Institute of Risk Management

Risk governance for charities

Risk management structures and accountabilities

www.theirm.org/charities

About the Institute of Risk Management (IRM)

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.

Our authors and editors

This guidance has been produced by members of the IRM Charities Special Interest Group (SIG).

The main authors are:

- Roberta Beaton, Nursing and Midwifery Council
- Alyson Pepperill, CFIRM, Arthur J. Gallagher and SIG Chair

With editing undertaken by:

- Marilyn Acker, VSO
- Charles Mitchell, Cancer Research UK
- Sara Dzregah, British Red Cross

Peer Review by:

- Amanda Wade, CARE International UK
- Anita Punwani, CFIRM, Save the Children UK
- Fiona Davidge, CFIRM, Wellcome Trust
- Jason Baker, British Heart Foundation
- Katy Leppard Barry, Ambition School Leadership

Foreword

Welcome to our fourth guide designed to help charities make sense of risk management.

Risk management is often viewed as a complex discipline – but we beg to differ and are here to offer practical information to help you manage risk within your organisation.

Our Getting started leaflet and supplementary guidance demonstrated that risk management is something often undertaken intuitively, with a little structure this can be embedded into an organisation to help it achieve objectives, support successful strategic planning, and reassure people at all levels that uncertainty and risk are being considered and managed appropriately. Integrating risk management into strategic planning can also result in new and different opportunities being identified.

In this guidance we consider who needs to be involved to make risk management successful and where the boundaries of accountability and decision making are.

If you're looking for further guidance about risk management, please refer to our other publications:

- Getting started: How to set up risk management
- Getting better: Understanding your risk maturity
- Setting your risk appetite: Understanding your appetite for risk

Alyson Pepperill
Chair of IRM Charities SIG

Roberta Beaton
Member of IRM Charities SIG

Contents

Purpose and benefits

In an ever changing sector, charities need to ensure that any risks they take are calculated and will ultimately lead to the achievement of its aims.

Risk is inherent in everything we do, whether it be crossing the road, piloting a new service or making a million-pound investment. The amount of risk a charity will experience depends on a number of factors, including their size, nature and complexity of their services.

Managing risks effectively involves identifying, assessing and treating potential risks. By doing this work you can decide whether the risk can be tolerated, treated, transferred, or terminated.

By having a deeper understanding of potential risks, organisations may take calculated risks to achieve their objectives, maximise benefits and achieve financial stability.

At the heart of good risk management is people, how they make decisions about risks and how well they engage with the organisation's risk management strategy.

Purpose of this guide

Implementing a clear structure for decision making (risk governance) is crucial to successful risk management and requires the engagement and awareness of various layers of stakeholders across the organisation.

Although Trustees are ultimately accountable for managing risk (as designated by The Charity Commission, the charity sector regulator), they should be supported by the organisation to enable them to fulfil this role effectively.

In this guide we examine the structures charities can use to make effective risk decisions and present options for small, medium and large charities.

Done, properly effective risk management will lead to explicitly addressing uncertainty as part of decision making, as well as ensuring that any new or subsequent risks can be taken into account as they arise.

Benefits of effective risk management

Before we begin, here is a reminder of the benefits you can expect from good risk management practice:

1. **The entire organisation plays a role in risk management** resulting in risk being managed at all levels of the organisation.
2. **Risk management is transparent** with assurances built into processes.
3. **Leaders make informed decisions** and take timely action.
4. **Risk taking is calculated**, controlled and monitored.
5. **The probability of success is increased** and with the organisation more likely to achieve its aims.
6. **Opportunities often result from taking calculated risks**; these are identified and then maximised to achieve the greatest benefits.
7. **The organisation understands its appetite for risk** and the level of risk that is acceptable to take.
8. **Good risk management is a requirement** of SORP (Statement of Recommended Practice) which needs to be detailed in a charities annual report and accounts.

When implementing risk management structures a charity will need to consider the prevailing culture and behaviours within the organisation and whether or not they are conducive to the proposed risk governance.

Culture and trust are areas that should flow from the Trustees downwards. It is very important to engender an atmosphere that empowers people to highlight uncertainty and raise risks as and when they observe them.

A positive risk management culture will ensure that risks are not considered in silos, that people feel empowered to raise risks, and that risk is not just delegated to the risk professionals (if any) to manage. Good risk management governance is one component of the charity’s overall governance structures.

Why implement a decision making culture that supports risk management?

It ensures that:

- Risk is owned and reviewed at all levels of organisation and becomes embedded into day-to-day management
- Decisions are taken by most appropriate team/person, meaning that specific risks can be delegated and managed at the appropriate level
- In larger organisations, the Board of Trustees should be focused on strategic risks or risks with the most exposure, rather than dealing with every potential risk faced
- Risk assurance is provided by multiple people and is built into the structure
- Risk management is not a separate activity to planning, monitoring and day-to-day management

Definitions	
What is a risk?	A risk is something uncertain – it might happen or it might not. A risk matters because (if it happens) it will have an impact on the delivery of your objectives.
What is risk management?	Any activity taken to identify and then control the level of risk your objectives may be exposed to.
What are issues?	Risks and issues are often mentioned in the same breath. An issue is an unplanned event that has already happened and needs immediate action to manage it.
Why manage risks?	Because managing risks effectively helps organisations achieve their objectives more successfully and helps protect their funds and assets.
What is risk governance?	Risk governance refers to the roles and responsibilities an organisation puts in place to make decisions about risk and take action. This includes both the people and processes.
What is the difference between risk management and risk governance?	Governance provides active direction, control and leadership. Management coordinates activities to direct and control an organisation's risks.
What are strategic risks?	These are risks that could affect or influence the delivery of your strategic aims and where the impact would be felt organisation-wide.
What are operational risks?	These are typically internal risks which are predictable and relate to day to day management. Examples include health & safety issues, compliance and regulatory risks. These are risks that can be controlled through the deployment of policies and procedures.

