Risk Governance:

EVOLUTION IN BEST PRACTICES FOR BOARDS

Author: Sheila Judd, Executive-in-Residence, Global Risk Institute

GLOBAL RISK INSTITUTE

The author is an independent contributor to the Global Risk Institute and is solely responsible for the content of the article.

Since the 2008 financial crisis, the role of the board has expanded and expectations for performance have increased. Directors are to guide development of strategy and risk appetite and oversee risk taking activities in the short and longer term, digest extensive reporting packages covering all facets of the firm's operations, root out areas where risk taking may be out of line with risk appetite, provide effective challenge of senior management's assessments of risk and action plans, and more.

To do all that effectively is challenging. The right structure, the right people and the right information flow provide the foundation for an effective board.

There is, however, no "one size fits all" or static solution. The right mix of people will change over time as strategy and risks evolve. For example, expertise in technology, cyber risk and climate science have become increasingly important. In addition, directors will need to continually determine the right level of, and areas for, constructive challenge. Too much probing could create an environment of mistrust and too much discussion on less important matters could detract from time available for key issues. The right volume and depth of reporting to deal with the inherent information imbalance between directors and senior management will also be dynamic.

Boards must also keep up with evolving best practices. We recommend that boards give consideration to their approaches to strategic risk, longer term thinking, corporate culture, crisis management, and technology risks to ensure they provide robust oversight in these important areas.

ABSTRACT

Banks and their regulators learned a lot from the 2008 global financial crisis. As a result, there have been significant changes in how financial institutions assess and manage risks, and in regulatory expectations.

The changes have not been confined to the risk management function: the role of the business as the "first line of defense" is now widely accepted, and boards play a more active role in overseeing risk taking activities. **At the Global Risk Institute (GRI), we emphasize that the most important role of the board is risk management.**

The adoption of enhanced risk management and governance practices has not been limited to the banking sector. Other financial firms as well as non-financial firms and governments have been applying some of the key learnings, including strengthening board membership and engagement.

Many firms are now transitioning from building their enhanced structures and practices to improving their effectiveness. Regulators are also refining their requirements. Specific to risk governance, in 2017 Canada's

Office of the Superintendent of Financial Institutions and the U.S. Federal Reserve each issued draft guidance to clarify the supervisory expectations for the role of boards.

Drawing from the regulatory guidance across major jurisdictions, along with the lessons that can be learned from recent examples of risk governance failures (two prime examples are Wells Fargo and Volkswagen), we have developed a "formula" to help firms implement enhanced risk governance practices.

A word of caution: our formula appears deceptively simple. We raise some of the many complexities in our commentary that follows, and further note that our formula is not intended to be the definitive answer for effective governance. Rather, it serves as a foundation to support robust discussion and more informed decision making.

THE RIGHT PEOPLE + **THE RIGHT STRUCTURE** + **THE RIGHT INFORMATION**

= **More robust discussion, with consideration of various perspectives, leading to more informed decision making**

We have also identified five areas where boards should examine their risk oversight:

Strategic risk:
Approval of strategy is a key role of the board, as is approval of a firm's risk appetite. Boards could improve their understanding and consideration of risk implications of strategic choices in both the near and longer term, better integrating the decisions made in the pursuit of earnings with the assessment of downside risks.

Longer term thinking:
Boards should ensure sufficient focus on identifying, assessing and planning for risks and trends that could impact longer term sustainability. Consequences of poor direction in this area can include missed opportunities, losses or in the extreme, corporate failure.

Corporate culture:
Boards should ensure that the firm's desired culture, including expectations for managing risk, is well defined, and embraced throughout the firm. Compensation systems should reinforce desired behaviours, balancing management of goals with management of culture.

Crisis management:
Boards should ensure management have developed a robust crisis management plan that includes stakeholder communication strategies. Senior leaders responsible for plan implementation should be trained, and the plan should be tested and kept up to date.

Technology risks:
Technology is an increasingly important and multi-faceted area of risk, comprising operational risks associated with system performance, cyber security risks, and risks to the business model arising from technological advancements. In addition, large scale technology projects involve a high degree of risk. Boards need to ensure they have the expertise to provide effective oversight.

INTRODUCTION

Risk taking is inherent in the activities of financial institutions; it is a necessary part of their business. It seems logical, therefore, for financial institutions and their boards to consider risk management as a key priority, if not the key priority, for running a successful financial institution. Yet the financial crisis of 2008 uncovered significant shortcomings in risk management at some firms and how boards of directors oversaw risk-taking activities.

- *Many boards were short on directors with financial industry experience generally, and risk management expertise more specifically.*
- *Information provided to the boards did not adequately identify and quantify risk, and risk tolerance had not been adequately articulated.*
- *Independence was an issue at some firms, where relationships existed among board members and / or with management such that management actions, or recommendations, were not subject to effective discussion and debate.*
- *Some firms had cultures and compensation structures that encouraged and rewarded excessive risk taking.*
- *The risk function was not always given adequate stature, respect and authority, and in some cases the risk function was not independent from the revenue generating business areas.*

As a result of such weaknesses, some firms failed to understand the level and complexity of the risks taken on.

