BRIEFING PAPER

Assurance with Vision

Three Lines of Defence

Introduction

2015/16 has been one of the hardest years on record; all NHS organisations have faced, and continue to face, significant financial and quality challenges. What is becoming increasingly clear is that governing bodies, the body of individuals that lead organisations, are identifying the need to ensure that there is greater clarity around medium and long term objectives and strategies and their sustainability within the local and regional health economies.

Governing bodies need to have the time and freedom to think about new ways to make services sustainable both within their own organisations and through greater integration, rather than becoming too involved in the day-to-day operation of controls, which should be the preserve of robust operational groups and committees. In support of releasing time at the strategic level of the organisation, all governing bodies should consider how they use their assurance providers to give them confidence around the operation of key controls, whilst recognising that, given current pressures, good control systems may not necessarily result in desired outcomes.

Risk Management Framework

Governing bodies are ultimately responsible and accountable for setting their organisation's objectives, defining strategies for their achievement, and establishing governance structures and processes to manage the risks to achieving them. They provide direction to senior management by setting an overall risk appetite and identifying the principal risks facing the organisation. Governing bodies should then delegate primary ownership and responsibility for operating risk management and control to senior management.

Management's job is to provide leadership and direction to employees in respect of risk management, and to control the organisation's overall risk-taking activities in line with agreed levels of risk appetite. Governing bodies should then be assuring themselves, on an ongoing basis, that senior management is responding appropriately to risks.

360 Assurance has a clear vision for the delivery of audit and assurance solutions. Our approach is one of Partnership and Collaboration. We work in partnership with you to provide a cost effective, quality driven service that helps you deliver your key priorities.

The Three Lines of Defence

The **Three Lines of Defence Model** is seen as a simple and effective way to clarify roles and responsibilities in relation to risk management. Importantly, it outlines the role Internal Audit plays in providing assurance on the effectiveness of governance, risk management arrangements and internal controls within an organisation.

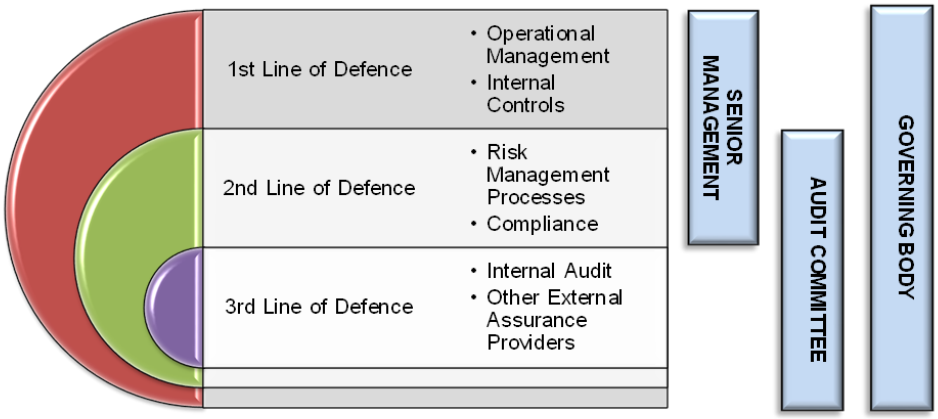
The Model is not new but has gained some recent provenance through the July 2015 paper produced by the Committee of Sponsoring Organisations (COSO) and the Institute of Internal Auditors[1]. The paper seeks to help organisations enhance their overall governance structures by providing guidance on how to articulate and assign specific roles and responsibilities regarding internal control by relating COSO's Internal Control - Integrated Framework[2] to the Three Lines of Defence Model.

All organisations should have an established risk management framework in place that provides for a range of risk and control functions. In designing those risk and control functions, it is important that organisations are clear in how they assign specific roles and coordinate them effectively and efficiently so that there are no gaps but also no unnecessary duplication.

The Model identifies 3 lines of defence in effective risk management:

1. **First line of defence** - functions that own and manage risk
2. **Second line of defence** - functions that oversee risk
3. **Third line of defence** - functions that provide independent assurance

The three lines of defence then work collectively to support the governing body, and senior management, in being able to focus at a strategic level. If responsibilities are clearly defined, each line of defence can understand the boundaries of its responsibilities and how its position fits with the overall organisational risk management structure. This is demonstrated in the diagram below.