Definitions	
What is project / programme risk?	These are risks related to a discrete activity that may have temporary or longer lasting consequences beyond the life of the project/programme.
What is 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 but is not limited to: Charity Commission, Fundraising Regulator, Information Commissioner's Office, Care Quality Commission, Ofsted, Financial Conduct Authority.
Senior Management Team	Within this guidance we use a couple of terms that also need clarification: The term '**Senior Management Team**' is used throughout but different charities may use different terms such as 'Executive Leadership Team', 'Senior Leadership Team' 'Strategic Leadership Team' etc. In all instances we are referring to the highest level of decision making officers within the charity. Smaller organisations may just use the term 'Management' or 'Management Team'.
Internal Risk Team	The term '**Internal Risk Team**' is used to distinguish the people or person within the organisation that provides risk management expertise and best practice. They provide day-to-day risk management support, advice, education and training. In addition they provide a challenge to the business units who implement risk management.

Roles and responsibilities when managing risk

Decision making about risk needs support from the Trustees who are accountable for managing risk. As such any structure your charity puts in place needs to be proportionate to the size of charity and the level of risk being taken.

Potential risks need to be understood by senior decision makers and factored into delivery plans and financial budgets to ensure action will be taken. The charity will also require clear guidance about the process people should use to escalate concerns for decision and action.

This is where clear roles and responsibilities can assist a charity to successfully manage their risks.

Types of roles

Board of Trustees		
Overview	**Focus**	**Comments**
As designated by the charity regulator (The Charity Commission), the Board of Trustees has the ultimate accountability for managing and controlling risk within a charity. For example, when a risk of a serious incident occurs (e.g. poor governance leading to the failure of the charity, or a serious breach of health and safety) it will be the Trustees that will be required to explain what happened to the Charity Commission/Select Committee.	They approve and oversee: > The setting of risk appetite and tolerance levels (i.e. the level of risk the organisation is willing to take) > The setting of risk policies (and in some organisations also procedures) > Identification and monitoring of potential risks that could affect the successful achievement of the charity's strategy and aims > Regular review of the risk management action plan/ register	Within a small charity it is likely that the Trustees will be responsible for managing and monitoring risks as well as having overall accountability. In medium and larger sized charities the Trustees may delegate authority for detailed risk management to sub-committees or directly to the Senior Management Team. This enables the trustees to retain their focus on other aspects of strategic leadership.

Senior Management Team

Overview	Focus	Comments
The Senior Management Team have delegated authority from the Trustees to provide day-to-day risk management on the behalf of the Board. Their role is to develop and recommend the organisation's risk management strategy, ensure that appropriate risk management processes are in place and deal with major organisational risks.	They approve and oversee: > The setting of the charity's risk appetite and tolerance levels > The setting of the charity's risk policies and procedures > Identification and monitoring of potential risks that could affect the successful achievement of the charity's strategy and aims > Taking action when significant risks arise both those identified by them and those escalated to them by others > Undertaking regular review of the risk management action plan and risk register Specific tasks include: > Assessing risks for likelihood and level of impact > Identifying risk owners from within the charity > Consideration of analysis, data and insights about risk > Providing reports to the Audit and Risk Committee and the Trustees	Depending on the size of the charity they may or may not have a Senior Management Team; where one doesn't exist authority remains with the Trustees. In very large charities the Senior Management Team may be supported by additional internal resources such as internal risk committee or internal risk team.

Audit and Risk Committee

Overview	Focus	Comments
The Audit and Risk Committee is a sub-committee of the Board of Trustees. They assure that the charity's internal controls are effective, this includes financial oversight, risk management, compliance with statutory/regulatory frameworks and internal audit (where applicable). They do not make decisions about risk management, but provide challenge and assurance to Trustees to support their role.	They provide assurance of: > Whether the charity abides by their risk policies and procedures > Whether the charity operates within subscribed regulatory frameworks > Scheduling, reviewing and monitoring internal audits	Smaller charities may have a different approach to independent assurance such as an independent review board or a single independent reviewer. It is important to ensure the charity has some independent assurance of how they manage risk, whether this is a sub-committee or a single independent assurer.

Internal Risk Team

Overview	Focus	Comments
The Internal Risk Team is an independent function that supports the Senior Management Team and wider charity with risk management expertise, support and best practice. The Internal Risk Team are not accountable for managing risk, this remains with the Trustees.	Their role may include: > Developing risk management policy > Escalating breaches of compliance or risk incidents to senior management > Developing risk metrics (measures) to track and analyse specific risks > Embedding risk into strategic and operational planning > Being a focal point of best practice and risk expertise > Providing of risk management education to the organisation	An Internal Risk Team is typically found in larger and more complex charities where resources are more readily available. In smaller charities this may be allocated to just one person. In very small charities this may fulfilled by seeking external advice or assurance.

Internal Risk Committee

Overview	Focus	Comments
In larger charities the Senior Management Team may be supported by an Internal Risk Committee who provide in depth oversight of risk management. The Committee reviews the progress against the risk management action plan and recommends further actions to the Senior Management Team. The Committee is not responsible for the delivery of risk actions.	Their role may include: > Regularly reviewing the risk register and progress against the risk action plan > Recommending options for management response and mitigations > Escalating risk management issues to the Senior Management Team > Delegating risk management actions to business units > Managing conflicts about risk ownership from within the charity > Undertaking risk monitoring and providing analysis to the Senior Management Team	The Internal Risk Committee typically includes leaders from across the charity who provide a broad spectrum of organisational knowledge and experience.

