Three Lines of Defense:

Failed Promises & What Comes Next

by ERICH HOEFER, MARK COOKE & THOMAS CURRY

AUGUST 21, 2020

starling

The financial industry trade group for operational risk leaders, ORX, recently reported a sharp decline in non-financial risk related loss incidents reported by its member banks over the past three months.[1] While it is possible that banks have universally embraced higher business standards and risk controls – amidst one of the most challenging business environments in history – we find alternative explanations more convincing. These range from the benign (e.g., a reduction in business volumes) to the more worrisome: that existing risk reporting systems are simply failing to cope with "the new normal" and that risk events are going unreported and—worse—undetected altogether.

Management Model

For the past decade, spending on non-financial risk management has exploded. Much of this was driven by legislative and regulatory changes implemented in the wake of the Financial Crisis and earlier scandals at firms like Enron. Banks in particular have invested billions into processes and systems for governance, risk and compliance (GRC) and intrusive surveillance and monitoring tools have become *de rigeur*.

Intent has been to manage risk through restrictive policies, processes, systems, and record-keeping. The risk management paradigm that supports these efforts and expenditures is known as the Three Lines of Defense (3LoD) model, defined in its current form in 2013 by the Institute of Internal Auditors (IIA).[2]

> *First Line accountabilities sit with key executives in customer-facing business units who must adopt risk related responsibilities. Operating "at the coal seam," these executives are believed to be best positioned to establish and maintain appropriate controls to manage risk effectively.*
>
> *The Second Line typically resides within compliance and risk functions. Leaders at the 2nd Line are meant to offer expertise and support to those on the 1st Line, serving as a resource, while at the same time posing an appropriate degree of "challenge" to encourage 1st Line accountability.*
>
> *The Third Line is internal audit, charged with overseeing the 1st and 2nd Lines to provide assurance that all parties are playing their respective risk management roles successfully – and that risk management is, in the parlance, "fit for purpose."*

"The current model has the benefit of being simple, easy to communicate, and easy to understand," the IIA asserts. "It helps organizations avoid confusion, gaps, and overlaps when they assign responsibilities for risk management and control activities."[3] Such features have made the 3LoD framework the standard for nonfinancial risk governance, globally.

For regulators, the 3LoD offers a roadmap of key decision making within complex organizations and provides clarity around questions of responsibility and accountability. Firms benefit by the 3LoD as it provides an industry standard schema by which to organize and to evidence their efforts to manage non-financial risk when facing questions from their Board of Directors, regulators, and other stakeholders.

Management Muddle

And yet the 3LoD has failed to fully deliver on this promise.

Just two years after the IIA formalized the current 3LoD model, the Bank for International Settlements (BIS) observed that, "Despite the enthusiastic embrace of the three-lines-of-defense model (...) the series of banking scandals that have occurred, and in which failures of internal control systems have played a role, have led to substantial financial losses and near-bankruptcies."[4]

Industry observers have pointed out various problems with the 3LoD model. Most critiques focus on confusion regarding roles and responsibilities across the 3 Lines, leading to coordination challenges, broken processes, and inaccurate reporting.

Some have proposed adding additional lines as a potential solution to this habitual incrementalism.

Suggestions include subdividing the 1st Line, or adding a 4th or 5th Line (or more). Other critiques focus on where roles and responsibilities should reside within the different Lines. Yet billions of dollars (not accounting for millions of staff hours) invested in such proposed fixes have not produced desired impact.

In response to these reactions from the marketplace, the IIA launched a Working Group early last year

to review the current state of the 3LoD and to offer recommendations for improvements. In July, the Working Group announced a broad update to the 3LoD framework, along with a name change.

Dropping "Defense" from the framework's title, the IIA's new "Three Lines Model" aims to signal that risk management should not be a mere reactive constraint on activity but, rather, that the risk function should serve as a key governance. "The basis for successful coherence is regular and effective coordination, collaboration, and communication,"[5] the IIA notes.[12] And here we get to the root of the challenge with the 3LoD – a challenge that remains unaddressed in the revised Three Lines Model.

Because the 3LoD is often narrowly viewed as a structural framework, solutions focus too often on structural tweaks that amount to little more than rearranging the deck chairs on the *Titanic*, leaving fundamental problems unacknowledged and unsolved.

Formal processes, systems and incentive structures hold far less sway than many leaders (and regulators) would like to believe. If the promise of the 3LoD model is to be realized, new approaches and tools for managing the informal drivers of behavior must be adopted.

Employees operate within a social context, one that works by informal social norms and peer pressures. Ignoring such insight from the behavioral sciences, both the IIA and its critics have failed to recognize that formal systems and processes putting practice to the 3LoD model are themselves fundamentally reliant upon countless personal interactions along collaborative networks of risk staff.

Each such network will have its own rules for membership: behavioral norms that must be adopted, with violators facing peer ostracism. These informal yet profound drivers of decision and action play out among the multitude of peer-connections that effectively constitute the Three Lines. Without appreciation of this, the Three Lines Model is not just impoverished, it is inoperable.

