level of compliance, as this impacts the ability of the organisation to deliver on its strategic aims and objectives.

There are a number of laws and regulations, which apply to most charities operating in the UK, for example:

- Charity Commission regulations
- Tax law and regulations
- Company law
- Employment law
- Health and Safety law and regulations
- Fundraising law and regulations

There may also be some laws and regulations which apply only to certain types of charities.

The trustees and senior manager(s) will want assurance that the charity is compliant with all these legal and regulatory requirements. If the charity operates in more than one jurisdiction you will need to make sure that your assurance covers the relevant laws and regulations in all the countries in which your charity operates.

2. Why do you need assurance around compliance with law and regulations?

Demonstrating compliance with relevant law and regulations brings a number of benefits to a charity, its trustees and managers:

- It helps build and maintain trust with regulators, beneficiaries, employees and volunteers, supporters, the general public, partners and government bodies.
- It may provide a competitive market advantage when applying for the delivery of commissioned services.
- It highlights instances where improvements should be made to internal processes and procedures to improve the level of compliance.
- It provides additional insights into the operational health and maturity of the organisation.
- It provides an independent perspective as to the level of compliance with regulatory risk, thereby ensuring decision making and actions are based on an accurate position.

Failure to demonstrate compliance can have serious consequences for a charity. These include:

- Loss of trust
- Loss of support,
- Reputational damage
- Regulatory censure
- Increased costs and financial penalties
- Redundancies and resignations
- Closure of the charity

3. What is compliance?

In general, compliance means conforming to a rule, such as a specification, regulation, standard or law.

In this guide, we describe legal and regulatory compliance as making sure that any activity conducted by an organisation is within legal and regulatory parameters and that reasonable actions have been taken in order to prevent incidents that breach these parameters.

It is important to remember that charities may be required to provide evidence to demonstrate the level of their compliance.

Tool 1: Developing an assurance framework

4. What is an assurance framework?

Overview

In general this framework sets out how a charity's trustees will seek assurance on the effectiveness of its governance arrangements and its risk and control frameworks. Providing assurance on complying with relevant laws and regulations is a key requirement for any charity and is the focus of this guide.

An assurance framework represents accepted good practice across sectors, supports trustees to ensure their delegated authority is exercised appropriately, and helps to evidence that the organisation is following the Charity Commission for England and Wales [“Essential Trustee” guide](#) (CC3) and the [Charity Governance code \(2017\)](#).

Principle 4 ‘Decision-making, risk and control.’ of the Code states:

“The board makes sure that its decision-making processes are informed, rigorous and timely, and that effective delegation, control and risk-assessment, and management systems are set up and monitored”.

An assurance framework sets out accountabilities within a charity for providing evidence of assurance. It also acts as an opportunity to showcase good practice and demonstrate for both internal and external stakeholders that the organisation is managing legal and regulatory risks effectively.

Principles

This guide recommends developing a framework that is informed by the charity's risk management arrangements. It should be proportionate to the charity's legal and regulatory context, size and needs. It should be based on principles agreed with the charity's trustees. The following principles may be helpful to consider with trustees:

- The focus of assurance activity will be risk based.
- Assurance will reflect the accountabilities set out in your charity's governance arrangements, including any scheme of delegation.
- Assurance arrangements will reflect accepted good practice (e.g. built around the ‘three lines of defence’ assurance model outlined in section 6 below).

5. How to develop an assurance framework for legal and regulatory risk

You will need to agree with your senior manager(s) and trustees the level of assurance that is reasonable and proportionate to the charity's needs. You will need to take account of the relevant legal and regulatory framework in which the charity operates and the frequency which the senior manager(s) and trustees expect to receive assurance.

Board of trustees – The trustees are legally responsible and accountable for their charity's compliance with relevant laws and regulations from a risk and assurance perspective. They need to determine the level of assurance they require and the scope of the assurance framework, based on the context in which the charity operates. The framework should make clear:

- Legal and regulatory requirements that are in scope.
- How assurance is provided, such as discussions with managers, assessment of policies and procedures, and internal/external audits
- The mechanisms by which evidence is gathered.
- How the organisation will report on the level of assurance to the trustees.
- How the organisation will deal with any gaps in assurance.
- How any weaknesses in controls will be addressed in order to provide the appropriate level of assurance.

The senior manager(s) as well as managing day-to-day activities, is/are ultimately responsible for providing the trustees with assurance on the charity's compliance with relevant legal and regulatory requirements.

Other roles and responsibilities – Dependent upon the size and structure of the charity there may be other individuals with specific responsibility for activities that are subject to regulations (for example financial management, people management, and fundraising). These managers are responsible for compliance within their areas of responsibility so are a valuable source of assurance.

Examples of sources of external assurance:

- Reports from in-house internal auditors
- Reports from external auditors where a charity is required to have its accounts audited
- Reports from a third party if used by a charity to provide an internal audit function
- A charity may choose to bring in external professionals to audit specific areas of compliance risk, for example Health and Safety

6. Sources of assurance – the three lines of defence

The three lines of defence model is accepted good practice and one way that organisations (including charities) seek to provide assurance. It is dependent on having adequate sources of assurance at certain levels within the organisation. It can be hard for charities, particularly small and medium, to have three distinct lines.