Directorate Leads

Overview	Focus	Comments
Directorate Leads (for example, the Director of Finance, Fundraising Director, HR Director etc.) are responsible for managing and monitoring risks across the business units assigned to them. Typically, Directorate Leads are found in larger charities that provide a number of diverse services and will manage a number of business units.	They operationalise the following for their business area: > Risk appetite and tolerance levels set by the Trustees > Owning and managing key organisational risks or implementing risk management actions > Implementing risk policies and procedures > Managing risks delegated from the senior leadership team Specific tasks include: > Identifying significant risks for their directorate > Preparing a directorate register and risk action plan > Escalating risk management issues to Senior Management Team (or risk committee or Trustees) when risks go beyond their remit or control > Ensuring that regular risk monitoring and risk analysis is undertaken and reviewed > Delegating risk management actions to business units	Directorate Leads can also be part of the Senior Management Team but there is a distinction in their role: > The Senior Management Team's focus is delegated responsibility for organisation wide risk management and they report directly into the Trustees. > At Directorate level, their responsibility is managing risks that affect the business units assigned to them. In this instance they report into the Senior Management Team.

Business Unit Leads

Overview	Focus	Comments
Similar to Directorate Leads, Business Unit Leads have responsibility for managing and monitoring risks within their service area. Business unit leads need to be mindful that if a risk materialises and they fail to escalate or manage the risk, they may be held accountable internally.	They operationalise the following for their business unit: > The risk appetite and tolerance levels set by the Directorate (or Senior Management Team or Trustees in small charities) > Owning key or organisational risks and implementing risk management actions > Implementing risk policies and procedures for their area of responsibility > Managing risks delegated from the Directorate (or Senior Management Team or Trustees in small charities) Specific tasks include: > Identifying significant risks for their Business Unit > Preparing a Business Unit register and risk action plan > Escalating risk management issues to the Directorate management team (or Senior Management Team or Trustees in small charities) when risks become outside the business units ability to control them > Ensuring that regular risk monitoring and risk analysis is undertaken and reviewed	In small charities Business Units may be a single service lead who is responsible for managing risks within their service delivery area.

Individual Employees and Volunteers

Overview	Focus	Comments
Everyone involved in delivering a charity's services has a responsibility to identify any risks associated with delivering their work and to escalate these to their manager or supervisor. This is done so that the charity can take any necessary and appropriate action.	Their role is: > Identifying risks within their work > Escalating risks that they observe > Implementing risk management actions where an action has been assigned	One of the most effective ways to create this level of engagement is to ensure that job descriptions and evaluation processes incorporate references to risk identification, escalation and where required implementation.

Internal Audit

Overview	Focus	Comments
Internal Audit provides independent assurance of risk management effectiveness by providing challenge and undertaking risk identification exercises. This may include confirming that policies and procedures are implemented satisfactorily and identifying the prevailing risk culture. Internal Audit can also provide commentary around how to integrate risk governance and processes within the organisation, and how to undertake risk management analysis to get a deeper understanding of specific topics.	They may provide assurance of: > Whether the charity abides by their risk policies and procedures > Whether the charity operates within subscribed regulatory frameworks > What level of risk maturity the charity operates at, and how well the risk culture has been embedded > Whether a specific risk event or failure was dealt with effectively > What the financial or reputational impact on the charity is likely to be > Key lessons learnt and undertake analysis to get a deeper understanding of the risk	Often this is not applicable in small to medium charities and can be provided by an independent reviewer. Many charities outsource Internal Audit to an external supplier for increased independent assurance. Some charities retain an internal audit function who provide quality assurance of internal policies and procedures. Your charity should pick a model that is suitable for its needs.

External Audit

Overview	Focus	Comments
External Audit provides independent assurance and is employed by the Trustees or the Audit and Risk Committee. Typically they focus on risk management effectiveness by providing challenges and undertaking risk identification exercises to provide an external review. Usually, they concentrate on financial aspects of risk management rather than culture, and are often employed when a major risk event or change has occurred.	They may provide assurance of: > Whether the charity abides by their risk policies and procedures > Whether the charity operates within subscribed regulatory frameworks > Whether a specific risk event or incident has been dealt with effectively > What the financial or reputational impact on the charity is likely to be > Consider key lessons learned	Often this is not applicable in small to medium charities where independent assurance or internal audit is used. The roles of External Audit and Internal Audit have many similarities; where charities outsource their audit services, their supplier usually provides a single audit service covering both internal and external auditing.

Escalating risks for management attention

Successful risk management is dependent on clearly stating what the charity's level of tolerance is for risk and setting out the routes for risks to be escalated. Risks generally should be escalated when they fall beyond the remit of the role of the person or group.

The IRM Charities SIG's "Setting your risk appetite" supplementary guide refers to the escalation and delegation of risks as being an important part of enabling or empowering people or groups within an organisation to do their job within the boundaries set by the organisation.

It is the decision-making and risk control that helps the person or group to understand to whom the risk should be escalated. For example, if the Business Unit Leader identifies a risk that is beyond their remit or a risk where they feel they are unable to control it within acceptable appetite levels, then they would escalate this to the Director of the Unit or the Senior Leadership/Management team. It is then for that group to consider whether they are able to manage the risk successfully within the appetite set by the Board or whether it requires further escalation.

Tailoring risk governance to your organisation

Risk roles and responsibilities tailoring guide

The appendix provides an overview of potential roles and responsibilities that your organisation may like to consider implementing.

This is a suggested approach based on good practice which may need to be tailored to suit your charity's current governance arrangements and risk culture.

The appendix is split into 'small', 'medium' and 'large' charities and presents:

- Common characteristics for the size of charity
- Tailoring options stating 'required', 'recommended' and 'optional' governance structures
- Diagram view of the structure

Where to find more information

The IRM has a wide range of information available free of charge. You can also sign up for webinars to hear live discussions about a range of risk topics. If you join the IRM you can gain access an even wider range of resources.

