360 ASSURANCE

BRIEFING PAPER

Assurance with Vision

An Introduction to The Three Lines of Defence

Introduction

FIRST rule of chess: Defend your king at all costs. Well, if, in this analogy, the king represents the health of the local population, CCGs - and their partners in secondary care organisations - have had to play a very tough game of chess indeed. 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. Like a chess player preparing to play a Grandmaster, senior NHS managers must review their tactics and approach to the 'game.' What is becoming increasingly clear, for example, is that governing bodies 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.

Ultimately, Governing Bodies are responsible for ensuring that the 'king' is defended. But they also 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 a strategic level, 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 always result in desired outcomes.

Just as there are several pieces on a chess board that all have a role to play in defending the king, so there are a number of mechanisms that governing bodies need to ensure are in place to protect achievement of their goals. They are generally referred to using the overall term Risk Management Framework.

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.

In This Paper

- **The 'Three Lines of Defence' management concept explained**
- **The importance of organisation culture in the application of controls**
- **An introduction to the factors involved in setting risk appetite**
- **Internal Audit's role in the 3rd Line of defence**
- **The vital role of the Audit Committee**
- **Sample self assessment questions to begin a review of your three lines of defence**

The Three Lines of Defence

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 that senior management is responding appropriately to risks.

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.

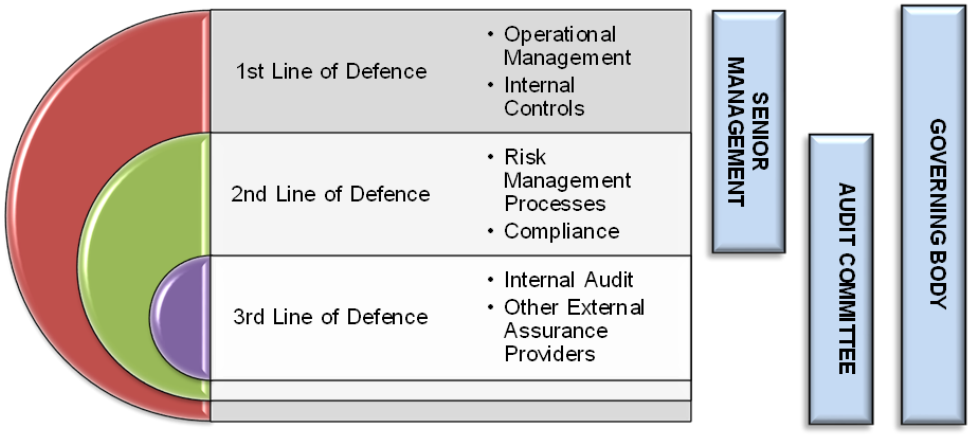
The Model is not new but has gained some recent providence through the July 2015 paper produced by the Committee of Sponsoring Organisations (COSO) and the Institute of Internal Auditors[1]. The paper seeks to help organisations enhance their overall governance structures by providing guidance on how 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.

Examples of first line of defence controls

- Authorisation of invoices prior to payment
- 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

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.

This last element of the first line of defence - the culture and the staff's response to it - should not be underestimated. Research into company failures - and, indeed, company successes[3] - consistently demonstrates that it is the commitment of staff to the company, and an existence of an open and honest culture, which will determine the strength of the first defence line. It is, after all, the staff who operate the controls that management puts in place.

[3] For example, see the Executive Summary of 'Roads to Resilience,' a report prepared by Cranford School of Management on behalf of Airmic.

Some Self-Assessment Questions:

Could we describe the culture of our organisation? Is it one in which staff feel valued for the work they do and are they therefore committed to the organisation's success? Do staff feel genuinely able to raise concerns?

Are we satisfied that staff have the skills and experience to deliver in the current environment? Do we have an appropriate organisational development strategy in place that really supports our staff?

Do we have an appropriately detailed understanding of our overall control environment, including how much reliance we are placing on the different control types? Do we, for example, place too much reliance on corrective controls and not enough on preventive ones?

Second Line of Defence

The **second line of defence** is the function (including personnel) that **oversees 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 & monitors the implementation of effective risk management and assists risk owners (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 that carried out 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 this second line is maintaining policies and procedures , to reflect changes in strategic priorities & risks and to ensure that staff receive training & 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

Some Self-Assessment Questions:

Are we satisfied that our risk register includes all the activities we are involved in (both statutory and non-statutory) where we are exposed to potential risks? Do we have up-to-date policies and procedures in place covering all these activities, and appropriate monitoring arrangements in place which would tell us if controls are not being followed?

Do all staff within the organisation really understand their role and responsibilities in relation to risk management and do they have the necessary skills to fulfil those responsibilities? For example, as Risk Management systems mature, is there evidence that risk owners have an increased understanding of risk appetite, assessing risk and identifying risk capacity and risk exposure? (See 'Improving the Defence' on the next page). Is our methodology for assessing risks clearly understood and consistently applied?

