STARLING

info@starlingtrust.com

November 6, 2020

Basel Committee on Banking Supervision
Bank for International Settlements

RE: Consultative Document on Revisions to the Principles for the Sound Management of Operational Risk

INTRODUCTION

Thank you for the opportunity to provide comments to the BCBS's Consultative Document *Revisions to the principles for the sound management of operational risk* (the "Revised PMSOR"). Starling (https://starlingtrust.com) is an innovative US-based RegTech startup that delivers analytics using internal bank data to improve non-financial risk governance, particularly with regard to risks that stem from firm culture.

Through our thought leadership and industry engagement, Starling has become recognized as an expert in our industry. Our annual white-paper, *Culture and Conduct Risk Management in the Banking Industry*[1], (aka the Starling '*Compendium*'), has become a must-read reference on the latest trends and strategies taken by bank supervisors globally to address these non-financial operational risks.

Starling also offers an AI-driven technology platform that applies advances in behavioral science and network theory to the challenge of identifying and mitigating non-financial risk in banks – proactively.

Our comments are responsive to the following questions posed in the Revised PMSOR.

Q1. Has the Committee incorporated the appropriate revisions to the Principles? Do you have any specific comments on the revisions to the Principles and supporting paragraphs?

Q2. Are there any aspects that the Committee should consider further?

BACKGROUND

As the BCBS has pointed out, Operational Risk the "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." For the past decade, spending on systems and processes to manage non-financial risk has exploded. Banks have invested billions into processes and systems for governance, risk and compliance (GRC). Increasingly, intrusive surveillance and monitoring tools, often powered by AI, are gaining traction. At the same time, compliance and risk

[1] https://starlingtrust.com/compendium/

functions are increasingly turning to Robotic Process Automation (RPA) to replace manual tracking and reporting activities with automation.

At the operational level, banks have again focused on implementing systems and process to manage misconduct through control processes or detect bad actors through surveillance and monitoring. The motivating desire has been to manage risk through documentation, restrictive processes, and by removing people from decision making loops.

Meanwhile, investment in the *people* element, namely tools for managing behavioral propensities and culture, has significantly lagged. Without this behavioral context, interventions based on systems and processes tend to be heavily rules-based, primarily target visible activities and processes, and therefore risk becoming simple tick-box exercises. Further, by focusing on outcomes rather than on the behavioral proclivities that lead to misconduct, these tools are hopelessly backward looking and require near universal compliance in order to provide adequate assurance.

Operational Risk Management Frameworks (ORMFs) modeled on the 3 Lines of Defense ('3LoD') are similarly affected. Banks have implemented complex reporting systems and detailed processes to manage these frameworks. Yet the success of the 3LoD framework depends entirely upon a complex web of interactions and critical behaviors among senior executives and risk management specialists in order to function effectively. As a result, banks have spent billions of dollars implementing such frameworks, only to realize they must spend billions more in order to effectively *embed* these frameworks into the culture of their organization.

Unfortunately, tools like online surveys and townhall meetings struggle to handle such complexity. Failing to contemplate this, the current standard approach to non-financial risk management is not sufficiently "fit for purpose," as is evidenced by continual bank misconduct scandals.

As the BCBS acknowledges in this consultation document, an effective approach to operational risk will incorporate all of the significant financial and operational factors that represent a bank's risk management practices. Whereas other financial-related risk controls can be supported by metrics and models, the capabilities of the Board of Directors and senior management remain largely subjective and imprecise. As a result, firms have difficulty knowing whether the systems and processes they've implemented are sufficient. It is also far more difficult to benchmark performance in these areas against peers through horizontal reviews. Furthermore, this opens regulators up to potential criticism when apparent inconsistencies between operations and assessments crop up.

WHAT'S MISSING

Regulators and firms have prioritized processes and systems for internal risk governance (and guarding against external threats such as those in cybersecurity). They have been far less inclined to address the people element – namely how to foster the necessary behaviors and cultural norms required to manage those systems and processes correctly. It is not enough to adopt cutting-edge controls and surveillance technologies. Senior management must also foster a culture that encourages staff to demonstrate accountability and to escalate problems. Unfortunately, this is an area where many firms fall short.

This is understandable because, for a long time, the tools available for measuring and managing behavior have not lent themselves to effective supervision. Banks have been forced to rely on tools such as staff surveys, townhall meetings, self-reported behavior journals, and online ethics training. These tools lack objectivity, specificity, and real-time responsiveness. And – when these measures fail – the fallback is to rely upon surveillance and monitoring systems. Such instruments produce enormous 'false-positive' signals which result in added expense as risk examiners are required to run each to ground. And, when successful in identifying an actual risk management failure, awareness of such is too little / too late.

One of the more significant remedies to emerge from the 2011 revision of the PSMOR was to focus on compensation systems. In the current revision, although the language is similar, we believe it is a positive step to more clearly emphasize the compensation component by breaking out in its own paragraph 16 the statement that "Compensation should be aligned to the bank's statement of risk appetite…." Here too, however, we must point out that as a means of addressing the *people* element of operational risk, relying on compensation schemes faces limitations.