There is ongoing discussion about the number of lines of defence but for the purpose of this introductory guide we use three lines as described below. Please see annex one for more information on how the three lines of defence could work in a small, medium and large charity (See Annex 1).

The first line of defence in ensuring compliance with relevant laws and regulations comes from individuals that own and manage risk. These could be frontline operational managers and those that work in support functions, such as Finance or Human Resources.

Compliance with relevant laws and regulations should be inherent in operational processes and procedures. We have called this line '**doing**' and it includes any initial level of operational management review or control.

The second line of defence comes from the charity's oversight arrangements. This is often carried out by individuals within the organisation that have a specialist expertise or knowledge in relation to the laws relevant to the charity and may write and own the organisations' policies. To ensure critical objectivity, second line assurance comes from an individual who is not doing the work they are checking. We have called this line '**checking**'.

The third line of defence typically comes from independent auditors who can be internal or external. We have called this line '**verifying**'.

The table below describes the three lines of defence model in more detail. It is important to remember that these lines of defence can have blurred rather than rigid boundaries.

First line: Doing	Second line: Checking	Third line: Verifying
Description: The processes in place at the 'front line' of the business that enables risks to be managed and relevant laws and regulations to be complied with.	Description: The processes associated with the oversight and review of front line activity. Provides management insight into how well work is being carried out compared to set expectations and policy, legal and regulatory requirements.	Description: Independent assurance conducted to provide trustees and the senior manager(s) with an opinion on the framework of governance, risk management and the design and operation of controls. This may involve commissioning a comparison with good practice of similar organisations.
Examples: Documented business process controls, management information, risk registers, performance reports, implementation of policies and processes to meet regulatory requirements , such as a business compliance self-assessment process	Examples: Regulation and compliance assessments, reviews of policy implementation, setting and monitoring internal guidelines, 'deep dive' reviews of risks and challenges to how legal and regulatory risks are managed.	Examples: Internal auditors, independent specialist bodies (e.g. Investors in People, ISO etc.), and external auditors. In the UK, some charities will require external auditors who have statutory responsibility for certification of the financial statements
Points of note: The value lies in the assurance coming from people who know the day-to-day business and its legal and regulatory requirements.	Points of note: Separate from those responsible for delivery. More objective than first line, but not independent of the management chain. They have more detailed knowledge about relevant laws and regulations and can horizon scan for future changes in laws and regulations and future risks. They may need to learn about new subjects in order to make a challenge.	Points of note: The value lies in the independence and objectivity of the assurance. Review of assurance mechanisms in first and second lines to target effectively areas of highest risk and identify gaps/weaknesses in the control framework. It may be expensive but there may be pro-bono support available for smaller charities.

Tool 2: Business compliance self-assessment

7. What is a business compliance self-assessment and where does it fit in the three lines of defence model?

A business compliance self-assessment (BCSA) is a way that managers can provide systematic assurance that they and their teams are complying with their organisation's policies and procedures. The BCSA is primarily a tool used by the second line for gathering evidence on compliance from the first line (see the model on the next page).

This guide focuses on using the BCSA for compliance with policies and procedures relating to legal and regulatory requirements. It can be used for checking compliance with any policy or procedure or other documented internal control requirement.

When used regularly, the BCSA provides ongoing evidence of compliance rather than a snap shot of adherence at a single point in time. Similar to an assurance framework, the BCSA needs to be proportionate to the charity's size, needs and the legal and regulatory framework in which it operates.

The BCSA comprises compliance statements and associated core evidence, against which relevant individuals in the organisation need to self-assess their compliance. The self-assessment should be signed as completed at agreed designated intervals.