Are we satisfied that the format and content of the risk register, assurance framework and action plans is appropriate given the challenges which face the organisation? For example, does the assurance framework focus on strategic issues whilst the risk register covers operational issues?

Enhancing one aspect of the second line of defence

- One of the keys to implementing a successful Risk Management Strategy is to define risk appetite and then use that definition to really drive the risk management agenda.
- In order to successfully achieve this, it is important to understand your organization's risk profile, capacity & culture, in addition to setting risk tolerances.
- Many organisations, in both the public and private sector struggle with the concept of risk appetite and how to use it to genuinely manage risk.
- We will be engaging with clients to explore how defining and using risk appetite can support health communities to manage risk in delivering their Sustainability and Transformation Plans.

An Example of Improving the Defence

The Institute of Risk Management (IRM) highlights the need for processes that are part of the second line of defence to mature, noting particularly that '*risk management becomes more important in times of rapid change and increased market volatility.*' Since this sentence could easily be describing the NHS, it makes sense that NHS organisations should be reviewing the Risk Management Strategies to determine whether they are mature enough to respond to the current agenda.

A consistent message which comes through from the latest developments in risk management theory is the need to properly define risk appetite. And whilst it is true that many NHS organisations have included a risk appetite statement in their Risk Management Strategies, some of the more recent guidance on the subject includes some interesting detail on factors that need to be considered when determining risk appetite. This is illustrated in the diagram below:

Interestingly, the IRM also notes that '*as the marketplace becomes more volatile, an organisation will be forced to increase its risk exposure. This requires a discussion in the boardroom leading to an agreement to increase the total value that the organisation is willing to put at risk and/or find mechanisms to reduce the total risk exposure.*' Translating this statement into actions within the NHS - where the stakes (peoples' lives) are higher than in the private sector and the constraints more restrictive (taxpayer's money; government edicts) - is a challenge. We found very little guidance on how NHS organisations can determine their risk profile and their capacity to take on risk in the current environment, with its emphasis on transformation and partnership. We will therefore be engaging with our clients over the next few months with the objective of identifying practical ways in which risk appetites across whole health communities can be developed to support Sustainability and Transformation Plans.

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 & 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 (IA) 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. Unlike many of the other sources of external assurance, the organisation has an opportunity to direct Internal Audit at specific areas of concern, and it can generally expect to receive more assurances from IA than any other source.

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.

Some Self-Assessment Questions:

Have we identified all activities and risks for which independent assurance is required? Are assurances available for all of them, for example, through the 3 year Strategic Internal Audit Plan, as well as other assurance sources? Do we have sufficient resources to be able to obtain all relevant sources of assurance?

Has the organisation identified all relevant providers of assurance? Are appropriate arrangements in place to ensure that assurance providers work together, sharing their work and findings, and providing the most cost effective combination of assurances?

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

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[4] 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.

4 *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

Some Self-Assessment Questions for the Audit Committee to Consider: *

Is the Audit Committee satisfied that Internal Audit's approach to developing the Strategic Plan covers all control systems that we need to receive assurance on? Are we satisfied that Internal Audit has the necessary skills and experience to be able to provide the breadth of assurances that we require?

Does management respond appropriately to the Internal Audit process, ensuring that it is as effective as possible?

Does the Audit Committee receive reports from all independent sources and have we ensured that the work of all assurance providers is co-ordinated?

* *These considerations are included within the HFMA Audit Committee Handbook Self Assessment Guide*

Conclusion

Learning the rules of chess is a relatively simple process. Becoming a master of the game is not. Similarly, the basics of risk management can be grasped easily. Indeed, there isn't really anything new in the 3 Lines of Defence as a management concept. However, dig a little bit deeper under the surface of each line and there is more to each aspect than may initially be obvious. Opportunities exist to improve each defence line by reflecting on its quality and being prepared to change arrangements that may have been in place for years. Given the challenge that lies ahead, we would advocate that all NHS organisations review their risk management arrangements using the 3 Lines of Defence model to drive improvements, beginning with (although not limited to) the sample self assessment questions in this paper.

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

360 ASSURANCE

Leicester Office:
Riverside House
Bridge Park Road
Thurmaston
Leicester

Nottingham Office:
Stapleford Care Centre
Church Street
Stapleford
Nottingham

Rotherham Office:
Oak House
Moorhead Way
Bramley
Rotherham

Contact Us

Call for more information about our services.

0116 225 6114

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

Key Contacts

Annette Tudor, Deputy Director	0116 2256124
Simon Gascoigne, Deputy Director	0115 8835305
Leanne Hawkes, Deputy Director	01709 428713
Tim Thomas, Director	0116 2256114