Adapted from 3 Lines of Defence Model – Institute of Risk Management

[1] Leveraging COSO Across the Three Lines of Defence, Institute of Internal Auditors, July 2015

[2] Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, Jersey City, NJ: American Institute of Certified Public Accountants, May 2013

First Line of Defence

The **first line of defence** is provided by front line staff and operational management and are the functions that **own and manage risks**.

Operational management is responsible for maintaining effective internal controls and for implementing risk and control procedures on a day-to-day basis. Operational management is responsible and accountable for identifying, assessing, controlling and mitigating risks.

There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight any breakdown in controls, inadequate processes and unexpected events. Typically, the controls in place will be '**preventative**' controls, those controls designed to limit the possibility of a risk being realised, and '**corrective** 'controls, those controls designed to limit or reduce the impact should a risk materialise.

How effective the first line of defence (and also second line of defence) is will be influenced by the overall control environment within the organisation and the way the governing body and senior management set the 'tone at the top'. It is part of an organisation's culture, management's philosophy, style and support provided, and the awareness of the controls established and maintained by management and staff, as well as staff attributes, such as their competence, ethical values, integrity and morale.

Examples of first line of defence controls

- Authorisation of invoices prior to payment
- Safe keeping of cash and other valuable items
- Checking the suitability of staff prior to their employment, e.g. DBS check
- IT system access controls
- Staff training and development
- Processes that have a positive impact on staff welfare and retention
- Anti-crime arrangements

Second Line of Defence

The **second line of defence** is the functions that **oversee risk**.

It is provided through the various risk management and compliance functions, such as policies, frameworks, tools and advice, that an organisation might put in place to support and monitor the effectiveness of the first line of defence. Typically, it will incorporate:

- a risk management function that facilitates and monitors the implementation of effective risk management and assists risk owners (the first line of defence) in determining an appropriate level of risk, as well as assisting with the reporting of risk-related information throughout the organisation;
- a compliance function that monitors various specific risks, such as health and safety and compliance with quality standards. This includes both monitoring that it does itself and also that carried out by others under its direction; and
- A financial control function that monitors financial risks and financial reporting issues.

Management establishes these functions to ensure that the first line of defence is properly designed, in place, and operating as intended. Typically, these are '**directive**', designed to ensure that a particular outcome is achieved, and '**detective**', designed to identify occasions when undesirable outcomes have been realised.

They design policies, set the direction for the organisation, introduce best practice and ensure compliance, however, being directly involved in the design and development of internal control and risk procedures, they have only limited independence from the first line of defence.

Key aspects for the second line of defence are maintaining policies and procedures, to reflect changes in strategic priorities and risks, and to ensure that staff receive training and support to discharge their role in respect of the first line of defence.

Examples of second line of defence functions

- Risk Management Strategy and/or Policy
- Risk registers and assurance framework and review of them
- Committee with responsibility for oversight of risk
- Monitoring compliance with laws and regulations
- Quality monitoring arrangements
- Contract monitoring arrangements
- Organisational policies and procedures

Providers of independent assurance

- **Internal Audit**
- **Anti-Crime**
- External Audit
- Care Quality Commission inspections of health and social care services
- NHS England's CCG Improvement and Assessment Framework 2016/17
- Risk Assessment Framework for Foundation Trusts
- Accountability Framework for NHS Trusts

Third Line of Defence

The **third line of defence** is supported by the functions that **provide independent assurance**.

Internal Audit is seen as one of the main components of this as it provides independent assurance to the governing body and senior management on the effectiveness of governance, risk management and internal controls, including the effectiveness of the first and second lines of defence, and provides advice on improvements which could be made.

The Head of Internal Audit provides an annual internal audit opinion based on an objective assessment of the framework of governance, risk management and internal control. The work of Internal Audit encompasses all aspects of an organisation's risk management framework from risk identification, risk assessment, risk management to reporting on risks.