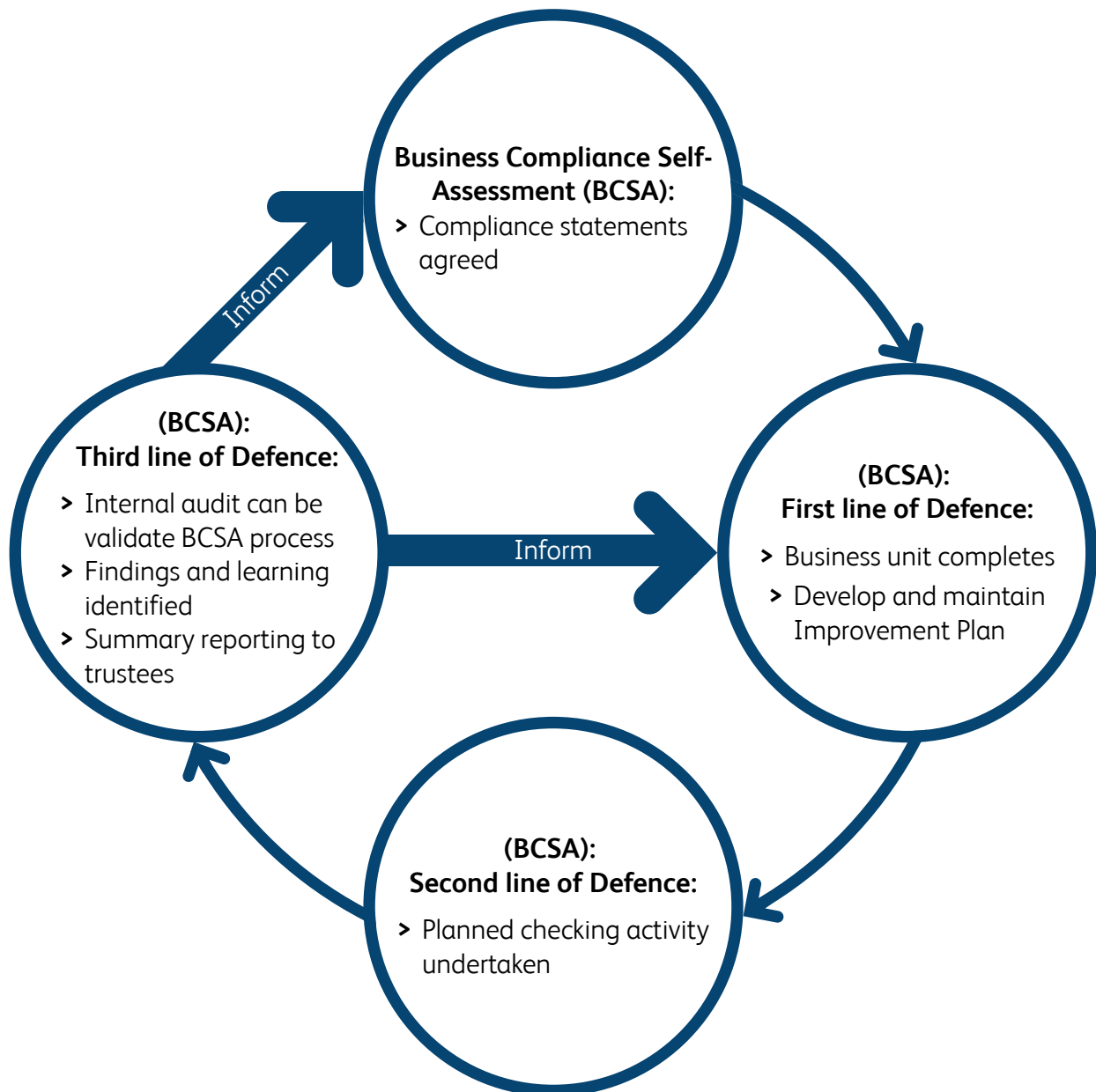
The BCSA is part of the organisation's assurance framework and acts as a formal record. It forms a basis for the assurance the charity seeks on legal and regulatory compliance from its operational managers. These managers are accountable for the accuracy and honesty of their returns.

The BCSA provides useful feedback on the organisation's existing controls. For example, the self-assessments should indicate if there are problems complying with policies and procedures at the front-line or in finding the evidence to support compliance.

This feedback can be used to both improve policies and procedures and to improve compliance. The diagram on the next page sets out the compliance assurance process.

Business Compliance Self-Assessment – Assurance Process

Version 1.0 – Date: 04 February 2019 (Author: Steve Brown)



Remember there are key things that you should make clear when implementing a BCSA:

- Make clear how the BCSA adds value to the core activities of the charity i.e. by helping to prevent non-compliance with relevant laws and regulations
- Make sure that managers are aware that they are accountable for the accuracy and honesty of their returns. Also, make clear that there will be a checking process so there are no surprises that evidence to support assessments within the BCSA will be checked and self-assessments will be challenged if the evidence does not support the self-assessment.
- Make clear that the results of the BCSA will be reported to the senior manager(s) and trustees and that completion is mandatory
- Make clear the frequency of the BCSA.
- Make sure you set the frequency to suit the needs of your organisation and the length of your questionnaire. Give sufficient time for any improvement actions to be conducted between questionnaires. In practice, a quarterly or bi-annual BCSA is often chosen. Depending on the organisation an annual return may not be frequent enough to add any value to improving your control framework.

8. What areas of activity does the Business Compliance Self-Assessment cover in relation to compliance with laws and regulations?

This will depend upon three things:

- The relevant legal and regulatory framework in which your charity operates
- The scope of the assurance framework agreed with your trustees
- The level of assurance that the organisation has on its controls to manage legal and regulatory risks through other mechanisms

You can cover any area of compliance relevant to your charity's legal and regulatory framework within your BCSA such as:

- Financial management
- People management
- Health and safety
- Data protection
- Anti-bribery and counter-fraud
- Safeguarding
- Fundraising

Remember the areas you cover should be informed by your legal and regulatory risks, the evidence you have gathered on the effectiveness of your existing controls, and any gaps in your controls. This will help you focus your BCSA on priority areas and keep it proportionate to your organisation.

