Return to the blog

Learning from Public Company Risk Management: Throwing out the Bathwater while Keeping the Baby

This article examines fundamentals of risk management and how they differ in application between public and private companies. The final section presents a scalable and actionable risk management framework for private companies.

Public companies are subjected to mandates from the SEC and the stock exchanges, along with other regulators. This process can tilt the balance toward larger companies, which have the critical mass to absorb the costs of complying with regulatory fiat. Private companies have more freedom to choose how they will cope with risk.

Private company directors who understand how risk management is pursued by public companies are better situated to oversee risk management. It is important to devise a risk management process that promotes the business, rather than one that burdens it. Scaling the activity to fit the resources of the company can produce a process that will be accepted by all layers of management and generate a productive conversation between management and the board regarding risks that the company intends to accept, avoid, or manage.

Risk Management Practices

Private and public companies vary widely in many respects, many of which have been discussed in depth elsewhere, such as SEC filings, listing requirements, and public company-specific laws such as Sarbanes Oxley. One less discussed but perhaps more import difference is risk management practices. In public companies, risk management is powerful, pervasive, and multi-layered. In private companies, by contrast, risk management is often either powerless or nonexistent.

Private companies could potentially learn much from public company risk management practices, but reflexive imitation is not desirable, either. Public company risk management practices are often formulaic and not proportional to the risks that they are attempting to mitigate, often as a result of laws, regulations, or regulators that are not applicable to private companies. Private companies are thus in a position where they can have the best of both worlds: emulating public company risk management practices that are beneficial while eschewing those that are not.

One of the most dramatic differences between public and private company risk management is how pervasive it is at the former, especially in the larger Fortune 500 and 100 public companies. At one such large public company where I worked, I joked that new hires were issued an ID badge, a compliance officer, a QA inspector, and an attorney. There were frequent exams and audits, many scheduled ahead of time with the regularity of the rising and setting sun, and many surprise, ad-hoc ones. It was not uncommon to get calls or emails at all hours of the day from risk management personnel I did not know from risk management units I had never heard of requesting documentation for actions that I thought had already been reviewed and approved multiple times. Docile employees at all ranks dutifully comply with such requests even when pushback might be warranted. Contrast that with many private companies, where risk management is often either absent or ignored, where modest intrusions by risk managers—where risk management personnel exist at all—are often met with hostility: "You can't tell me what to do with ***my*** clients!"

Not only is risk management pervasive at public companies, it is multi-layered. The Institute of Internal Auditors (IAA) popularized the now-standard Three Lines of Defense ("3LoD") model in 2013, but it did not invent it. In the 1995 movie *Casino* depicting a 1970's Las Vegas, casino-manager Sam Rothstein,

JOIN PDA

Contact Support

Forgot Your Credentials?

Existing Users/Prospects

If you cannot remember your username, please click here.

If you cannot remember your password, please click here.

Quick Links

Events
Chapters
View Board Roles
Post Board Opportunities
Subscribe to Our Newsletter

Upcoming Events

Tue Jan 10, 2023
Atlanta In-Person Event | Acquiring a Seat on a Private Company Board
Category: Atlanta

Wed Jan 11, 2023
Minnesota Chapter In-Person Event | Board Role in CEO Succession
Category: Minnesota

Wed Jan 11, 2023
Houston In-Person Event | Membership Drive Happy Hour
Category: Houston

Tue Jan 17, 2023
Philadelphia Chapter Virtual Event | Speed Networking for Philadelphia Chapter Members
Category: Greater Philadelphia

Tue Jan 17, 2023
Detroit Chapter In-Person Event | New Year Social & Networking Event
Category: Detroit

Event List

Twitter Feed

Tweets from @PrivDirAssoc

Privat... @ · Jan 2

Join our virtual - four-chapter networking event on February 7. PDA Chapters Atlanta, NY, New England, and

played by Robert DeNiro, describes his casino's multi-layered approach to risk management:

In Vegas, everybody's gotta watch everybody else. Since the players are looking to beat the casino, the dealers are watching the players. The box men are watching the dealers. The floor men are watching the box men. The pit bosses are watching the floormen. The shift bosses are watching the pit bosses. The casino manager is watching the shift bosses. I'm watching the casino manager, and the eye in the sky [cameras] is watching us all.

In 3LoD, as classically depicted and understood, the first line of defense is the business units that touch products and customers. They are the ones closest to risk and the ones in the best position to understand and manage it. The most important take-away from 3LoD is that risk management is ***everyone's*** responsibility. The second line in 3LoD, upper-case "Risk Management," oversees the first line. They must have the expertise to oversee and advise the first line but also the independence and authority to provide it with ***effective challenge***—reports and memos that no one reads or heeds do not suffice. The third line, internal audit, oversees the first two lines and provides ***assurance*** that the first two lines are performing their roles. To ensure the independence of the second and third lines, they must have reporting lines and compensation structures that are separate from the first line. Risk Management should report to the Chief Risk Officer and Internal Audit should report directly to the board of directors or a committee thereof.

