Five Suggestions for The IIA's Three Lines of Defense 2.0

Douglas Hileman, CRMA, CPEA, FSA

The Institute of Internal Auditors (IIA) published "the Three Lines of Defense in Effective Risk Management and Control" in 2013. The "3LOD" model was successful – likely beyond the IIA's wildest dreams – and has been adopted by countless organizations worldwide. It attracted its share of commentary and detractors as well. The IIA is working to refresh the position paper, as evidenced by publication of an exposure draft in June 2019. Unfortunately, the exposure draft missed the mark in several areas. Here are five suggestions to improve the 3LOD position paper, as well as to improve risk management and governance at organizations that adopt this model.

1. Don't just mitigate risk, manage it.
2. The lines of defense (LODs) to end with Internal Audit; acknowledge and explain five of them.
3. Differentiate between 2LOD audit and other 2LOD functions.
4. Revise the graphic.
5. Make it practical.

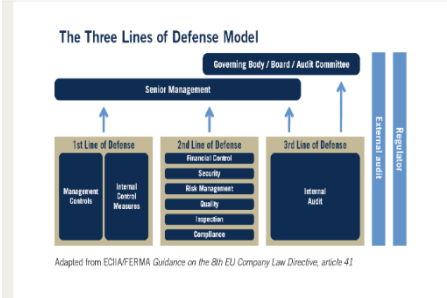
Manage – don't just mitigate – risk. The typical attitude towards "risk" is that it is something bad. There is a data breach, a product launch goes poorly, the stock price falls, or an employee commits a fraud against the organization. Yet organizations success by taking calculated, informed risk. "Risk" also involves an upside – Apple took a risk on the iPhone. Failure to recognize and pursue upsides is another risk, as with Blockbuster Video when Netflix appeared on the scene. Game theory shows that people fear losses more than they take risks for an upside. The IIA's 3LOD Position Paper can help by focusing on "risk management" and not entirely on "risk mitigation." But the emphasis on "value creation" in the Exposure Draft is too pervasive. Long-standing, common attitudes will not be altered in one Position Paper.

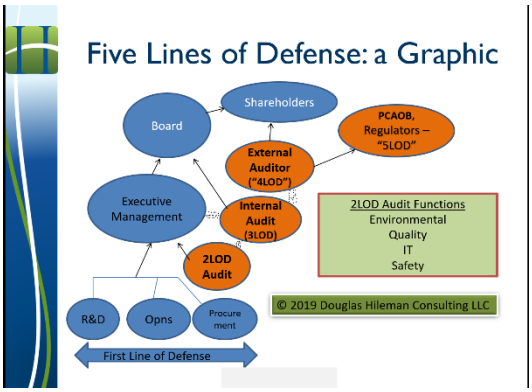
Acknowledge five Lines of Defense. Risk management and control doesn't stop with Internal Audit. External auditors are another LOD, acting on behalf of shareholders. In the US, Internal Audit play a role in testing internal controls over financial reporting (ICFR), in part to reduce the burden – and cost – of having external audit do so. Even external auditors aren't the last word. The Enron and Arthur Andersen fiasco exposed the situation that nobody was auditing the auditors. The Public Company Accounting Oversight Board (PCAOB) does so now. Many other regulators serve as a

line of defense for risk management and control, including the Securities and Exchange Commission, the Environmental Protection Agency, the Food and Drug Administration, the Federal Aviation Administration and more. These can be considered a fifth line of defense. Internal Audit is uniquely positioned and qualified to play a role in providing comfort in risk management to the Board, Management and other stakeholders.

2LOD and 2LOD audit: There are 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. There must be independence and objectivity to be valid, meaningful audit activities. Many organizations that rely on the 3LOD model fail to recognize the distinction that should be made between 2LOD audit and other 2LOD function. The Internal Audit profession ("audit" is in our name!) is in the unique position of setting guidelines for maintaining valid audit activities – period. Whatever the line of defense. Failure to distinguish the two creates the risk that these 2LOD 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 – which can come back to haunt 3LOD.

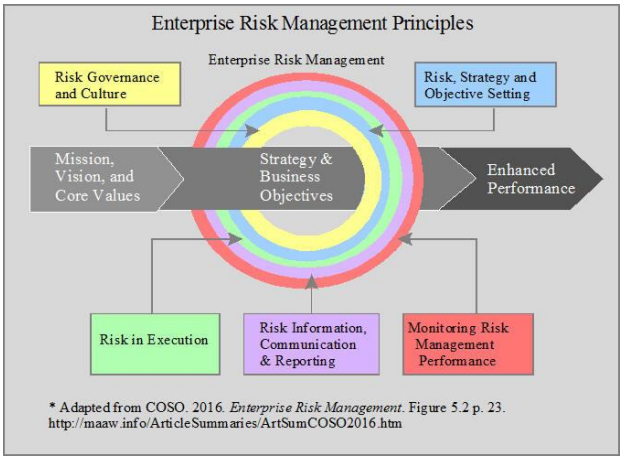
Revise the graphic: The exposure draft noted some limitations in the current graphic, including the fact that the "hard bars" suggested inflexible "silos" that never communicated with each other. Another limitation is that external audit and regulators are both depicted, but exist with no relationship to any other function. The graphic can be revised to be a better fit with roles, responsibilities, and the position the IIA suggests for governance and risk management.





I've devised graphic that depicts a 5LOD model with primary and secondary reporting relationships (see graphic); more on this at www.douglashileman.com.

Make it practical: The 3LOD model has been successful – likely beyond the IIA's wildest expectations. Revisions to the position paper must be practical. Version 2.0 must be understandable by a wide range of stakeholders – including all those who have adopted it (either as intended or otherwise), those considering it, or the stakeholders who rely upon organizations who use it. The IIA can learn a lesson from COSO, the organization that published the Enterprise Risk Management (ERM) framework in 2004. One criticism of the original 2004 COSO ERM framework was that it was esoteric, and required professionals (usually external and paid) to implement it. ISO adopted the 31000 standard for risk management, more of a "cookbook approach" to ERM, at least in part to this limitation. COSO refreshed the ERM framework in 2017. The update included a new graphic, replacing the familiar "COSO Cube", in part because the 7-layer ERM cube was confused with the 5-layer COSO cube for internal controls. The revised graphic is more complicated, and is not readily understandable by organizations and practitioners who would attempt to adopt it. The LOD model should be explained and illustrated in terms simple enough to encourage widespread understanding and adoption, and to achieve the objective of more effective risk management and control. Revise it with a broad array of stakeholders in mind.



Contact doug@douglashileman.com to start or improve your organization's lines of defense.

For more useful blogs, see:

www.douglashileman.com