9. What are compliance statements and how are they developed?

In the context of legal and regulatory risk a compliance statement asks a manager to self-assess to what level they and their team comply with relevant requirements. The statement should reference the organisation's policy and procedures relevant to the compliance area under consideration. The view of the person completing the self-assessment must be supported by evidence. The BCSA includes core evidence for each statement and allows managers to add in any additional evidence. For consistency the BCSA in this guide gives the person completing the BCSA four options in terms of the assessment of the level compliance:

- Met
- Partially met
- Not met
- Not applicable

If asked, the manager should be able to provide the evidence to support their response to the compliance statement. Additionally the evidence should be easy to check.

If the compliance statement is 'partially met' or 'not met', the BCSA should make clear that the manager must record improvement action(s) that show how they plan to reach full compliance within an appropriate timescale (or get documented approval from the policy owner for any compliance exemption).

The statements and their supporting core evidence are best developed with the individual(s) in your organisation who own or have the lead on the areas of compliance that the trustees wish to see included within the BCSA.

We recommend that a test of the statements and evidence is done before the BCSA is implemented. The test should include a pilot of the statements and the process with a sample of managers who will be completing the self-assessments. This provides an opportunity to make sure it makes sense to people who have not been involved in the development of the BCSA. The pilot may give rise to further amendments and re-writes of statements and evidence in order to get the BCSA as accurate as possible before it is implemented organisation-wide. When testing, keep the following questions in mind:

- Can you easily find the written policy, process or guidance to which the statement relates?
- Does the statement ask for compliance with something that is not clearly stated in the relevant policy, process or guidance?
- Is the relevant policy, process or guidance in date?
- Is the evidence to support compliance with the statements easy to access?

If the answer to any of the above questions is '**No**', go back to the statement owner and ask them to resolve the issues before the compliance statement is included within the BCSA. This may also indicate that there would be value in improving arrangements for the governance of policies in your charity.

It is good practice for trustees and senior managers check and confirm the content, and to sign off the BCSA to demonstrate good governance and ownership.

An example of a compliance statement

In this example, the trustees want to include a section in the BCSA on data protection. Their assurance map has evidenced that their data protection policies and procedures are up-to-date but they have no current mechanism to know or evidence that their staff and volunteers are complying with these policies and procedures in their day-to-day activities (see pages [20-21] for the assurance map example).

The charity has now completed its assurance map action to review the incident/breach log. The review highlighted a key theme:

- Incidents in the log evidenced that some new employees and volunteers had not completed their mandatory training or read the key policies during their induction period as required by the organisation's policy.

An example of the relevant entry in the BCSA for this compliance area could be:

Data protection

Compliance Statement DP1

Learning and awareness – **All** staff and volunteers in my team understand the importance of complying with our policies and procedures in relation to protecting personal data, and have the knowledge to ensure they are able to meet expectations.

Met ☐ Partially met ☐ Not met ☐ Not applicable ☐

Core evidence	Percentage
% of new employees who have completed the Data Protection mandatory training within their induction period.	
% of new volunteers who have completed the Data Protection mandatory training within their induction period	
% of employees who have recorded that they have read and understood our data protection policy and procedure	
% of volunteers who have recorded that they have read and understood our data protection policy and procedure	
Optional: Any additional evidence?	

Actions required (Please list any improvement actions required to achieve compliance, where you have ticked Partial or None in your assessment of your current compliance)				
No	Action	Who	When	Update
1				
2				

Some key points to note when developing your BCSA:

- Make the statements easy to understand, fact-based, and clear so they are not open to interpretation. Develop them with the relevant subject matter experts or leads in your organisation – these people must own the statements,
- Make sure the statements relate to relevant policy or procedure – resist asking people to assess their team's compliance with aspects that are not written down anywhere or with requirements they have never been asked to do.
- Make sure the evidence is available and verifiable. For example, resist asking people to provide evidence that they have read and understood policies, if no such recording mechanism is in place within the organisation.
- Pilot the statements before implementing the BCSA organisation-wide

10. Completing, checking and reporting of Business Compliance Self-Assessment returns

Completing returns

- Make sure guidance can be provided on completing returns to ensure people understand what is expected of them so that returns are completed consistently.
- Make sure it is clear that where compliance is shown as partial or not met, SMART (Specific, Measurable, Achievable, Relevant and Time-based) action(s) need to be added to illustrate how compliance can be achieved.
- Make sure managers completing the return understand that they have accountability for completing improvement actions to achieve compliance within their area of responsibility.

Verifying the BCSA returns

To ensure accountability there must be a validation procedure in place to check evidence exists to support assessments and improvement actions are completed. The validation procedures should be carried out by individuals from the second line of defence wherever possible.

The person validating the returns should also follow up with the relevant manager where the evidence does not support the self-assessment and/or improvement actions are not completed. The diagram in section 7 indicates how this validation programme forms a key part of the assurance process.

If there are a large number of returns, the validation procedure can be based on a sample of returns. The sample may be selected on a risk managed basis depending on the type of work carried out by the organisation. If sampling is carried out, ensure that the validation procedures sample returns from all teams within a reasonable period.

