# Three Lines of Defense:
# Four Limitations

Douglas Hileman, CRMA, CPEA, FSA

Many organizations worldwide have adopted the "three lines of defense" (3LOD) model. The Institute of Internal Auditors (IIA)'s position paper from January 2013 is the most commonly-cited reference.[1] The IIA published an exposure draft seeking comments. So it's a good time to revisit the position paper – flaws and all. Here are four things I believe are limitations to the IIA's position paper.

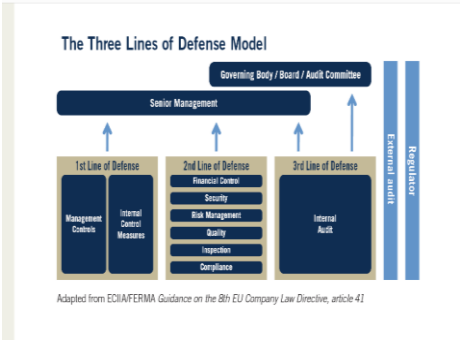
1. It's short.
2. It focuses on Internal Audit.
3. 2LOD audit is not differentiated from other 2LOD.
4. Governance isn't explained.

**It's seven pages.** As such, it is a high-level overview of an organizational model. The good news is that, being at a high level, organizations adapt and apply it as it fits them. The bad news is that organizations must think about the model, and develop a rationale for how to apply it. There are scores of publications about it, and they don't all agree. Many companies confuse first and second lines of defense. Companies may be placing undue reliance on a model they don't understand, or have not applied to be fit for purpose.

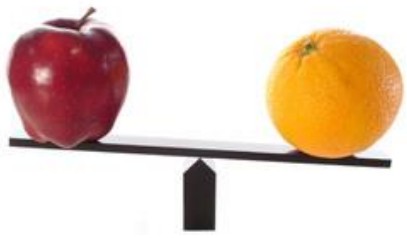
**The Focus is on 3LOD.** As a position paper written by the global organization for Internal Auditors, this is perhaps to be expected. After all, it is a position paper. However, there are other lines of defense in risk management and control. External auditors and regulators even appear in the graphic in the IIA's position paper, and in the original document published by the European Confederation of Institutes of Internal Auditing (ECIIA). The graphic in the ECIIA publication showed Operational Management and Internal Controls within the 1LOD box. Risk Management, Compliance, and Others were depicted in the 2LOD box, with only Internal Audit in the 3LOD box. They also serve as "lines of defense" and warrant inclusion as a fourth and fifth line of defense.

[1] See https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

**2LOD Support Functions & Audit Functions Not Differentiated.**




The graphic in the ECIIA publication showed Operational Management and Internal Controls within the 1LOD box. Risk Management, Compliance, and Others were depicted in the 2LOD box. There are also internal audit functions to monitor areas of high risk. Organizations have IT audit, quality audit, environmental audit, safety audit, security audit and other audit functions. These are 2LOD functions – authorized by, and existing at the discretion of management. These are not 3LOD Internal Audit, authorized by the Board. There must be independence and objectivity to be valid and meaningful audit activities. Failure to distinguish the two creates the risk that these internal audit functions will be ineffective in mitigating risks in these high-risk areas. Management can place undue reliance on these internal audit functions, creating blind spots of increased risk.



**The term "governance" is not adequately explained or covered**. Risk management is not the sole responsibility of any person or department. As with quality, it is everybody's job. As with quality, allocating roles, responsibilities, and tasks becomes the challenge. There are interfaces between departments. Organizations rightfully desire efficiency, avoiding duplicate efforts and costs. But effective risk management calls for identification, assessment and appropriate management of risks -all key aspects of risk management must have a home somewhere. "GRC" is a common term for Governance, Risk Management and Compliance. "Governance" is not mentioned as frequently as the other two, and is less understood. Governance can be thought of as a system of checks and balances that keeps different parts of the organization in synch, and in line with the organization's objectives and risk appetite. The LOD model for risk management and control involves many departments, empowered by different parts of the organization and its stakeholders. The governance among them is important.

The IIA released an Exposure Document in June 2019. The next in this series provides a perspective – and highlights several problems.

Contact doug@douglashileman.com for assistance or more information.

For more useful blogs, see:

www.douglashileman.com