Please find some resources listed below:

- Section 3 of the Charities & Risk Management CC26 publication by the Charity Commission briefly reviews governance
- Find out more about the Charities Special Interest Group and our previous risk management publications for charities on the IRM website
- If you have any concerns about how to get started with risk management please read our Getting Started guide and listen to the short presentations on each step of that process

More generally on the topic of governance:

- The Charity Commission document: Charity governance, finance and resilience: 15 questions trustees should ask
- The Code for Good Governance for the Voluntary Sector

Appendix: Risk governance for charities

Small charities

A. Characteristics of a small charity

- Locally focused (including PTAs, village halls, scout groups, local leisure groups etc.)
- Small scope of activities
- Income is less than £100,000[1]
- Income tends to come from individuals (approx.70%)
- Spend minimal amounts generating funds (approx. 8% of income)
- Least likely to have 3 months expenditures in reserves
- 90% of spending is on grants and charitable activities
- Generally, run by volunteers with limited staff resources

B. Tailoring options

1. Required (minimum level assurance):

Role	Summary of the role
Board of Trustees	As designated by The Charity Commission (the charity regulator), Trustees are accountable for organisation wide risk management across the charity and are the highest level of decision makers. They are ultimately accountable for risk incidents and in their role, they approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Managing and reviewing the risk management action plan and risk register > Taking action when risks are escalated to them
Individual Employees and Volunteers	Everyone involved in delivering a charity's services has a responsibility to identify any risks associated with delivering their work. They are to escalate these risks to their manager or supervisor so that the organisation can take appropriate action. Their role is to: > Identify risks within their work > Escalate risks that they observe > Implement risk management actions where an action has been assigned

[1] NCVO UK Civil Society Almanac 2016

2. Recommended (good practice):

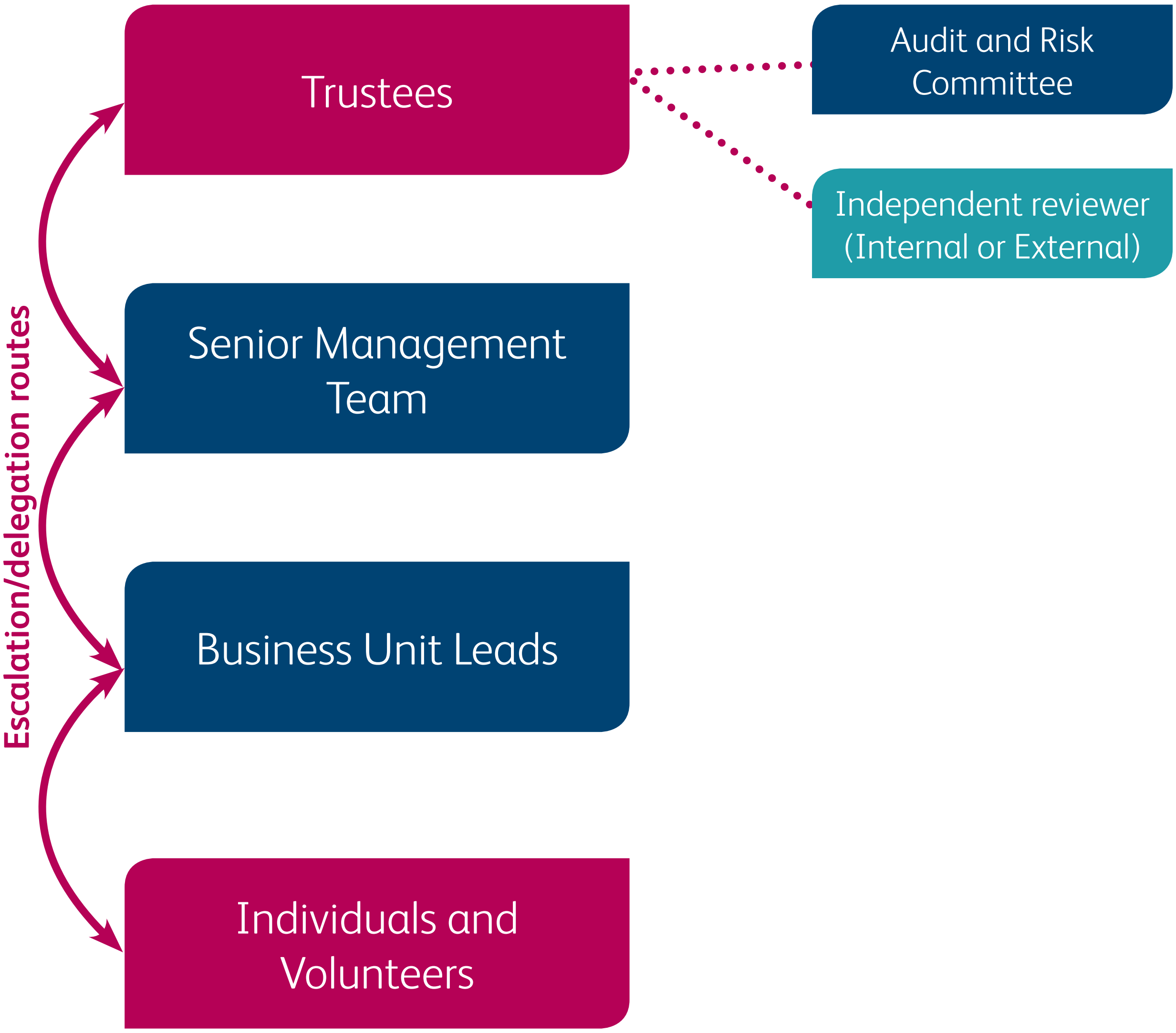
Role	Summary of the role
Senior Management Team ***(Aka. Executive Board, Senior Leadership Team etc.)***	The Senior Management Team have delegated responsibility from the Trustees to make decisions about day to day risk management for the charity. They are the second highest level of decision making in a charity and support the Trustees to fulfil their risk obligations. They develop and recommend the Charity's risk management strategy and are responsible for risk failures and reporting the Trustees. In their role they approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Regular review of the risk management action plan and register > Responding to significant risks (those escalated to them or identified by them) They also provide risk management reports to the Trustees.
Business Unit Leads ***(Aka. Service leads / function leads)***	Similar to Directorate Leads, Business Unit have responsibility for managing and monitoring risks within their service area. They receive and operationalise the following for their business area: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Risks delegated from the Senior Management Team Their role is to: > Identify significant risks for their business unit > To prepare and review the Business Unit risk management action plan and risk register > Ensure that risk monitoring and analysis takes place and is reviewed regularly > Recommend options to Directorate Leads for risk mitigation for their business area > Escalate risk issues to Directorate Lead > Manages escalated risks from within their business unit > Delegate risk management actions to relevant employees within the business unit

