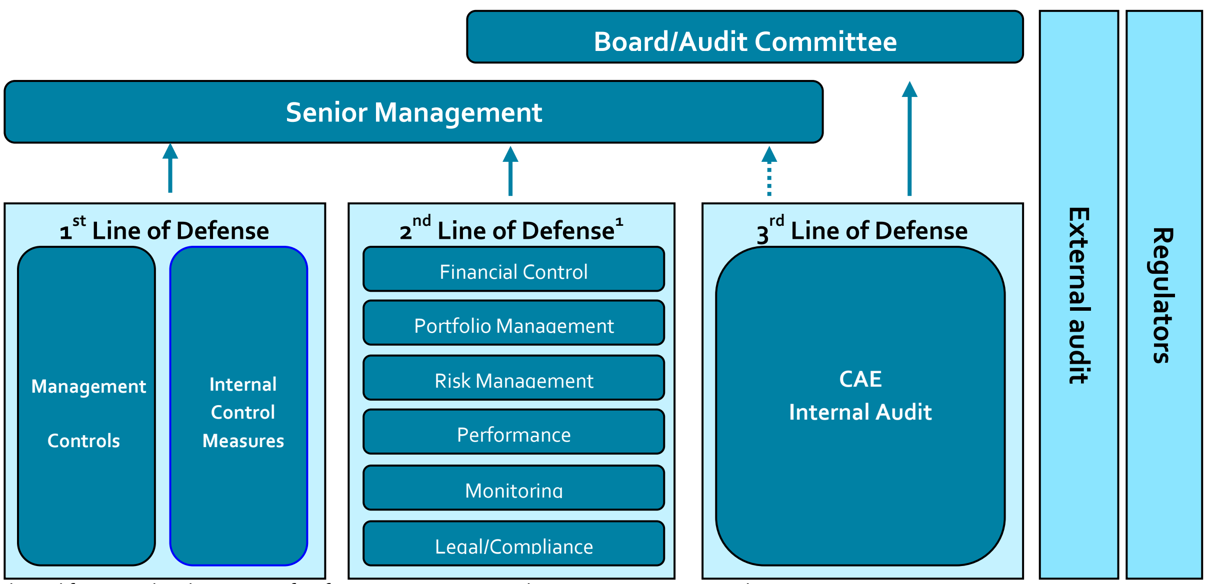
# Case Study: The Three Lines of Defense Model for Risk Management and Control – Adaptation to an In-house Asset Manager

Steve Harding, CPA

Recently we advised the Audit Committee of a corporate board on the structure of the internal auditing function at its subsidiary in-house asset manager. We'll refer to the organization as StudyCo. StudyCo manages over $15 billion in defined benefit pension and other benefit plan assets and also administers the associated benefits using a mix of retained and delegated responsibilities in conjunction with various third party providers. A recent IIA position paper on best practices for risk management and control was used as a guide on best practices. We recognize that best practices are not applied universally, nor should they be. However, all parties were comfortable that the IIA model represents best practices. Although the Audit Committee has had concerns about this for some time, they had accepted it with some mitigating controls in place. They decided to revisit it because StudyCo seeks to increase its sphere of operations to include assets of affiliates with the possibility of eventually providing advisory services to non-affiliates.

Diagram 1 depicts the latest thinking on best practices in this area.