Internal Audit should not be relied on as a control measure. It needs to maintain its independence from the first and second lines of defence and its role is largely 'detective' and 'corrective'. At the same time, it should not be relied upon to detect every control failure, error or deficiency.

Importantly, Internal Audit needs to report to a sufficiently high level in an organisation to be able to perform its duties independently. This should be directly to the governing body although, in practice, this is typically through an organisation's audit committee.

Internal Audit might also give assurance that appropriate controls and processes are in place and operating effectively to other external organisation, such as regulators and external auditors. Similarly, those other external organisations are sometimes seen as providing an additional line of defence as they may set requirements for how an organisation should be controlled and may carry out their own assessments on an organisation or a particular part of it.

Audit Committee's Role

Governing bodies are ultimately responsible and accountable for setting their organisation's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to manage the risks to achieving them.

Governing bodies should be assuring themselves, on an ongoing basis, that senior management is responding appropriately to risks through the operation of effective governance, risk management and internal control procedures.

Typically, governing bodies delegate this assurance 'task' to an audit committee, a sub-committee of the governing body. The audit committee's role is then to maintain oversight and to monitor the effectiveness of internal controls and risk management arrangements, on behalf of the governing body. It should also have oversight of Internal Audit's work as well as that of other external assurance providers, ensuring that Internal Audit's work evaluates both first and second line of defence activities.

Existing publications on the Three Lines of Defence[3] comment on the role of the audit committee and what it needs to do to be effective in fulfilling this role:

- it needs to have oversight of the whole risk and control framework and all activities of the organisation;
- there needs to be open and honest communication between management, compliance functions, all assurance providers and the audit committee;
- Internal Audit needs to be effective in what it does;
- Internal Audit's plan of work should be risk-based and focusing, primarily, on the areas of greatest risk to the organisation;
- it should be ensuring that the work of all assurance providers is coordinated and optimised to ensure that there are no significant gaps and that duplication of effort is avoided.

How the Audit Committee might gain assurance

- Direct reporting to the Audit Committee by Internal Audit
- Direct reporting to the Audit Committee by External Audit and other external assurance providers
- 'Deep dive' reviews of high scoring risks
- Reviewing the adequacy and effectiveness of policies and procedures (but not approving them)
- Reviewing the adequacy and effectiveness of risk management procedures

[3] *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control*, Institute of Internal Auditors, July 2013

The Three Lines of Defence, Audit Committee Institute Sponsored by KPMG, 2009

Glossary of Terms

Control - any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved (IIA definition).

Control environment - the way the governing body and senior management set the tone of an organisation. It is part of the organisation's culture, influencing how risk is viewed and the 'control consciousness' of its staff. Every organisation operates differently and will be influenced by their organisational ethics, values, structure, reporting lines, authority, rules and the documentation of policies and procedures.

Risk appetite - an organisation's willingness to accept risks and what sorts of risks it is willing to accept in pursuit of its strategic objectives.

Preventive control - a control that relates to actions that are taken before an event occurs and are designed to limit the possibility of a risk being realised.

Corrective control - a control that is designed to limit the scope for loss and reduce the extent of any undesirable outcomes when a risk is realised.

Directive control - a control that is designed to ensure that a particular outcome is achieved.

Detective control - a control designed to identify occasions when an event has occurred and undesired outcomes have been realised.

Assurance with Vision

Contact Us

Call for more information about our services.

0116 225 6114

Visit us on the web at www.360assurance.co.uk

Leicester Office:
Riverside House
Bridge Park Road
Thurmaston
Leicester
LE4 8BL

Nottingham Office:
Stapleford Care Centre
Church Street
Stapleford
Nottingham
NG9 8DB

Rotherham Office:
Oak House
Moorhead Way
Bramley
Rotherham
S66 1YY

Key Contacts

Annette Tudor, Deputy Director	0116 225 6124
Simon Gascoigne, Deputy Director	0115 883 5305
Leanne Hawkes, Deputy Director	01709 428713
Tim Thomas, Director	0116 225 6114

This paper is provided for information only. 360 Assurance cannot accept liability for loss or damage as a result of action taken by an organisation in relation to its contents.