Reporting

You need to analyse the returns to report on the outcomes to managers, trustees and the subject matter experts responsible for the areas of regulatory compliance covered by the BCSA.

11. How to use the outcomes of the Business Compliance Self-Assessment

Prioritising areas for support and development

The BCSA can be useful in highlighting areas where compliance is problematic or highlight areas where partial or non-compliance is systemic within the organisation.

BCSA can also highlight that the organisation's policies and procedures in certain areas may not be fit for purpose and need review.

The BCSA outcomes can be also used to inform trustees so that they can direct 'finite' third line resource such as internal audit, to focus on priority areas.

Senior management have responsibility for ensuring adequate oversight of the progress of improvement actions across the organisation.

Identifying trends

The organisation can prepare a trend analysis to show where compliance has changed, for either better or worse. This can be linked back to the trends in scores of relevant risks.

Managers should take action if trend analysis shows that compliance is not improving over time.

Managers completing the return have accountability for completing improvement actions to achieve compliance within their area of responsibility.

Annual report

The outcomes of the BCSA can be used in the charity's annual report as evidence of how the organisation is managing the major regulatory risks.

Tool 3: Assurance Map

12. Using an assurance map

When the trustees have agreed an assurance framework a baseline of current compliance with relevant legal and regulatory requirements should be established.

One tool for doing this is to use an assurance map, which visually maps out the legal and regulatory requirements on which the trustees want assurance and the current sources of assurance that the organisation has at each line of defence.

The people in the charity, who are most knowledgeable about relevant laws and regulatory requirements, should be involved in completing the assurance map. These may often be the individuals who own the organisational policies and processes for complying with these requirements. Their involvement will help to identify existing sources of assurance, potential assurance gaps, and potential gaps in evidence of compliance.

Before starting the mapping process we recommend you consider these tips:

Include clear definitions to ensure all users understand each column and entry in the map. Depending on what you want it to show, the map could show any, or all of, the following:

- Existence/coverage of assurance activity against a risk
- Source(s) of assurance
- Quality (depth, breadth, reliability) of the assurance activity
- Outcome of the assurance activity

Where the map shows more than one of the above and uses Red/Amber/Green (RAG) status indicators try to avoid rating everything on one map as it may become visually confusing.

Depending on the charity's needs, the assurance map can be structured in a variety of ways. In this guide we provide an example of an assurance map of a charity's controls to manage data protection compliance risk.

Example Assurance Map

Objective	Risk	Risk ref and owner	Controls	Impact	Likelihood	Risk trend (*)	
1.1 To protect the privacy of individuals and comply with Data Protection regulations	Data Protection regulations breach because our people are not following our agreed policies and procedures	Risk: 1 Director of charity	Data Protection policies and procedures Mandatory Data Protection training Incident reporting	High	Possible	Constant	

* Risk trend = has the risk increased, decreased or remained constant since the previous review

** SMART = Specific, Measurable, Attainable, Realistic and Timely.

	Management Oversight and gaps	Governance oversight and gaps	Independent assurance	Sufficient assurance Y/N	Action Plan Actions should be SMART (**) and include action owners and due dates
	<p>Regular review and update of policies and procedures</p> <p>Training logs</p> <p>Incident log</p> <p>Gap- no method of checking ongoing compliance with policies and procedures</p>	Gap – no formal reporting to trustees	None	No	<p>Management oversight:</p> <ol style="list-style-type: none"> 1. Review incident log and identify themes by 2. Provide additional training and support by 3. Carry out internal audit by..... <p>Governance oversight:</p> <ol style="list-style-type: none"> 1. Set up regular reporting on incidents and breaches to Board meetings by.....

Example of a current state assurance assessment dashboard for an organisation's data protection risk

Risk	Current risk score	Management oversight	Governance oversight	Independent assurance	Sufficient Assurance Yes/No	Overall Assurance
Risk 1. Data Protection regulations breach because our people are not following our agreed policies and procedures					No	
Risk 2						

Key:

Current risk score – RAG rating taken from your risk register. If your charity does not have a risk register, we recommend that you do have one - please see our guide on “Getting Started with Risk Management” for help.

Oversight/Assurance colour code:

Green = evidence exists that adequate oversight/assurance is in place for all controls

Amber = evidence exists that adequate oversight/assurance is in place for some of the controls

Red = there is no evidence that adequate oversight/assurance exists for any of the controls

Remember:

1. The overall assurance map provides a clear indicator of the effectiveness of controls for a specific risk, and compliance with those controls. If the assurance map shows red as there are no controls or existing controls are not effective, this should prompt a review of the risk itself.
2. The overall levels of assurance should be reported back to trustees
3. It should be clear who completes and updates the assurance map on a regular basis at the frequency agreed with the trustees. Consider who is best placed within your organisation to do this.

13. Key messages from this guide

This guide is a companion to our guide, [*An introduction to understanding and managing regulatory risk*](#).

An assurance map is a useful tool to set out a charity's sources of assurance for managing regulatory risk (and other types of risk) in the context in which a charity operates.