**Diagram 1. The Three Lines of Defense Model for Risk Management and Control**

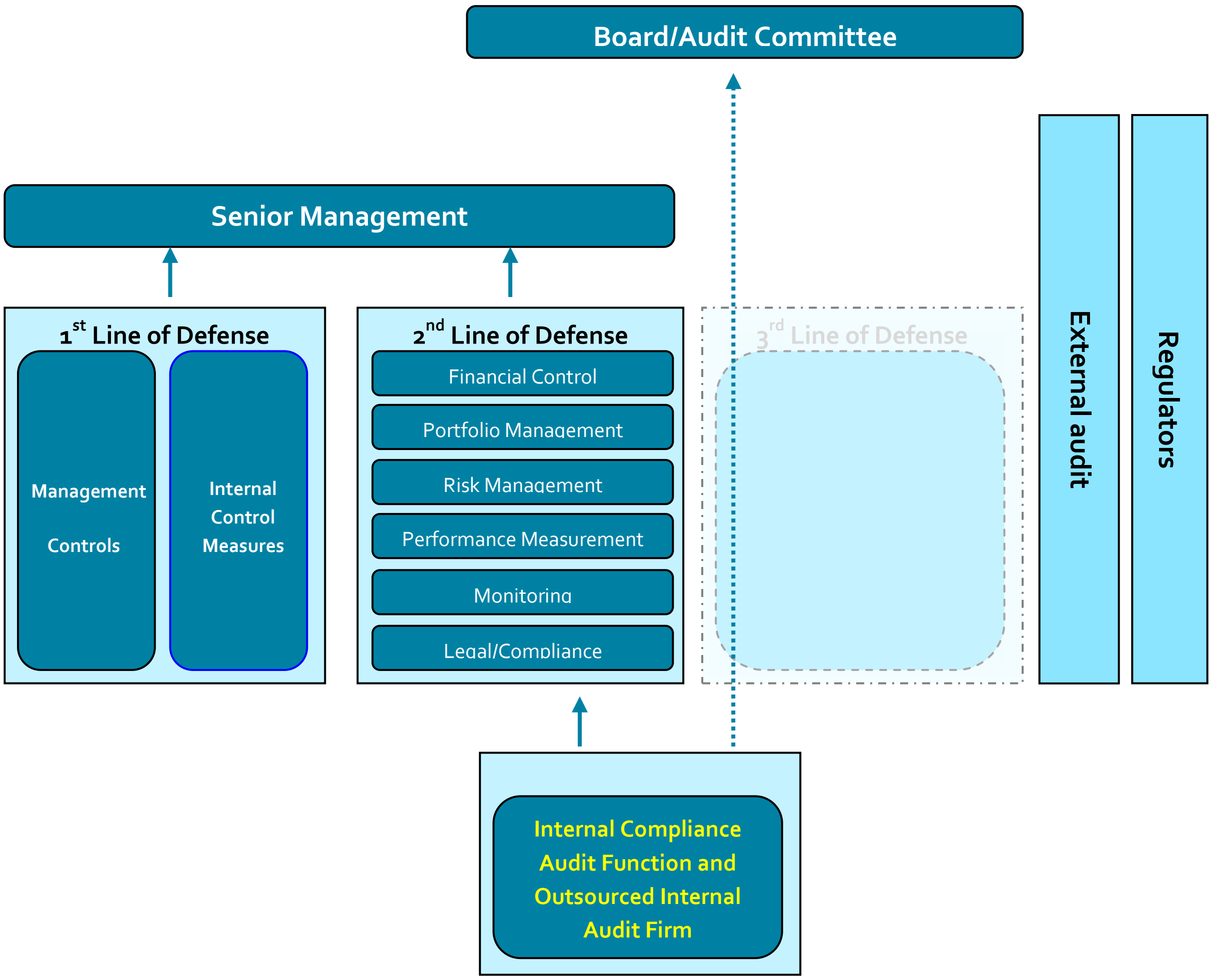



*Adapted from IIA The Three Lines of Defense position paper and* (ECIIA/FERMA, September 2010)

[1] Components of the second line of defense can vary by industry.

Diagram 2 depicts the structure at StudyCo using an adaptation of the best practice model.

Diagram 2. StudyCo's Risk Management and Control Structure (Before)




In its current structure, StudyCo's Chief Legal Officer ("CLO") (who also wears the Chief Audit Executive "CAE" hat) reports directly to the CEO and has direct responsibility over internal legal and compliance services for StudyCo. He also has responsibility over the internal audit services. The internal audit services consist of 1.) regular planned 'compliance' auditing done by staff that reports to the Chief Legal Officer and, 2.) regular planned outsourced internal audit services done by an external auditing firm. In his CAE role, the Chief Legal Officer provides audit reports to the Board of Directors and the Audit Committee as do the internal compliance audit staff and the Outsource Firm. The Outsource Firm provides a significant level of internal auditing services.

