The three lines of defence for assurance and reassurance

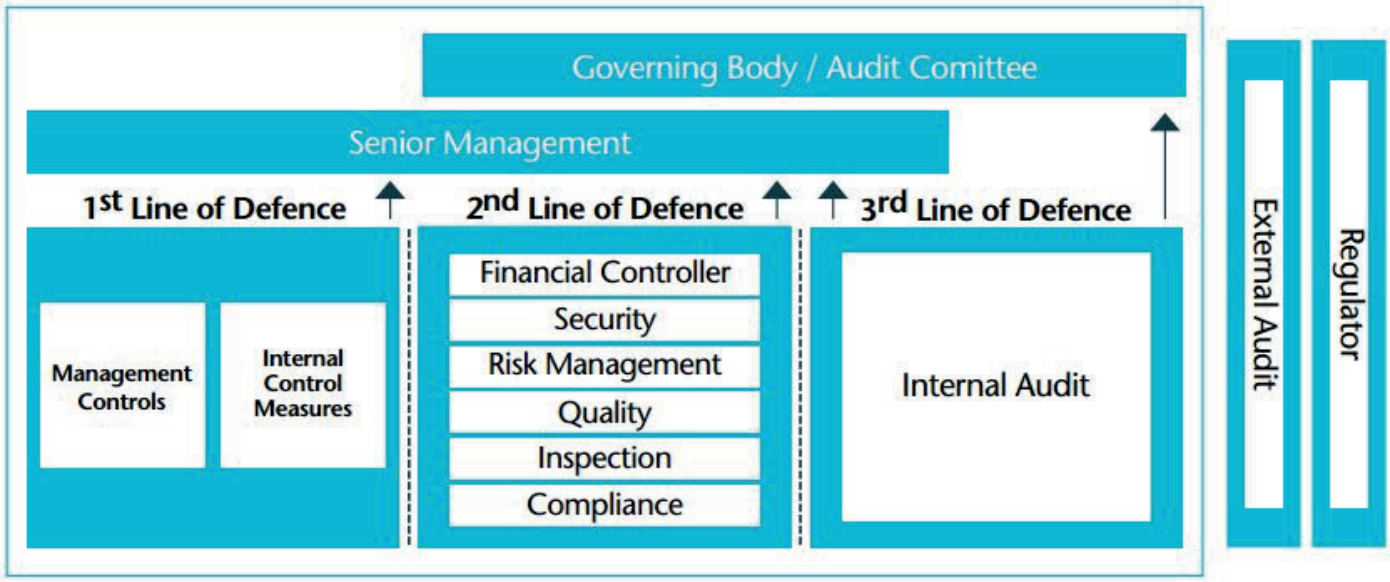
by David Holden.

In our last blog on assurance and reassurance, I explained the differences between these terms, why these differences matter and how boards can deliver both effectively.

Today we introduce a useful tool to address assurance and reassurance – the widely adopted three lines of defence model endorsed by professional bodies such as the Chartered Institute of Internal Auditors and the Institute of Risk Management, and also used here at GGI.

But what are these lines of defence protecting us from? In the words of the Institute of Internal Auditors: "Without a cohesive, coordinated approach, limited risk and control resources may not be deployed effectively, and significant risks may not be identified or managed appropriately. In the worst cases, communications among the various risk and control groups may devolve to little more than an ongoing debate about whose job it is to accomplish specific tasks."

The three lines of defence



This model provides a useful way to understand how an organisation's management and assurance functions operate and interact. The model shows the boundaries between different roles and responsibilities in the management and assurance of risks. This helps an organisation to avoid duplication and gaps in its risk management, performance management, governance and control arrangements.

By setting out roles and responsibilities relating to risk management and assurance, the model links to an organisation's assurance framework.

Line of defence	Involves
1	**operational functions** that directly own and manage services and their associated risks.
2	**oversight of management activity,** separate from those responsible for delivery but not independent of the organisation's management chain.
3	functions that provide **independent and objective assurance** regarding the integrity and effectiveness of risk management and related controls in the organisation.

The first line of defence contains operational functions that directly own and manage services and their associated risks.

The organisation's first line of defence constitutes teams and managers in operational or service delivery functions and in support functions. Typically these are operational managers and staff who manage services and risks as part of their day-to-day work (e.g. ward managers, service leads, 'shop floor workers'). Managers and staff in the first line are responsible for the correct and consistent application of organisational policies and standard operating procedures (SOPs) regarding risk management practice.

The second line of defence comes from the oversight of management activity, separate from those responsible for delivery but not independent of the organisation's management chain.

These functions contain 'corporate' or 'central' functions that oversee, assure or specialise in risk management or related control and compliance activities. For example, the organisation's second line of defence will include the corporate governance and risk management team.

The second line of defence provides the:

- frameworks
- policies
- procedures
- guidelines
- tools
- techniques
- and other forms of support

to enable first line operational managers and staff to manage risk well and therefore provide assurance. The second line also carries out:

- quality assurance
- financial control
- security
- risk management
- monitoring and inspection
- reporting activities relating to compliance against national and local standards.

The third line of defence contains functions that provide independent and objective assurance regarding the integrity and effectiveness of risk management and related controls in the organisation.

Internal audit is the key function in an organisation's third line of defence. Reporting to the board via the audit committee, internal audit provides risk-based evaluation of the effectiveness of risk management, governance and internal control in the organisation.

The third line of defence interfaces with other external providers of independent and objective assurance, including external audit, regulators (such as the Care Quality Commission), and in health services the royal colleges and national commissioners of services.

Whatever the level of defence, it is important that every report to senior management and to the board/ governing body/ audit committee advises about the level and source of assurance.

It is also important to remember that assurances can be positive or negative. Positive, that risks are mitigated and objectives are being achieved. Negative, that controls are not in place or are not working and there is strong possibility that objectives will not be met.

Sources of assurance could include, but are not limited to:

- reviews or checks within a department (e.g. manager reviews information completed by staff under their particular area of responsibility)
- an organisation-wide review
- internal audit reports
- inspection and review by an external body (e.g. Royal College).

The three lines of defence model is a useful tool to help boards and committees understand where their assurance is coming from - and whether it is positive or negative. If you have any questions or comments, or you'd like to discuss how this tool might help you, please call us on 07732 681120 or email advice@good-governance.org.uk.