There are other tools for assurance mapping available online. The tool presented here is an example tested by the IRM Charities SIG members, and is shared to provide other charities with guidance on the topic.

A 'business compliance self-assessment' is a useful tool to gather evidence from first-line management of compliance with relevant legal and regulatory requirements. The checklist needs to be tailored to ensure it is proportionate to the size and needs of the charity. An example is presented in this guide.

The business compliance self-assessment and the assurance map tools seek to aid the charity to manage regulatory risks. The trustees representing the governing body of the charity are accountable for their charity's compliance with relevant legal and regulatory requirements. To do this they need assurance that relevant policies and procedures are fit for purpose and being followed. Clear, open, honest assessments of where compliance is adequate and planned improvements where it is not will enable a charity to meet or exceed stakeholders' expectations of behaviour, competence and performance.

We hope you find this guide of interest. Other publications available on our web page <https://www.theirm.org/events/special-interest-groups/charities/> includes:

[Getting Started with Risk Management](#)

[Risk Management for Charities: Getting Better](#)

[Risk Maturity Framework](#)

[Setting Risk Appetite](#)

[Risk Governance for Charities: Risk Management Structures](#)

[Accountabilities Stakeholder Mapping](#)

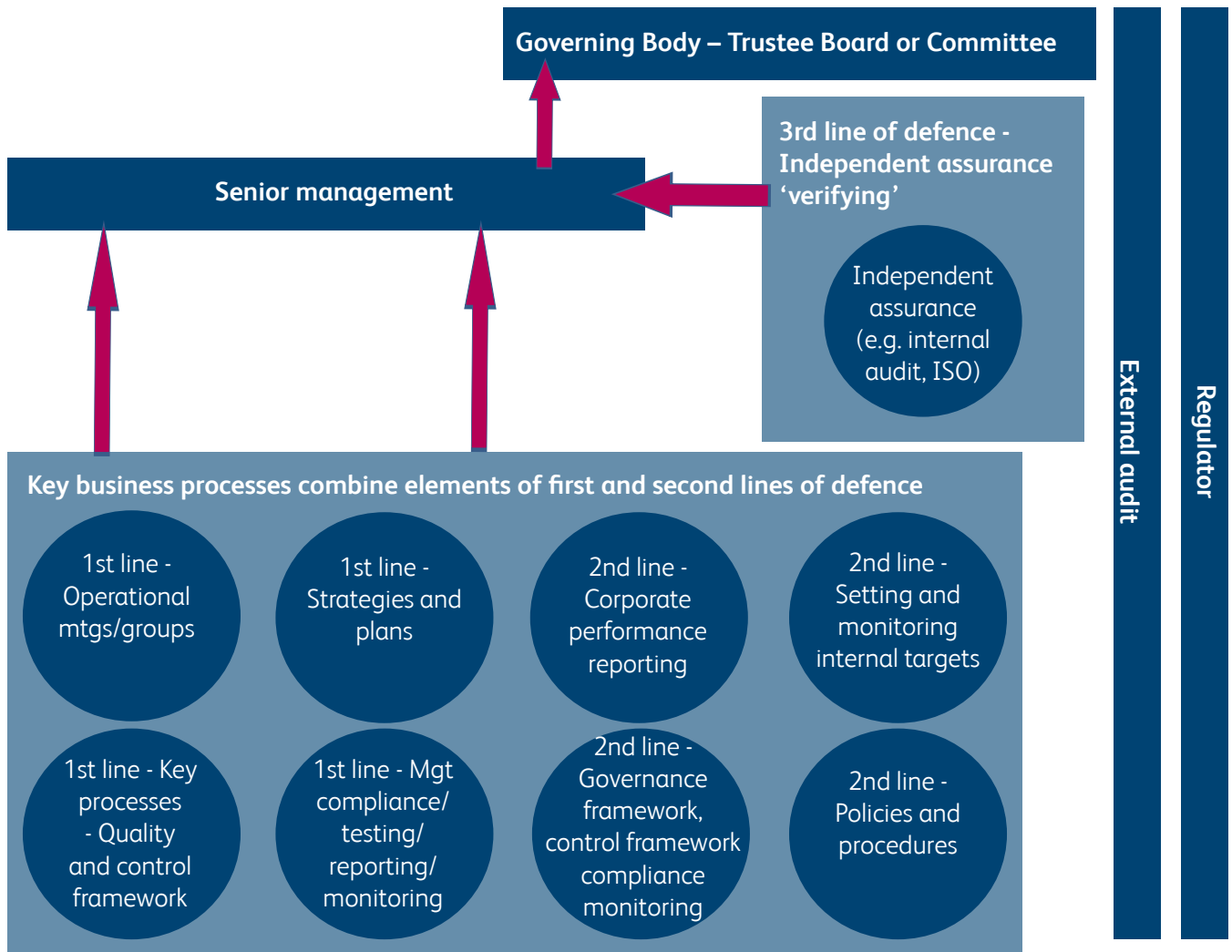
[An introduction to understanding and managing regulatory risk](#)