3LoD is an abstract conceptual framework that must be operationalized to be effective. In addition to the authority and independence already discussed, effective risk management has four components:

- Board oversight
- Policies and procedures
- Management Information Systems (MIS)
- Controls

Board oversight. The board is responsible for establishing what types and levels of risks the company is willing to assume. It should develop a risk appetite statement (RAS) to set the top-of-the-house risk limits that guide business units in developing their more granular policies and procedures. In tidy academic fashion, the RAS is supposed to "cascade" from the board down. In practice, it has to be a two-way street to be effective. "Stateways cannot change folkways" (sociologist William Graham Sumner, 1913). A RAS is that is grossly out of step with what employees are actually doing will be short-lived, ineffective, and might ultimately be counter-productive through diminished board credibility.

Boards are responsible for guiding and monitoring strategy, but their role does not stop there. They are also responsible for assessing the risk management implications of strategy. A seemingly innocuous experiment with a new product, geography, demographic, or sales channel could open a floodgate for new risks: HR, IT, legal, regulatory, operational, reputational, geopolitical. Boards need to fully think through the risk management implications of their strategies.

Policies and procedures. Business units must have detailed written policies and procedures that operationalize the RAS. "Detailed" does not mean so long that no one reads them. Shorter documents that employees actually read and understand are preferrable to longer and theoretically better ones that they do not. Also, technology has broadened how policies and procedures are conceptualized and operationalized. Instead of just dusty binders sitting on a shelf, internal wikis, intranets, and chat bots can be excellent resources to help employees adhere to policies and procedures and manage risk.

In all the exams and audits I have been involved with as a banker, regulator, auditor, and consultant, there has not been a single one that did not involve an issue with inadequate documentation at some level of materiality—not one. Maintaining documentation, along with the training to ensure that everyone understands it, is a full-time job and should be staffed accordingly. A relatively small investment at the front end can save a lot of money and headaches on the backend.

Management Information Systems (MIS). "What gets measured gets managed." This is one area where public companies go overboard. It is critical to right-size reporting for metrics that are relevant, accurate, and timely, while recognizing that there are often tradeoffs between the three. Imperfect prior information about uncertain doom is preferable to perfect information about realized doom.

Controls. Controls were popularized by the 1992 Commission of Sponsoring Organizations (COSO) report, but like 3LoD, they predate time. A control is any risk mitigant. A child's piggy bank to prevent him from misplacing his allowance or his siblings from stealing it is a control. Controls fall into one or more of the following four categories:

- **Directive.** Tell people to do or not to do something. This is a start but usually an incomplete solution.
- **Preventive.** These are mechanisms that impede undesired activity or compel desired activity. Those include locks on doors, password on systems, segregation of duties, such as separating sales and cash collection, and multiple authorizations, such as dual signatures on checks.
- **Detective.** These detect activity after the fact. Alarm systems are an example. Much MIS falls in this category, too.
- **Compensating.** This is any control undertaken to mitigate the absence or weaknesses of another control. For example, if it is not possible to prevent people from entering a dangerous area, making them wear hardhats is a compensating control.

The reasons for the differences in public and private company risk management are numerous. Private companies are often smaller and have more trouble bearing the lumpy fixed costs of risk management functions, and their investors often target them because they offer both higher risk and higher returns. Public companies tend to be more risk averse. The Street rewards mundane but predictable earnings-per-share growth and punishes salacious headlines

per share growth and punishes calculous headlines.

Private companies are spared from much of the formulaic requirements that public companies face, but they still need to understand their risks and ensure that they are managing and being compensated for them to maximize their long-term value for their stakeholders. Also, many private companies will eventually try to go public or seek private equity (PE) funding, the latter of which is increasingly requiring public company-type risk management. Listings and PE deals often die in the due diligence phase due to poor risk management practices. The time to get serious about risk management is before you need to.

Andy Feltovich is a risk manager and data scientist who currently serves as a Vice President in Global Risk Management at Northern Trust. Prior to that he held roles at KPMG, the Federal Reserve Bank of Chicago, TransUnion, and HSBC. He earned a BA in political science from Southern Illinois University at Carbondale and a MA in economics from the University of Illinois at Chicago. He also holds the Chartered Financial Analyst (CFA) and Chartered Alternative Investment Analyst (CAIA) designations as well as several certifications in programming and business analytics from the SAS Institute. In addition to his "day job," he teaches fitness professionally and is an avid public speaker on a variety of topics, including risk management, analytics, wellness, and professional development.

Share this post: