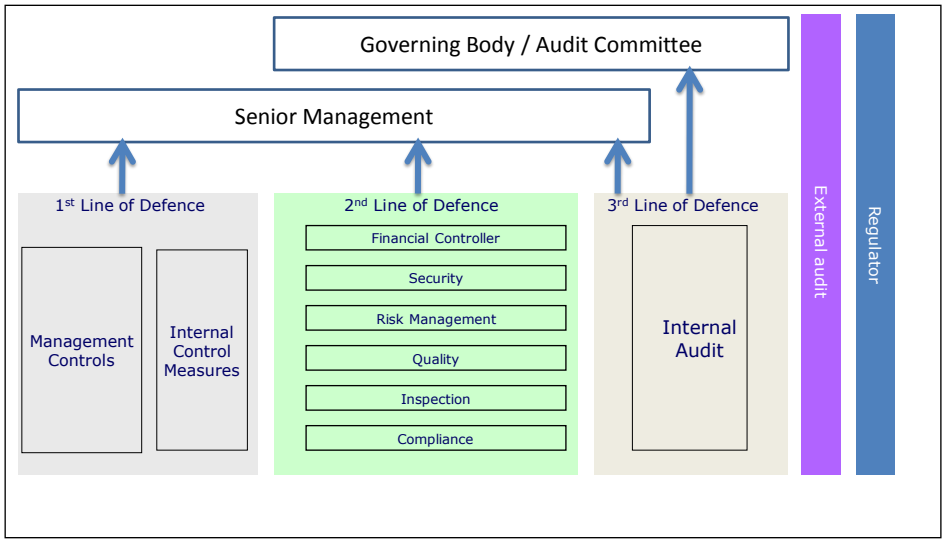
Three Lines of Defence
The ECIIA supports the "Three Lines of Defence" (3LoD) model as a benchmark for future regulatory guidance. This model, which is rapidly gaining universal recognition, can be illustrated as follows:

The Three Lines of Defence



- **As a first line of defence**, operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks
- **As a second line of defence,** the risk management, compliance and similar functions facilitate and monitor the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the organisation.
- **As a third line of defence**, the internal auditing function will, through a risk based approach, provide assurance to the organisation's governing body and senior management, on how effective the organization assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an institution's risk management framework: i.e. from risk identification, risk assessment and response to communication of risk related information (throughout the organisation and to senior management and the governing body).

While the above-mentioned functions operate within the organisation, the **external auditor** contributes as an outside body**,** providing assurance regarding the true and fair view of an organisation's financial statements. However, given the specific scope and objectives of their mission, the risk information gathered by external auditors is limited to financial reporting risks and does not include the manner in which senior management and the governing body are managing/overseeing other (strategic, operational and compliance) risks, and for which the risk management- and internal auditing function provide monitoring , respectively assurance.

This three lines of defence model has been increasingly applied to corporate governance, and particularly risk management, over recent years. The ECIIA finds that it is a useful tool to explain and demonstrate the different roles in governance and risk management, the interplay between them and how they fit together to provide stronger corporate governance. It also forms the basis of a recent paper, jointly issued by ECIIA and the Federation of European Risk Management Associations (FERMA) on "Guidance for boards and audit committees on the implementation of Art 41. 2 of the 8th Directive"