What is at issue?

**1.) Does the current structure of the internal audit function create a potential impairment to the Chief Audit Executive's independence or objectivity?**

On one level, there is a lack of independence because the Chief Legal Officer is in position to audit the activities he oversees, i.e., compliance and legal. On another level, since he is a direct report of the CEO, there is a lack of independence in the event that internal audit needed to investigate the CEO. The StudyCo Board and management have recognized some of this and have instituted some mitigating controls, but the structural problem remains.

**2.) Is the third line of defense missing?**

As it stands, the current structure lacks the third line of defense that comes from an independent internal audit function that reports directly to the Audit Committee. The typical structure in place at the best run firms has the internal auditor serve at the pleasure of the Board. That is not the case at StudyCo. The current structure does not sufficiently protect the organization, the benefit plans, or the Board from potential problems that could arise in the future out of the inherent split loyalty. While a high level of assurance is provided currently, comprehensive assurance is based on the *highest* level of independence and objectivity within the organization.[2]

**3.) Is the weakness apparent to knowledgeable observers seeking to do business with StudyCo?**

For any knowledgeable affiliate looking into an advisory relationship with StudyCo, the problem with its control structure should be easy to see. For most experienced managers performing due diligence on StudyCo, this would be flagged. Questions would be drawn and these would be raised with StudyCo's management team for discussion, e.g., what is the reason for the current structure vis-à-vis internal audit? How do you compensate for the lack of independence? Why did the Board decide to set it up this way, etc?

*Dual lines of responsibility*[3] (wearing multiple hats) are acceptable only in small organizations, e.g., emerging managers. Also, the weakness remains even if the Board decides to not pursue expansion of its advisory services to affiliates. These questions could be avoided by correcting the weakness.

**4.) Does the current structure create an unduly awkward and demanding position for the CLO?**

The Audit Committee revisited and discussed the issues with our assistance. The Committee decided that full-time professionals are needed and justifiable for both legal counsel and internal audit at an investment manager of the size of StudyCo which has approximately 250 employees.

