BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

"Risks are by their very nature dynamic, fluid, and highly interdependent. As such, they cannot be broken into separate components and managed independently. Enterprises operating in today's volatile environment require a much more integrated approach to managing their portfolio of risks."
J.Lam, Enterprise Risk Management: From Incentives to Controls, Second Edition, p.51

August 31, 2022

Overcoming Organizational Silos in the Risk Management Arena

By Andrew H. Moyad

Today's supercharged business risk landscape demands that boards embed an integrated risk management approach into the firms they oversee, breaking through harmful, often long standing, internal silos. Organization and culture change starts at the top, and boards have a clear obligation to lead the charge reinvigorating today's all-too-frequently siloed risk management programs.

Absent a regular, focused process of effective challenge at and below the board level, organizational inertia routinely obscures strategic opportunities for holistic enterprise risk management (ERM) and leaves a firm mired in multiple tactical risk management programs that fail to function in an integrated manner. While seemingly harmless over many months or even years, these risk management silos increasingly expose an organization to a range of emerging, cascading risks that the firm is unable to address.

A range of opportunities is available to identify and correct these organizational deficiencies, including cross-functional recovery testing, tabletop exercises scoped and managed by independent parties, and explicit obligations for combined, multi-function resource sharing and risk reporting. In combination, these are the hallmarks of a truly comprehensive, organic risk culture (and not merely an academic, often pointless, set of risk activities) that enables an organization to respond and adjust to a dynamically changing risk landscape.

DISASTER RECOVERY EXERCISES: ARE WE TRULY STRESS TESTING?

Far too many organizations conduct no meaningful form of regular disaster recovery (systems and technology infrastructure) or business continuity (human resource) exercises. When conducted thoughtfully, these exercises routinely identify gaps in business continuity plans, disaster communications protocols, and system recovery capabilities. However, many organizations dilute the value of these exercises by providing extended advance notice and conducting tests under very constrained, staged circumstances that fail to stress actual operational resilience.

Disaster recovery tests should be designed to find and correct gaps in a real learning exercise. However, when tests yield an easy pass, an illusory mirage of operational resilience results. Accordingly, boards should look for indications that resilience testing is truly rigorous, and lead to learning and improvement. For a board, reviewing the details of such tests often reveals far more about the organization's risk culture than what is written in hundreds or thousands of pages of policies, procedures, or operating manuals. A true, collaborative learning culture that values meaningful ERM practices ultimately accepts (and even encourages) the benefits of learning from failure as an equal and often superior alternative to learning from success.

To give one example of a lost risk management opportunity, the author participated in a regional business continuity test for a global financial services firm that required all participants within two driving hours of the headquarters to travel to an alternative workplace equipped with backup generators. The test was designed to assess the firm's ability to operate trading systems during a regional power outage. Ironically, heavy rains the morning of the test forced a six-hour delay. In fact, the designated alternative site was located in a coastal flood zone that routinely inundated during storms. Hours later, when the roads cleared and the test finally started, the business was granted a passing grade for meeting the two-hour recovery time objective (RTO), even as the test window was moved six hours.

Importantly, the real lesson learned was that data centers and alternative work locations in coastal flood zones are a poor choice, but this essential insight was omitted from the final, published results, and the test was declared a success (a failed grade would have required a repeat test). Remarkably, the Compliance, Cyber, and Third Party Risk Management (TPRM) teams had no authority to change the test plan or final results, and all of these units considered the test a failure. All were overruled because senior business leadership did not want to lose another Saturday to re-test. Neither the firm's ERM function nor the Board was made aware of those details. Nothing about the program changed, and there was no point made about the poor location or conditions of the recovery site. The combined voices of the organization's risk silos were ignored, and the firm lost a major opportunity to improve its recovery options.

What Boards Should Do:

- Take a page from the compliance and cyber playbook: expect management to conduct resilience and other risk event testing in ways designed to identify real program weaknesses, not tolerate carefully staged tests rigged for an easy pass;
- Require cross-functional risk functions to participate in and exercise authority with business continuity planning, test design, and establishing success criteria;
- Hold your applause if management boasts a recurring pattern of successful resilience and other risk stress testing without material changes to ERM program design or operations; and
- Demand that all ERM or other risk functions document their respective "lessons learned" from test results; do not allow business units alone to dictate or to report findings.

STRUCTURING THE RIGHT TABLE TOP EXERCISES: FINDING BIASES AND BLIND SPOTS

Unlike various forms of physical or technological stress testing, well-structured table top exercises allow organizational leaders to talk through a range of evolving risk scenarios that provide meaningful opportunities to collaborate and to build trust. Such scenarios are routinely scripted but, importantly, provide participants no advance notice about the test details. The exercises can be structured to expose functional misalignment or imbalances in organizational power that could affect an organization's success when managing a real emergency.

The author participated in an exceptional table top exercise with a large financial services company that was organized by the business continuity team (BCT). The exercise included business leadership, physical security, cyber, and third party risk management (TPRM) professionals. The business continuity team, however, did not participate. As we learned that day, the test assumption was that the business continuity team was attending on offsite and had lost communication with the firm. As a result, business leadership was given exclusive authority to decide whether employees stayed on the trading floor or were sent home during a simulated hurricane approaching New York City on a trading day. Since the fabricated hurricane started at a lower category and was slow moving, business management wanted to send employees home only when absolutely necessary, in part with the knowledge of the calculated financial losses from an interrupted trading day.

Despite the protestations of the physical security, cyber, and other risk teams as the exercise progressed, the business leadership team kept people at their desks with each simulated hourly update (provided about 5-10 minutes apart to discuss their evolving assessment of the risks).

By design, the business continuity team provided no feedback during the exercise and only disclosed the changing storm conditions. By the time business leadership finally made the decision to send staff home, subways and major roads were closed, the projected hurricane landfall accelerated by several hours at higher wind speeds, and the majority of the workforce was trapped inside the building. While the published result of the exercise was a failure (the organization did not protect staff above all other considerations), it was a significant, humbling lesson for business leadership. The test reinforced the actual business continuity team governance process that authorized their function to declare an emergency without business consent under potentially disastrous conditions.

Questions Boards Should Consider:

- Does management / ERM sponsor regular table top exercises (e.g., semi-annually) and report the results to the board?;
- Do these exercises require cross-functional risk team collaboration and participation?;
- To avoid internal organizational bias, are table top exercises ever designed and managed by independent parties that report their results directly to the board?; and
- Which people or functions are authorized to declare a disaster or other major event? Do these processes rely entirely on senior business leadership?
- Is enterprise risk management or another function authorized to intervene where human health or safety are at risk?

CAN WE CREATE ANTIFRAGILE ORGANIZATIONS?

"It is far easier to figure out if something is fragile than to predict the occurrence of an event that may harm it. Fragility can be measured; risk is not measurable (outside of casinos or the minds of people who call themselves 'risk experts.'). This provides a solution to…the Black Swan problem – the impossibility of calculating the risks of consequential rare events and predicting their occurrence….Crucially, if antifragility is the property of all those natural (and complex) systems that have survived, depriving these systems of volatility, randomness, and stressors will harm them." (N.N. Taleb, Antifragile: Things That Gain From Disorder, Prologue.)

In his *Black Swan* follow up work *Antifragile* (2012), N. N. Taleb argued that the acceptance of regular, unpredictable, and improbable events is the essential first step to creating systems and organizations that

reduce their own fragility. He wrote that allowing any organization to experience stressors and learn from them should reduce that organization's fragility and improve its prospects during risk events. In short, antifragile firms are more likely to thrive, not stagnate or wither.

How can a board assess the fragility of the organization it oversees? Arguably, an organization that adopts, tests, and reports on the following measures to its board moves towards antifragility, while an organization that performs only a few or none of these or similar tasks is potentially fragile and warrants the attention of its board.

Questions Boards Should Ask To Assess Fragility:

- Has management or the ERM program identified the most significant internal and external exposures that place the organization at greatest risk, whether current or emerging? Is there a dynamic "Top 10" or another list of risks that the organization regularly assesses and updates to evaluate the firm's fragility?
- Do strategic business plans include a corresponding evaluation of market and other operational risks (e.g., third party) that could undermine or prevent successful outcomes?
- If it exists, does the enterprise risk management function directly evaluate and comment on the potential risks to strategic business plans and provide recommendations on how best to address them?
- Has the organization expressed a clear risk appetite and risk tolerances based on both business and ERM feedback?
- Does the ERM program regularly report the details of relevant risk programs in an integrated format that includes measures of cross-functional risk team collaboration with the business?

ABOUT THE AUTHOR

Andrew H. Moyad
CEO, Shared Assessments

Andrew Moyad is the Chief Executive Officer of Shared Assessments. He has more than 25 years of leadership roles in risk management, information security, and procurement. Prior to joining Shared Assessments in 2022, he served as Senior Vice President, Vendor Risk Management at Blackstone, where he led a team of risk professionals responsible for overseeing all phases of the vendor lifecycle at the firm, including risk assessments, control diligence, contract reviews, financial checks, performance monitoring, issue tracking, and management reporting. Prior to Blackstone, he served as a Director and Global Head of Vendor Risk Management at BlackRock, and before that he was Senior Vice President for Citigroup, working as a Business Information Security Officer in Global Fixed Income and led onsite third party risk assessments for the business globally.

UPCOMING EVENT - Tuesday, September 20, 2022

Featuring Jo Ann Barefoot (Author of the June 2022 Board Risk Report)

The Future of Cryptocurrency and Blockchains in the U.S.
Navigating risks with a clear eye to the opportunities
Tuesday, September 20, 2022
1:00 pm - 2:00 pm ET
Virtual Event (Zoom)
CLICK HERE TO REGISTER

Panelists:

- **Jo Ann Barefoot**, CEO & Cofounder of the Alliance for Innovative Regulation, host of the global podcast show Barefoot Innovation, and Senior Fellow Emerita at the Harvard University Kennedy School Center for Business & Government
- **Soups Ranjan**, CEO/Co-Founder, Sardine AI

Moderator:

- **Charlie Miller**, Senior Advisor, Shared Assessments

Cryptocurrencies are much in the news, with recent failures and plummeting values sparking doubts about their future. While they have existed for well over a decade, we are still in the early days of analyzing and debating their benefits, risks and likely impacts, as well as how they should be regulated. Corporate boards need to consider whether and how to get involved in this dynamic space.

Join the Board Risk Committee for this virtual event featuring Jo Ann Barefoot and Soups Ranjan. The 1-hour webinar will be based on Jo Ann Barefoot's June 2022 *Board Risk Report* (click here to access the report). The webinar will be an opportunity to hear a discussion of key points from the report and take a deeper dive into selected concepts. Attendees will be able to ask the panelists questions in the final 15-minutes of the webinar (via typing into the chat function in the zoom platform).

***The Board Risk Report** is the periodic publication of the BRC. **SUBSCRIBE NOW** to receive complimentary world-class risk management practices delivered directly to your inbox.*

WHO WE ARE

The Board Risk Committee (BRC) is the foremost thought leadership peer council for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC is affiliated with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

Contact:
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org