www.theirm.org/charities

Developing risk professionals

Annex 1: Three Lines of Defence - Compliance assurance models by charity size

Assurance model: Small charities



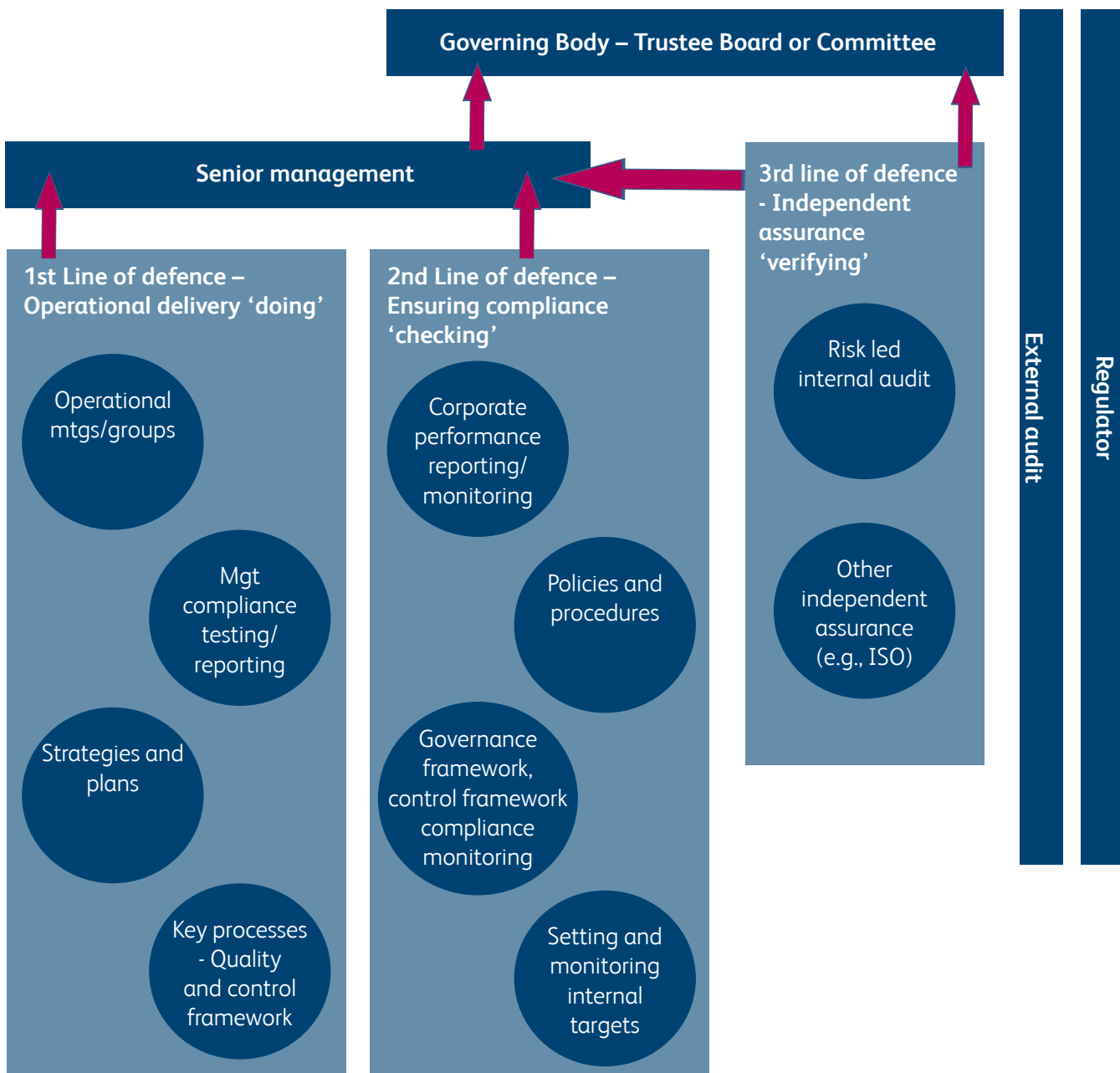
Charity size and Assurance features

Small sized charity (1) (2)

- Locally focused (including PTAs, village halls, scout groups, local leisure groups etc.)
- Small scope of activities
- Income is less than £100,000 (3)
- Income tends to come from individuals (approx. 70 %)
- Spend minimal amounts generating funds (approx. 8 % of income)
- Unlikely to have 3 months expenditure in reserves
- 90 % of spending is on grants and charitable activity
- Unlikely to have any internal audit provision
- Generally run by volunteers with limited staff resources
- Unlikely to have defined first and second line of defence activities

1. Micro charities may be considerably below this threshold and will require regulatory assurance arrangements that are proportionate while meeting the expectations of their stakeholders
2. Under Charity Commission Guidance ('Charity reporting and Accounting: The Essentials' (CC15b), section 1.4) some charities with annual income under £500k per annum are exempt from having their accounts externally audited, although they may still require an independent examination.
3. NCVO UK Civil Society Almanac 2016

