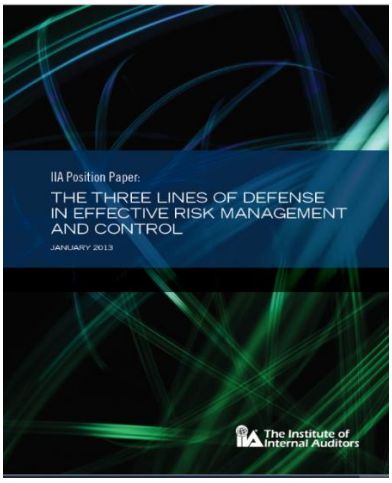
Three Lines of Defense:
Five Things You're Probably Missing

Douglas Hileman, CRMA, CPEA, FSA

Many organizations worldwide have adopted the "three lines of defense" (3LOD) model, with the Institute of Internal Auditors (IIA)'s position paper from January 2013 is the most commonly-cited reference. The IIA published an exposure draft on the 3LOD, so it's worth stopping to revisit it. Here are five things that many people miss about the 3LOD model.



1. The title is "Three Lines of Defense *in Effective Risk Management and Control*[1]" (emphasis added)
2. It didn't start with the IIA.
3. It's a Position Paper
4. External Audit is "Hiding in Plain Sight"
5. It Succeeded Beyond Wildest Dreams

More on each one below.

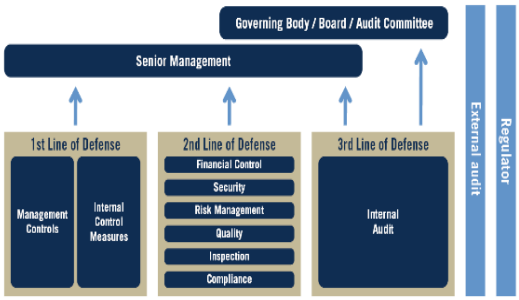
The title: It's worth asking – about the 3LOD – "defense … against what?" The title is "Three Lines of Defense *in Effective Risk Management and Control."* The 3LOD model describes roles and responsibilities for operations, support functions and the Internal Audit function – which are all familiar to most organizations. It describes roles, responsibilities, and reporting relationships. The 3LOD model also describes checks and balances – a system of governance for risk management and control. The 3LOD model seeks to remedy two common flaws in risk management and control. First, that some key risks or aspects of control aren't being done – by anybody. When things fall between the cracks, the impacts of these risks occur – and nobody was watching. Second, by establishing a common understanding of these roles and responsibilities, it can help avoid duplication and overlap.

Where it Started: The "three lines of defense" model was developed by the European Confederation of Institutes of Internal Auditors (ECIIA). The ECIAA's publication "Guidance on the 8th Company Law Directive, Article 41" explained and described different corporate governance roles and their interplay. It also included the graphic. Even the IDW's Assurance Standard for performing external risk assessment engagements acknowledged that the 3LOD model gained international recognition with the IIA position paper in January 2013.

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

It's a Position Paper. That's it. The 3LOD model is not a statutory or regulatory requirement. Organizations take positions on matters relevant to them; they typically present a perspective that benefits them and their members. Both are true of the IIA's 3LOD position paper. Even though there are other defenses for risk management (see next point), the model stops at three – because Internal Audit wrote it. It puts Internal Audit's role and value proposition into clear focus. The widespread adoption shows the need for a framework to manage risk, as well as the power of a simple model.

External Audit is "Hiding in Plain Sight." The IIA's position paper includes a graphic that depicts the 1LOD, 2LOD and 3LOD each reporting upwards to Senior Management and (for 3LOD only) to the Governing Body – or the (Audit Committee) of the Board. The graphic also includes External Audit and Regulators. Each are standalone vertical boxes, with no arrow to any other box. External auditors provide assurance on financial statements, and (in the U.S.) internal controls over financial reporting. Regulators are depicted in another lonely, disconnected silo at the far right. Regulators provide checks against risks of all types. In the U.S., the Securities and Exchange Commission regulates filings of publicly-traded entities. The Public Company Accounting Oversight Board audits the auditors. The Food and Drug Administration, the Environmental Protection Agency, the Federal Aviation Administration – all provide a line of defense for risk management, yet they are not incorporated in the model.



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

It Succeeded Beyond Wildest Dreams. Timing matters. Sarbanes-Oxley was passed in 2002. In the ensuing years, many Internal Audit departments were relegated to performing testing on internal controls over financial reporting, and not fulfilling their original role for risk management. When the financial crisis hit in 2008, the Internal Audit function was still being underutilized and undervalued. The IIA likely did not imagine that these seven pages would be embraced by 1000s of organizations worldwide. It has become the cornerstone for organization charts, roles and responsibilities, governance models. Yet at seven pages, it provides a oly high-level overview, with the flexibility for organizations to fill in the blanks for themselves.

The IIA's Position Paper on 3LOD has some limitations. See blog post at www.douglashileman.com for more.

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

For more useful blogs, see:

www.douglashileman.com