

Connect > Support > Advance

Factsheet: '3 Lines of Defence' Combined Assurance Model

What are the '3 Lines of Defence'?

- All organisation assurance activities should be visible to the Audit Committee and Senior Management, including assessment of their effectiveness.
- The '3 Lines of Defence' is a model used to identify the elements of an organisation's assurance environment.
- When used in conjunction with assurance maps, a
 documented '3 Lines of Defence' model can help inform
 the Board of Directors, Audit Committee and Senior
 Management how well the organisation's assurance
 functions are operating.

History

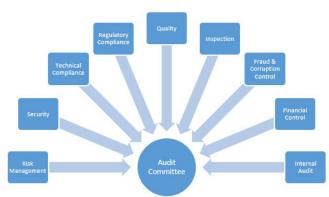
- The '3 Lines of Defence' combined assurance model was developed for HSBC by KPMG within the United Kingdom in the 1990s.
- It was later adopted by the Basel Committee on Banking Supervision as a good model for internal control management.
- The IIA—Global has adopted the '3 Lines of Defence' model.
- COSO and many other organisations, such as 'Big 4' service providers, have published information on the '3 Lines of Defence'.
- Its use is widespread in corporate and public sector organisations.

What does the '3 Lines of Defence' look like?



Rationale for the '3 Lines of Defence'

- Assurance is expensive. For this reason, it is important
 for entities to get it right when determining the make-up
 of their assurance environment. Typically, a wide range
 of specialist risk and control areas undertake assurance
 activities, as illustrated at right.
- It is easy to expend more effort and money than necessary when there is no co-ordinated approach to assurance. The '3 Lines of Defence' is a concept used by organisations to define their assurance environment to:
 - Establish boundaries and assign responsibilities to each risk and control group.
 - Avoid gaps in controls and unnecessary duplication of coverage.
 - Deliver strong, integrated and cost-effective organisation-wide assurance activities.



Connect > Support > Advance

The '3 Lines of Defence' explained

The 1st Line of Defence is concerned with management controls and generally has a real-time focus.

- It is aimed at review of governance and compliance arrangements to demonstrate 'checks and balances' are working effectively.
- The 2nd Line of Defence centres on risk oversight and involves some degree of real-time activity, with a mandate to review 1st Line of Defence activities.
- This encompasses the work of specialist areas like risk management, technical and regulatory compliance, and safety.
- This aims to confirm the effectiveness of governance and compliance arrangements, and to identify and action improvements.
- The 3rd Line of Defence involves independent assurance that evaluates the adequacy and effectiveness of both 1st Line and 2nd Line risk management approaches.
- This is typically undertaken by Internal Auditors, to independently confirm governance and compliance effectiveness, and to recommend improvements.

Why is the '3 Lines of Defence' model useful?

- Coverage Ensures assurance coverage against key risks.
- Comprehensiveness Ensures there is a comprehensive risk management and assurance process.
- Gap analysis Identifies assurance gaps and implement remediation actions.
- Effort Minimises duplication of assurance effort.
- Cost Minimises assurance cost.
- Stakeholders Provides comfort to stakeholders there is the right amount of assurance activities – and they're working.
- Understanding Helps to understand where risk management and assurance roles and accountabilities reside.
- Skills Identifies skills required to deliver required assurance as a guide to resourcing.

Guidance

- IIA—Global Position Paper 'The Three Lines of Defense in Effective Risk Management and Control'
- IIA—Global Practice Guide 'Internal Audit and the Second Line of Defense'
- IIA—Netherlands White Paper 'Combining Internal Audit and Second Line of Defense Functions'
- IIA—Global GTAG 'Assessing Cybersecurity Risk Roles of the Three Lines of Defense'

© 2018 The Institute of Internal Auditors—Australia