Assurance model



Charity size and Assurance features

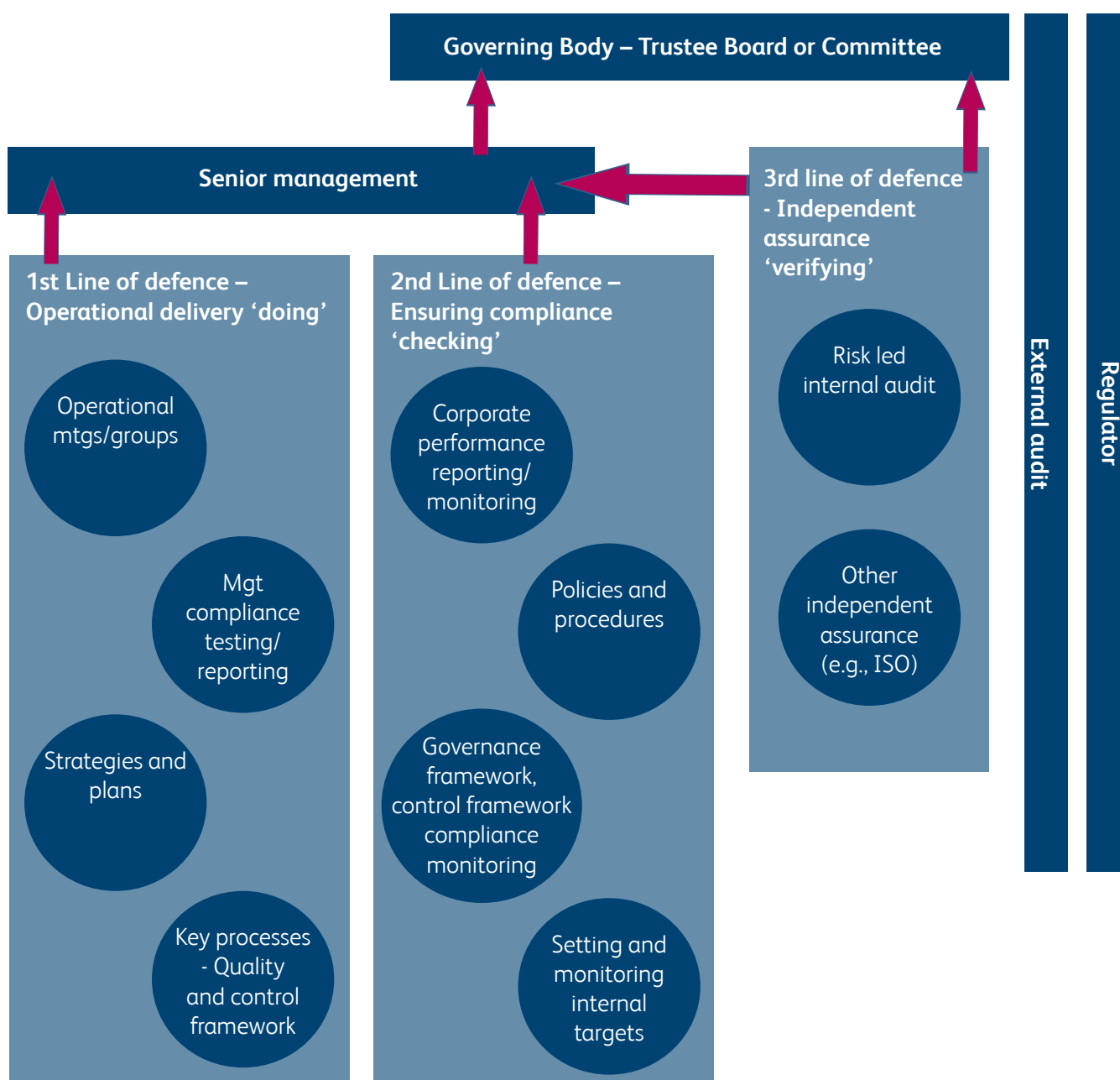
Medium sized charity

- Have a broader scope of activities (several services), may have national or international remit with some localised service delivery
- Income of £100,000 - £10 million (3)
- Spend around 12.5 % of income generating funds
- Generally, have sufficient reserves of at least 1-3 months of expenditure
- Key funding sources are individuals, local and national government funding, grants and trusts, national lottery
- Will have a paid workforce and volunteers

Depending on resource priorities:

- Third line internal audit provision may not be available or limited in scope
- Some activity(s) in first and second lines may be combined

Assurance model



Charity size and Assurance features

Large sized charity

- The majority of their activities are delivered at national or international level
- They will provide an number of services, have national a remit and may/do undertake international / overseas work
- Income of £10 million+ (3)
- Generally, have sufficient reserves of at least 1-3 months expenditures
- Spend around 12.5 % of income generating funds
- Key funding sources are generally split between individuals and local and national government funding
- Will have a significant paid workforce across a range of roles including a CEO
- Will have high numbers of volunteers and/or members
- To meet governance expectations of key stakeholders likely to have fully specified and defined three lines of defence in operation

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**



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

www.theirm.org

irm

Developing risk professionals