The Basel Committee on Banking Supervision (BCBS) defines Operational Risk as the risk of loss resulting from inadequate or failed processes, systems, and people, or by external events.[6] Firms focus attention and resources on processes, systems and guarding against external threats (e.g., cybersecurity). They have been far less successful at addressing the people element.

Uncrossing the Lines

Strategically targeted management interventions, along key behavioral fault lines, are necessary if the Three Lines framework is to achieve its potential. Fortunately, advances in behavioral science and data technology have now enabled the creations of tools that make this easier.

With this development, there are three main areas where we see opportunity.

1. "Even if functions in the second line of defence are organisationally independent, they may lack sufficient skills and expertise to challenge effectively practices and controls in the first line," the BIS observes. As a result, the 2nd Line can be too deferential, or too restrictive, depending on the prevailing influence from the C-suite and – critically – the levels of trust at work between the Lines. This disconnect typically extends to the 3rd Line as well which, the BIS notes, is often too far removed from the rest of the business to provide appropriate guidance and support.[7]

   Dynamics over Structure: *Rather than emphasizing structural changes, management must focus on building stronger linkages and more robust*

engagement between the 1st and 2nd Lines. Trust is critical to such peer exchange. Shifting responsibilities to the 1st Line, without attending to the interpersonal trust dynamics between employees and teams, leaves the critical enabling element of the Three Lines model to chance.

2. The 1st Line faces conflicts between interest in short term pursuit of profit and nebulous risks that may not manifest. Moreover, calculus around operational risk is necessarily based on subjective management judgement. When pressed, such qualitative risk assessments simply cannot compete with quantitative metrics – most particularly, those at the bottom line.

   Contagion over Control: *With leadership is blind to these conflicts, conduct risks are permitted to spread, contagion-like and undetected, throughout a firm.*[8] *Surveillance and monitoring systems may catch conduct violations, after damage has been done. More meaningful safeguards may be achieved through cultivation of a culture that encourages challenge and speak-up behavior, and within which staff feels encouraged to push back the moment they perceive that risky behaviors threaten to take hold.*

3. Most 3LoD frameworks fail to acknowledge "the company behind the chart"[9] or to take into account the dynamics of social influence ('culture') that drive propensity for misconduct. As such, they do little to permit for proactive insight into the likelihood of risk events. With a focus instead on maintaining "systems of record" by which to track process driven exercises, conduct risk management becomes a *Kabuki* theater in which tick-box efforts are valued over efficacy.

   People over Process: *If it is to be of any value at all, process-based reporting must be complemented by an ability to view the organization through a cultural lens that allows us to peer into the social dynamics that produce conduct risk propensities. Advances in behavioral science, network theory, and machine learning now make this possible, enabling us to anticipate performance outcomes, to commit resources in a more timely, efficient and effective manner, and to manage risks proactively.*

Establishing such capabilities is all the more important when staff are primarily working from home. Now more than ever, we need real-time, data driven metrics that provide leading indicators of misconduct before it takes hold, and insight into the relational pathways by which misconduct is most likely to spread.

An ability to identify *predilection* for misconduct would permit for proactive management interventions, targeted precisely. Such capabilities would empower the 1st Line to manage risk exposures from the front-foot. More, these capabilities may be devoted towards unlocking improved business performance as well as discouraging misconduct.

"When you change the way you look at things," Max Plank once said, "the things you look at change."

ERICH HOEFER is the COO of Starling, a leading US-based Regtech firm

THOMAS CURRY was Comptroller of the Currency, the U.S. agency that regulates and supervises national banks. He is a Senior Regulatory Advisor to Starling.

MARK COOKE is former Group Head of Operational Risk at HSBC and former Chairman of ORX, now serving on the Risk & Governance Advisory Board at Starling

About Starling

Starling is an applied behavioral sciences company that helps customers to create, preserve, and restore value.

Combining machine learning and network science, Starling's Predictive Behavioral Analytics platform allows managers to anticipate the behavior of employees and teams, and to shape it proactively.

Starling provides actionable insights that allow leaders to optimize performance and to identify and mitigate culture and conduct related risks before they cascade into crises.

This article is excerpted from a lengthier piece produced for The SEACEN Centre – the South East Asian Central Banks Research and Training Centre. This abbreviated version first appeared on the Thomson Reuters Risk Intelligence subscription platform (2.Sept.20) A second version was run subsequently by Regulation Asia (4.Sept.20).

ENDNOTES

1 https://managingrisktogether.orx.org/orx-news/5-largest-operational-risk-losses-june-2020

2 https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

3 https://na.theiia.org/about-ia/PublicDocuments/3LOD-IIA-Exposure-Document.pdf

4 https://www.bis.org/fsi/fsipapers11.pdf

5 https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf

6 https://www.bis.org/publ/bcbs96.htm

7 https://www.bis.org/fsi/fsipapers11.pdf

8 https://jumpshare.com/v/kj1VhNU5zEln7M5pj4wp

9 https://hbr.org/1993/07/informal-networks-the-company-behind-the-chart