Role	Summary of the role
Independent Reviewer **(or Internal Audit or External Audit)**	Their role is to provide independent assurance of risk management effectiveness by providing challenge and undertaking risk identification exercises. This may include confirming that policies and procedures are implemented satisfactorily. They may provide assurance of: > Adherence to risk policies and procedures > Adherence to subscribed regulatory frameworks A small charity may choose to hire an outsourced Internal or External Auditor if an independent reviewer isn't available internally.

3. Optional:

Role	Summary of the role
Audit and Risk Committee	The Audit and Risk Committee is a sub-committee of the Board of Trustees. They assure that the Charity's internal controls are effective, this includes financial oversight, risk management, compliance with statutory frameworks and internal audit. They do not make decisions about risk management but provide challenge and assurance to the Trustees to support Trustee oversight. In their role they assure: > Adherence to policies > Adherence to regulatory frameworks > And schedule, review and monitor internal audits

C. Diagram of the model (small charities)


Trustees
Audit and Risk Committee
Independent reviewer (Internal or External)
Senior Management Team
Business Unit Leads
Individuals and Volunteers
Escalation/delegation routes

Key

- Required
- Recommended
- Optional

Medium charities

A. Characteristics of a medium charity

- Have a broader scope of activities (several services), may have national remit with some localised service delivery or all three
- Income of £100,000 - £10 million[2]
- 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

B. Tailoring options

1. Required (minimum level assurance):

Role	Summary of the role
Board of Trustees	As designated by The Charity Commission (the charity regulator), Trustees are accountable for organisation wide risk management across the charity and are the highest level of decision makers. They are ultimately accountable for risk failures and in their role, approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Managing and reviewing the risk management action plan and risk register > Taking action when risks are escalated to them Usually they delegate risk management responsibility to Senior Management Team and Audit and Risk Committee but still have a key role to provide oversight.
Senior Management Team ***(Aka. Executive Board, Senior Leadership Team)***	The Senior Management Team have delegated responsibility from the Trustees to make decisions about day to day risk management for the charity. They are the second highest level of decision making in a charity and support the Trustees to fulfil their risk obligations. They develop and recommend the charity's risk management strategy and are responsible for the implementation of effective risk management action plans and reporting to the Trustees.

[2] NCVO UK Civil Society Almanac 2016

Role	Summary of the role
Senior Management Team (cont.)	In their role they approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Regular review of the risk management action plan and register > Responding to significant risks (those escalated to them or identified by them) The Senior Management Team delegate specific aspects of risk management to the next level of management (e.g. Directorate Leads or Business Unit Leads) so that they can operationalise the risk management strategy and risk action plan across the charity. They are typically supported by an internal risk team and sometimes an internal risk committee in large charities. They provide risk management reports to the Trustees and Audit and Risk Committee and support Internal and External Audit to fulfil their role.
Business Unit Leads ***(Aka. Service leads / function leads)***	Similar to Directorate Leads, Business Unit have responsibility for managing and monitoring risks within their service area. They receive and operationalise the following for their business area: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Risks delegated from the Senior Management Team Their role is to: > Identify significant risks for their business unit > To prepare and review the business unit risk management action plan and risk register > Ensure that risk monitoring and analysis takes place and is reviewed regularly > Recommend options to Directorate Leads for risk mitigation for their business area > Escalate risk issues to Directorate Lead > Manage escalated risks from within their Business Unit > Delegate risk management actions to relevant employees within the Business Unit

Role	Summary of the role
Individual Employees and Volunteers	Everyone involved in delivering a charity's services has a responsibility to identify any risks associated with delivering their work and to escalate these risks to their manager or supervisor so that the organisation can take appropriate action. Their role is to: > Identify risks within their work > Escalate risks that they observe > Implement risk management actions where an action has been assigned

2. Recommended (good practice):

Role	Summary of the role
Audit and Risk Committee	The Audit and Risk Committee is a sub-committee of the Board of Trustees. They assure that the Charity's internal controls are effective, this includes financial oversight, risk management, compliance with statutory frameworks and internal audit. They do not make decisions about risk management but provide challenge and assurance to the Trustees to support Trustee oversight. In their role they assure: > Adherence to policies > Adherence to regulatory frameworks > And schedule, review and monitor internal audits
Directorate leads ***(Aka. Divisional leads, operational leads)***	Directorate Leads (for example, the Director of Finance, Fundraising Director, HR Director etc.) are responsible for running and making day to day decision about area of the charity they manage. They will typically have several Business Units they are responsible for. They receive and operationalise the following for their business area: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Risks delegated from the Senior Management Team

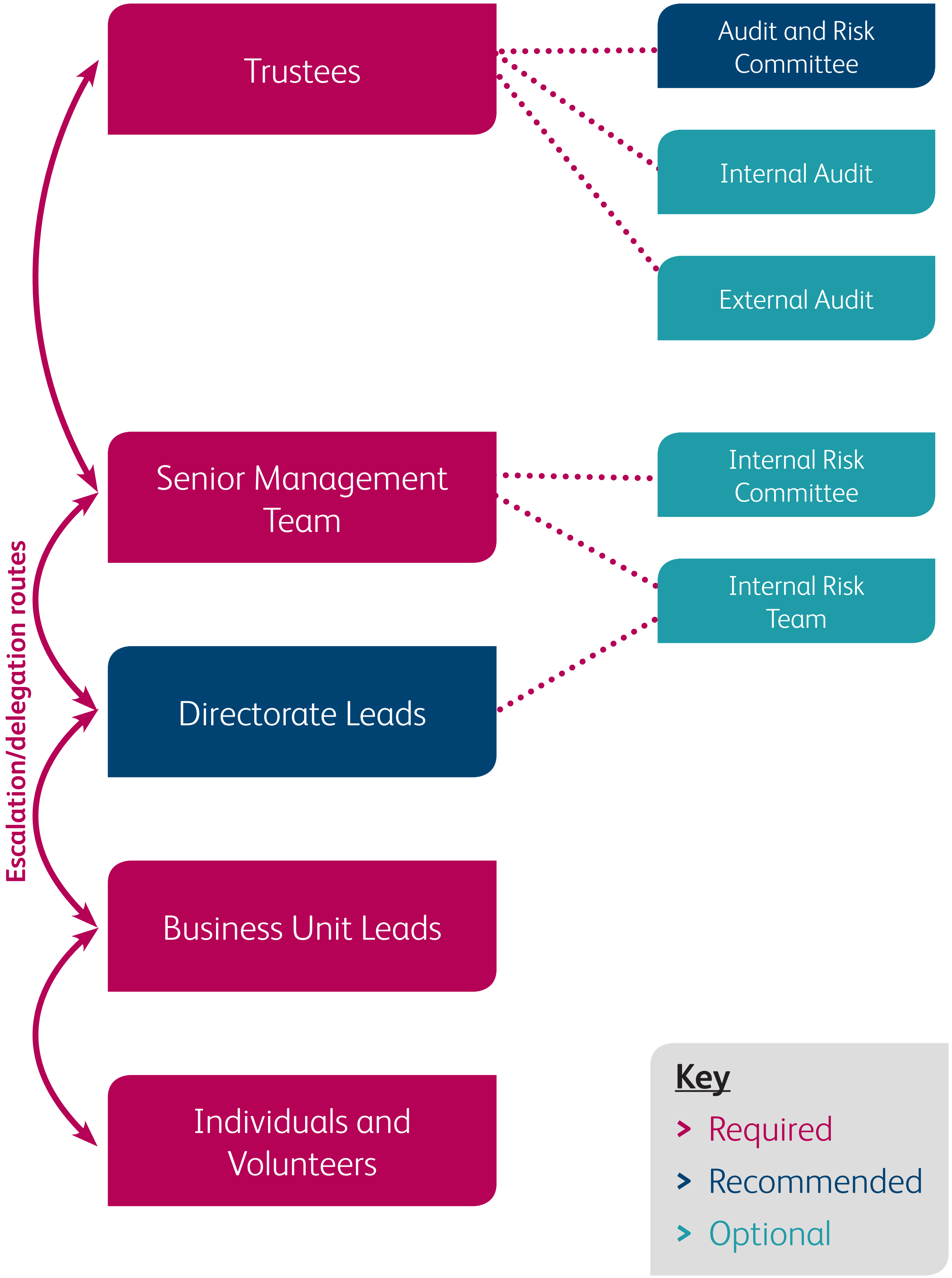
Role	Summary of the role
Directorate leads (cont.)	In their role they assure: > Identify significant risks for their directorate or division > To prepare and review the directorate risk management action plan and risk register > Ensure that risk monitoring and analysis takes place for their directorate and is reviewed regularly > Recommend options to Senior Management Team for risk mitigation in their business area > Escalate risk issues to Senior Management Team (or risk committee) > Manage risks escalated from business units > Delegate risk management actions to business units > Provide reports for senior leadership
Internal Audit	Internal Audit provides independent assurance of risk management effectiveness by providing challenge and undertaking risk identification exercises. This may include confirming that policies and procedures are implemented satisfactorily and identifying the pervading risk culture. Internal Audit can also provide commentary around how to integrate risk governance and processes within the organisation and undertake risk management analysis to gain a deeper understanding on specific topics. They may provide assurance of: > Adherence to risk policies and procedures > Adherence to subscribed regulatory frameworks > Identification of the risk maturity the charity operates at, and how well the risk culture has been embedded > Whether a specific risk event or failure was dealt with effectively > What the financial or reputational impact on the charity is likely to be > Consider key lessons learnt and undertake analysis

3. Optional:

Role	Summary of the role
Internal Risk Team	The Internal Risk Team is an independent function that supports the Senior Management Team and wider charity with risk management expertise, support and best practice. The Internal Risk Team are not accountable for managing risk, this remains with the Trustees. Instead they provide risk management expertise, support and advice on best practice to the Senior Management Team and wider organisation. Their role may include: > Development of risk management policy > Escalation of breaches of compliance or risk incidents to senior management > Development of risk metrics (measures) to track and analyse specific risks > Embedding risk into strategic and operational planning > Being a focal point of best practice and risk expertise > Provision of risk management education to the organisation In medium sized charities this might be allocated to just one person.
Internal Risk Committee ***(Made up of senior leaders and operational leads. This could include trustees and risk officers)***	In larger charities the Senior Leadership Team may be supported by an Internal Risk Committee who provide in depth oversight of organisational risk management. The Committee reviews the progress against risk management action plan and recommends further actions to the Senior Management Team. They do not make decisions about risk and are not responsible for the delivery of risk management actions. Their role may include: > Regularly reviewing the charity's risk register and the progress against the risk action plan > Recommending options for management response and mitigations > Escalating risk management issues to the Senior Management Team > Delegating risk management actions to business units > Managing conflicts about risk ownership from within the charity > Undertaking risk monitoring and providing analysis to the Senior Management Team

Role	Summary of the role
External Audit	External Audit provide independent assurance and are employed by the Trustees or Audit and Risk Committee and will focus on risk management effectiveness by providing challenge and undertaking risk identification exercises. Their role is similar to that of Internal Audit but they usually concentrate on financial aspects of risk management rather than culture and are often employed when a major risk event or change has occurred. They may: > Assure adherence to risk policies and procedures > Assure adherence to subscribed regulatory frameworks > Identify the risk maturity the charity operates at, and how well the risk culture has been embedded > Assess whether a specific risk event or failure was dealt with effectively > What the financial or reputational impact on the charity is likely to be > Consider key lessons learnt and undertake analysis.

C. Diagram of the model (medium charities)



Large charities

A. Characteristics of a large charity

- The majority of their activities are delivered at national or international level
- They will provide a number of services, have a national remit and undertake some international/overseas work
- Income of £10 million+[3] (NCVO methodology definition of major)
- 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 including a CEO
- Will have high numbers of volunteers and/or members

B. Tailoring options

1. Required (minimum level assurance):

Role	Summary of the role
Board of Trustees	The Senior Management Team have delegated responsibility from the Trustees to make decisions as designated by The Charity Commission (the charity regulator), Trustees are accountable for organisation wide risk management across the charity and are the highest level of decision makers. They are ultimately accountable for risk incidents and in their role, approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Managing and reviewing the risk management action plan and risk register > Taking action when risks are escalated to them

[3] NCVO UK Civil Society Almanac 2016

Role	Summary of the role
Audit and Risk Committee	The Audit and Risk Committee is a sub-committee of the Board of Trustees. They assure that the Charity's internal controls are effective, this includes financial oversight, risk management, compliance with statutory frameworks and internal audit. They do not make decisions about risk management but provide challenge and assurance to the Trustees to support Trustee oversight. In their role they assure: > Adherence to policies > Adherence to regulatory frameworks > And schedule, review and monitor internal audits
Senior Management Team ***(Aka. Executive Board, Senior Leadership Team)***	The Senior Management Team have delegated responsibility from the Trustees to make decisions about day to day risk management. They are the second highest level of decision making in a charity and support the Trustees to fulfil their risk obligations. They develop and recommend the Charity's risk management strategy and are responsible for the implementation of effective risk management action plans and reporting the Trustees. In their role they approve and oversee: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Regular review of the risk management action plan and register > Responding to significant risks (those escalated to them or identified by them) They delegate specific aspects of risk management to the next level of management (e.g. Directorate Leads or Business Unit Leads) so that they can operationalise the risk management strategy and risk action plan across the charity. The Senior Management Team are typically supported by an internal risk team and sometimes an internal risk committee in large charities. They provide risk management reports to the Trustees and Audit and Risk Committee and support Internal and External Audit to fulfil their role.

Role	Summary of the role
Directorate leads ***(Aka. Divisional leads, operational leads)***	Directorate Leads (for example, the Director of Finance, Fundraising Director, HR Director etc) are responsible for running and making day to day decisions about area of the charity they manage. They will typically have several Business Units they are responsible for. They receive and operationalise the following for their business area: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Risks delegated from the Senior Management Team Their role is to: > Identify significant risks for their directorate or division > To prepare and review the directorate risk management action plan and risk register > Ensure that risk monitoring and analysis takes place for their directorate and is reviewed regularly > Recommend options to Senior Management Team for risk mitigation in their business area > Escalate risk issues to Senior Management Team (or risk committee) > Manages risks escalated from business units > Delegate risk management actions to business units > Provide reports for senior leadership
Business Unit Leads ***(Aka. Service leads / function leads)***	Similar to Directorate Leads, Business Unit have responsibility for managing and monitoring risks within their service area. They receive and operationalise the following for their business area: > Risk appetite and tolerance levels > Risk policies and procedures > Key risks to delivering the charity's strategy and aims > Risks delegated from the Senior Management Team

Role	Summary of the role
Business Unit Leads (cont.)	Their role is to: > Identify significant risks for their business unit > To prepare and review the Business Unit risk management action plan and risk register > Ensure that risk monitoring and analysis takes place and is reviewed regularly > Recommend options to Directorate Leads for risk mitigation for their business area > Escalate risk issues to Directorate Lead > Manages escalated risks from within their business unit > Delegate risk management actions to relevant employees within the business unit
Individual Employees and Volunteers	Everyone involved in delivering a charity's services has a responsibility to identify any risks associated with delivering their work and to escalate these risks to their manager or supervisor so that the organisation can take appropriate action. Their role is to: > Identify risks within their work > Escalate risks that they observe > Implement risk management actions where an action has been assigned
Internal Audit	Internal Audit provides independent assurance of risk management effectiveness by providing challenge and undertaking risk identification exercises. This may include confirming that policies and procedures are implemented and identifying the pervading risk culture. Internal Audit can also provide commentary around how to integrate risk governance and processes within the organisation and undertake risk management analysis to gain a deeper understanding on specific topics They may provide assurance of: > Adherence to risk policies and procedures > Adherence to subscribed regulatory frameworks > Identification of the risk maturity the charity operates at, and how well the risk culture has been embedded > Whether a specific risk event was dealt with effectively and what the financial or reputational impact on the charity is > Consider key lessons learnt and undertake analysis

2. Recommended (good practice):

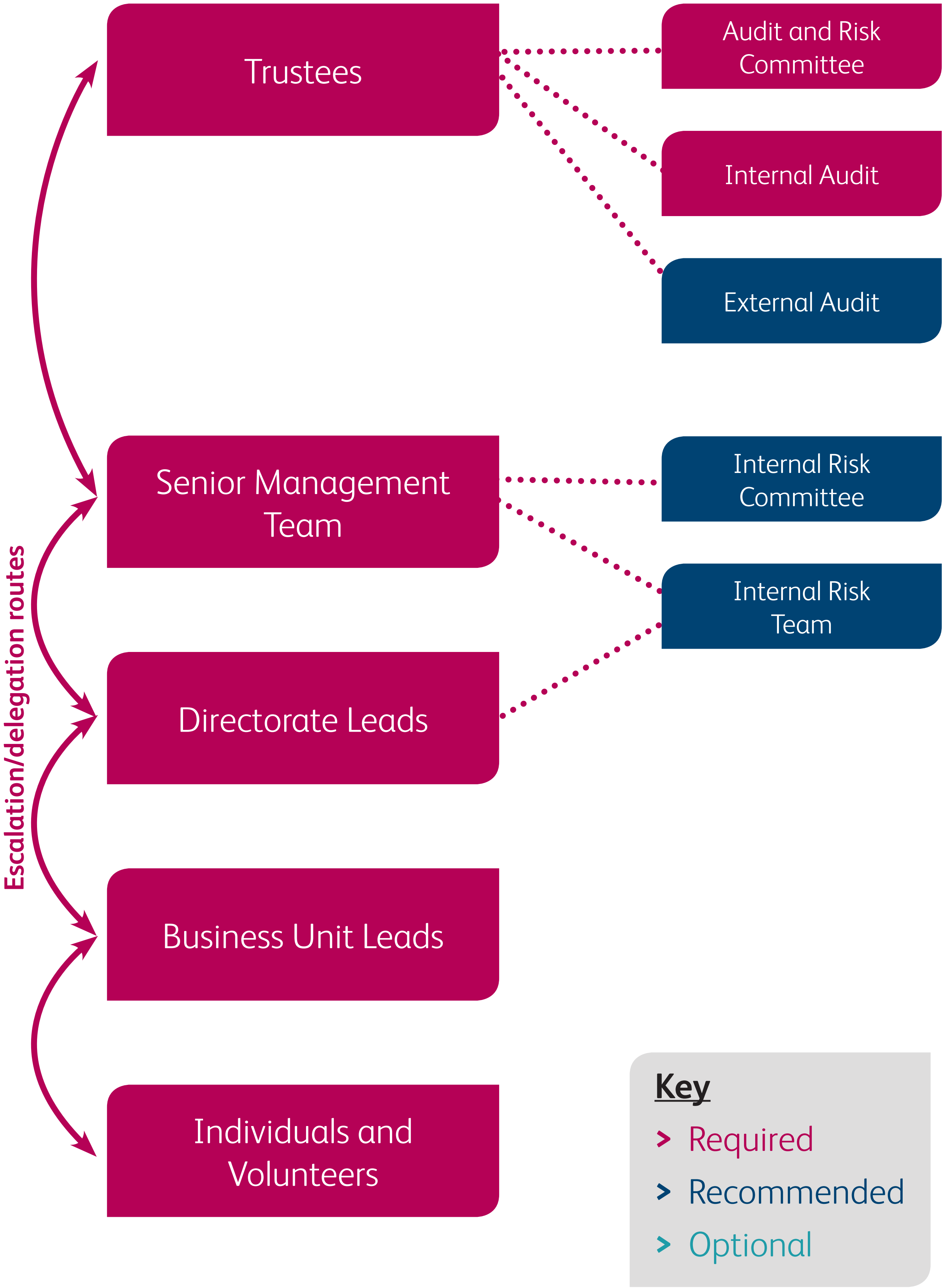
Role	Summary of the role
Internal Risk Team	The Internal Risk Team is an independent function that supports the Senior Management Team and wider charity with risk management expertise, support and best practice. The Internal Risk Team is not accountable for managing risk, this remains with the Trustees. Their role may include: > Development of risk management policy > Escalation of breaches of compliance or risk incidents to senior management > Development of risk metrics (measures) to track and analyse specific risks > Embedding risk into strategic and operational planning > Being a focal point of best practice and risk expertise > Provision of risk management education to the organisation
Internal Risk Committee ***(Made up of senior leaders and operational leads. This could include trustees and risk officers)***	In larger charities the Senior Management Team may be supported by an Internal Risk Committee who provide in depth oversight of organisational risk management. The Committee reviews the progress against risk management action plan and recommends further actions to the Senior Management Team. They do not make decisions about risk and are not responsible for the delivery of risk management actions. Their role may include: > Regularly reviewing the charity's risk register and the progress against the risk action plan > Recommending options for management response and mitigations > Escalating risk management issues to the Senior Management Team > Delegating risk management actions to business units > Managing conflicts about risk ownership from within the charity > Undertaking risk monitoring and providing analysis to the Senior Management Team

Role	Summary of the role
External Audit	External Audit provides independent assurance and are employed by the Trustees or Audit and Risk Committee and will focus on risk management effectiveness by providing challenge and undertaking risk identification exercises. Their role is similar to that of Internal Audit but they usually concentrate on financial aspects of risk management rather than culture and are often employed when a major risk event or change has occurred. They may provide assurance of: > Adherence to risk policies and procedures > Adherence to subscribed regulatory frameworks > Identification of the risk maturity the charity operates at, and how well the risk culture has been embedded > Whether a specific risk event or failure was dealt with effectively and what the financial or reputational impact on the charity is likely to be > Consider key lessons learnt and undertake analysis to gain a deeper understanding of risks

3. Optional

Role	Summary of the role
None	None.

C. Diagram of the model (large charities)



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

www.theirm.org/charities

Tel +44 (0)20 7709 9808

Email enquiries@theirm.org