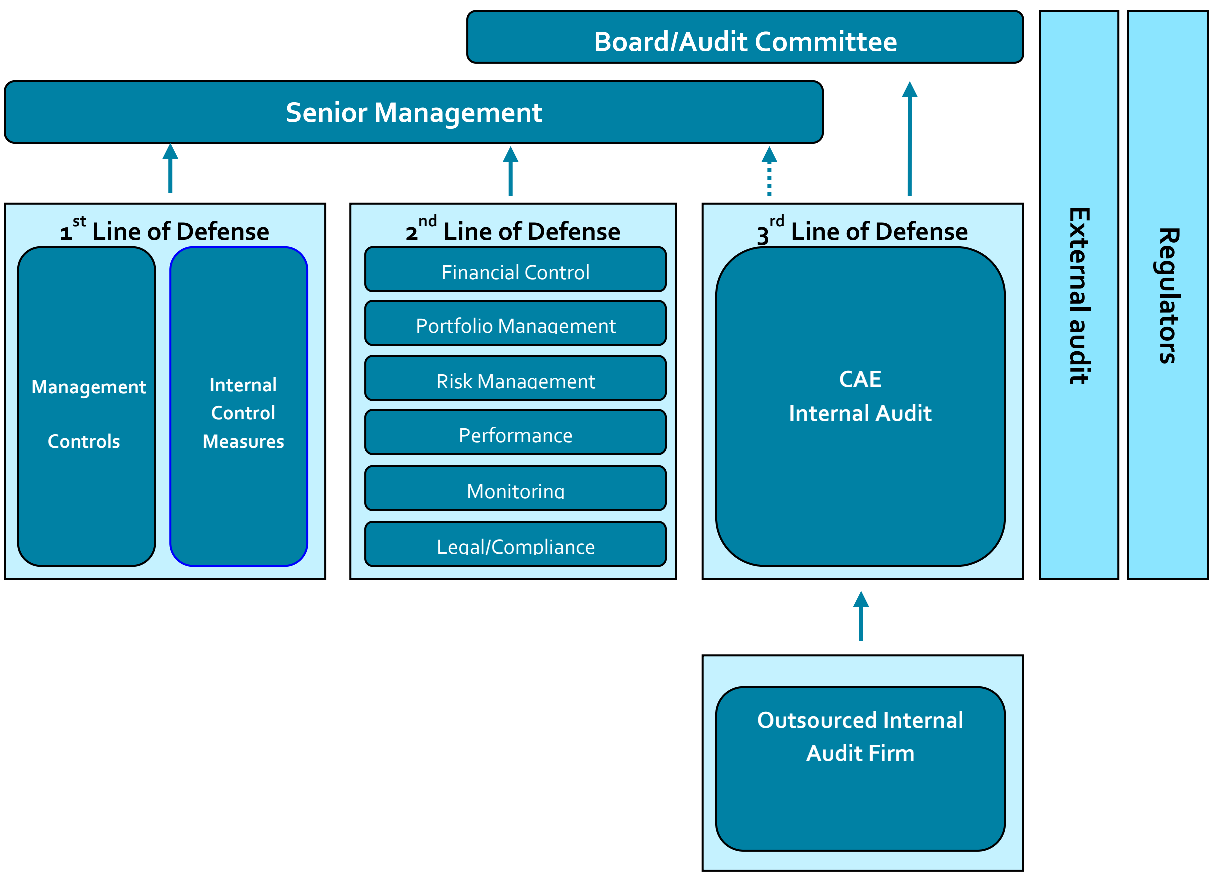
[2] (The Institute of Internal Auditors, January 2013, p. 5)
[3] "To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. <u>This can be achieved through a dual-reporting relationship.</u>" Standard 1100. International Standards for the Professional Practice of Internal Auditing. The dual reporting referred to in this section of the Standards is the administrative reporting to the CEO. Direct reporting to the Audit Committee remains paramount.

The Committee recognized the tremendous effort of the CLO, but acknowledged that they were expecting too much.

The next section describes the Three Lines of Defense Model with a solution that corrected the problem.

The revised control structure was set up to parallel the best practice model and provide the independence that was missing. Diagram 3 depicts the structure that restored the third line of defense and corrected the relationship between the internal auditing function and the rest of the organization.

### Diagram 3. StudyCo's Risk Management and Control Structure (After)




The costs and benefits to the proposed structure were considered. First, StudyCo would have to hire a qualified Chief Audit Executive. The Audit Committee and the CAE continue to use outsourced internal audit services as necessary. A potential offset to the compensation cost of the CAE is that some of the work that the Outsource Firm does could be performed by the CAE. The CAE salary and benefits package would be dependent on the position description decided upon by the Audit Committee and the market competition. Second, separating the function and adding a CAE could lead to expansion of internal audit staff and even a restructuring of the current compliance auditing staff. We did not suggest this; rather we noted that it could happen down the road and thereby increase the cost. There are possible offsets to cost here also.

Several benefits were achieved. The StudyCo Board strengthened the organization's overall control architecture. The Board eliminated an area of potential criticism of StudyCo's control structure. This was critical as StudyCo sought to expand advisory services. The legal, compliance and auditing functions would have the attention they need from dedicated department heads and would have clearer lines of separation, authority and responsibility. The Chief Legal Officer could devote more time to support of StudyCo's legal, regulatory and compliance needs and was relieved of the pressure from owning the internal audit function. The CEO required less time to devote to the internal audit, control and risk monitoring processes. The Audit Committee now has a more direct connection into the organization's control framework through a dedicated Chief Audit Executive.

## References

ECIIA/FERMA. (September 2010). *Guidance on the 8th EU Company Law Directive; Article 41.* Brussels: European Confederation of Institutes of Internal Auditing & FERMA.

The Institute of Internal Auditors. (January 2013). *The Three Lines of Defense in Effective Risk Management and Control.* Altamonte Springs: The IIA.

The author may be contacted by email at Steve@AnodosAdvisors.com