Revised compensation frameworks including multi-year evaluation thresholds, deferrals, and even clawbacks certainly can help to align the mismatch between current income and potential longer tail risk realization periods. In that sense they can help address risks that carry over multiple years. Nonetheless, just as with other controls and penalties, changing incentives will fail if the individual believes, as most people do, that they are unlikely to get caught. Compensation adjustment for tail risks necessarily must be done ex post as it would be inappropriate for people to be compensated for inappropriate risk taking. But as a preventative measure, the only way to properly address misconduct is to embed a risk culture.

The foregoing challenges are all the more relevant in the current COVID-19 pandemic. Controls and surveillance systems that were established in a time when everyone worked together have been upended. Further, the most effective protection is provided by a culture that encourages challenge and speak-up behavior, and where staff feels able and encouraged to push back the moment that risk behaviors threaten to take hold.

In a work-from-home environment, this too has been severely weakened. During a recent interview with *Bloomberg*, Gary Cohn, past-COO of Goldman Sachs and advisor to Starling, was quoted as saying: "Banks need people to be working together in a cooperative fashion and watching and listening to each other," adding, "That is what the Fed would call a first line of defense: overhearing conversations, looking at presentations, or looking at the way you talk to a client. […] When people are sitting in their bedrooms, there is no one there to look over their shoulder."[2]

With traditional tools for managing behavior and culture proving inadequate, and given the added pressures stemming from the COVID-19 pandemic, we would urge the BCBS to consider incorporating innovation and investments to apply new behavioral metrics to the challenge of governance and operational risk management.

---

[2] https://www.bloomberg.com/opinion/articles/2020-07-08/covid-19-pandemic-is-a-great-incubator-for-financial-fraud?sref=GNTXiFne

THE SOLUTION

Advances in machine learning have made it possible to process vast troves of internal bank data at scale. By applying novel approaches in the field of "computational social science," it is now possible to detect signals within those massive data sets that tie to particular behaviors of interest to management and supervisors. This may be behaviors that represent a predilection for misconduct or, equally, behaviors that are necessary to enable critical non-financial risk management systems and processes. Furthermore, by incorporating network science, it becomes possible to determine the key influencers of such behavior.

Analyzing these signals leads to metrics that update continuously and reveal where specific behavioral propensities are likely to appear. Through use of these *predictive behavioral analytics*, a new generation of management tools can illuminate the pathways by which certain behaviors are most likely to spread – contagion-like – throughout an organization. Such 'behavioral epidemiology' positions management to operate from the front-foot. It also allows precision targeting of audit activities and risk management interventions, enabling firms and supervisors to scale their risk oversight and to act in a more timely, effective, and efficient manner.

To illustrate one example of this, Principle 5 emphasizes the importance of a "robust governance structure." The first subpoint thereunder in paragraph 22 is that "Senior management is responsible for establishing and maintaining <u>robust challenge mechanisms</u> and effective issue-resolution processes." (emphasis added). The BCBS goes on to emphasize formal implementation of the framework and supporting processes – all of which can be documented or viewed on a static basis. What is far more challenging is to measure the *informal organization* and whether the framework is fit for purpose and has been embedded and lived in daily operations, including through risk events. It is only through measuring the informal organization that a governance structure can be considered "robust." This "robust challenge mechanisms" language was introduced in the 2011 revisions; the modern approaches and tools we are describing now give us the possibility to actually implement it.

A significant additional benefit is to be had once such technologies are established as industry-standard best practice: standardized risk metrics such as those we describe here may permit for horizontal reviews on an apples-to-apples basis, system-wide, across any given jurisdictional space. And the adoption of such metrics among regulators in other financial markets may permit for more efficient collaborative oversight of firms with an extensive global footprint. (e.g., the G-SIBs)

RECOMMENDATION

Advances in behavioral science and advanced analytics, principally machine learning, are now enabling new tools that generate real-time metrics that allow for proactive assessment of management and board oversight, effectiveness of audit and compliance systems and processes, and proactive identification and mitigation of non-financial risk.

On behalf of Starling, we suggest the BCBS should actively encourage boards and senior management teams to invest in technology to efficiently embed the principles into their organizations.

Specifically, Principles 1 and 2 reference the need to embed an effective *corporate culture* and *ORMF* respectively. Larger firms in particular will struggle to do so without leveraging technology that can detect and measure behaviors of interest at scale. Likewise, we believe that the remedies offered in

Principle 5 related to hiring experts (paragraph 31) and implementing a governance committee structure paragraph 32) will be more likely to fall short of expectations if they fail to make use of these new tools.

We would also urge the committee to reference such technologies as part of Principle 5 to support a strong control environment. In particular, these tools can support the kinds of monitoring of control assignments and processes as described in paragraphs 47 and 49.

Finally, banks have suffered severe reputational damage following from the financial crisis and through ongoing scandals that have occurred since. This highlights a need for boards and senior management to evidence to investors and other stakeholders that the principles incorporated into the Revised PMSOR have not only been adopted, but have been effectively embedded into their organizations. The BCBS should consider adding tools that incorporate predictive behavioral analytics as a category of solutions as part of Principle 6 paragraph 34. Likewise, as adoption of these technologies increases, these results should ultimately become part of a firm's regular disclosures to stakeholders as described in Principle 12.