In the wake of the financial crisis, both risk management and risk governance practices have been in the spotlight: international bodies such as the Organization for Economic Co-operation and Development, the Financial Stability Board, the European Commission, and the Senior Supervisors Group have each published reports on lessons learned [1]; and major regulators around the world have published new or updated guidance to improve both risk management and risk governance practices. [2]

Despite the increased regulatory guidance, we continue to see unacceptable behavior within some firms in the financial services industry and in other industries as well, raising questions as to how to continue to improve the effectiveness of the boards in overseeing how companies operate.

1 *A full list of publication references can be found at the end of this article.*

2 *A full list of the primary regulatory guidance used for this paper is provided at the end of this article.*

DEFINING RISK GOVERNANCE

In its publication, Risk Taking: A Corporate Governance Perspective, the International Finance Corporation (IFC) of the World Bank notes that there is no consensus definition for risk governance. The IFC defines it as “the ways in which directors authorize, optimize, and monitor risk taking in an enterprise”; the IFC also states that it “includes the skills, infrastructure (i.e., organization structure, controls and information systems), and culture deployed as directors exercise their oversight.”

LESSONS LEARNED

REGULATORY ENHANCEMENTS

Regulators responded to the financial crisis with new or updated guidance, laying the foundation for more effective oversight of risk. The scope of regulatory guidance varies: some incorporate governance into broader documents; some focus on general governance principles, not just risk governance; some focus on governance by the board whereas others include management; some provide a lot of detail while others are higher level only. Notwithstanding these differences, there are many commonalities:

- *Most regulators offer similar guidance on board structure, composition and independence, with the goal being for boards to be able to understand, and exercise independent objective judgment about, the risks the firm is taking or planning to take.*
- *Most set out the board's role regarding risk appetite, risk culture and compensation, with a view to setting limits on the amount and type of risks deemed appropriate in pursing the firm's strategic goals, and defining and reinforcing the risk taking behaviours that are, or are not, acceptable.*

The Appendix to this document provides a summary of the various regulatory guidance documents, highlighting where some regulators have been more explicit, or have taken unique positions.

Most financial firms have made changes to align with the regulatory expectations. However, as noted by the Senior Supervisors Group:

> *"Many changes that firms have undertaken are organizational and appear to have been relatively easy to implement. Less clear is whether these organizational changes will – without further effort – improve future governance practices."*[3]

A similar observation was made by the OECD in their February 2010 report[4], wherein it was noted that implementation of governance standards may have been implemented more in form than content, reflecting a "tick the box" approach.

These early responses indicate that firms need to move beyond laying the foundation of enhanced structures and practices in order to be effective.

Supporting the transition from "build" mode to "enhance effectiveness", two regulators issued draft guidance in 2017 with a view to refining requirements.[5] The Office of the Superintendent of Financial Institutions (OSFI) guidance, which is an update to its 2013 Governance Guideline, follows its review of the expectations for boards, which was intended to "ensure that OSFI's guidance continues to reflect evolving governance standards and enables boards to focus on key risks and execute their oversight roles efficiently".[6] The revised OSFI guidance is clearer as to board vs. management responsibilities. It also adds culture to the board responsibilities, including oversight of codes of ethics and conduct.

The U.S. Federal Reserve (Fed) guidance follows its multi-year review of practices of boards of banking organizations which identified a need for greater clarity in expectations for boards (vs. management) to ensure boards focus on their core responsibilities, as well as a need to actively manage information flow to overcome challenges associated with volume and complexity of information.[7]

3 *"Risk Management Lessons Learned from the Global Banking Crisis of 2008", Senior Supervisors Group, October 2009.*

4 *Corporate Governance and the Financial Crisis – Conclusions and emerging good practices to enhance implementation of the Principles", Organization for Economic Cooperation and Development, February 24, 2010*

5 *The OSFI draft, which is an update to OSFI's 2013 guidance, was issued on November 7, 2017 and was open for comments until December 22, 2017. The Fed's guidance, issued August 9, 2017 and open for comment until October 10, 2017, is net new.*

6 *Government of Canada, "Proposals for a more focused and effective approach to governance of Canadian financial institutions" News Release Nov. 2017*

7 *Federal Register / Vol. 82, No. 152 / Wednesday, August 9, 2017*

WHERE LESSONS HAVE NOT BEEN LEARNED

In addition to reviewing the lessons learned about risk governance from the financial crisis as documented by bank regulators, we looked at a variety of missteps that have occurred more recently.

Wells Fargo's scandal around its aggressive sales practices is a prime example of ineffective governance.

In the fall of 2016, Wells Fargo admitted that its employees had opened more than two million bank accounts or credit cards without customer consent and authorization. The bank had set extremely aggressive sales targets for the employees, with an incentive program encouraging more cross-selling. The scandal proved very costly, with a fine of $185 million and an agreement to pay $110 million in compensation to affected customers. The scandal also pushed the CEO, John Stumpf, to resign and forfeit $41 million in share compensation, one of the largest clawbacks of CEO pay in the financial industry.

The board's oversight of the bank's activities has been called into question. In a July 2017 letter to Federal Reserve Chair Janet Yellen, U.S Senator Elizabeth Warren stated:

> *"The Board did nothing to stop rampant misconduct in the Community Bank that resulted in more than 5000 bank employees creating more than two million fake accounts over four years."* [8]

On February 2, 2018, the Federal Reserve Board announced its enforcement action, restricting growth of the firm until it sufficiently improves its governance and risk management processes, including strengthening the effectiveness of oversight by its board of directors. The Fed sent letters to each of the firm's board members to emphasize the need to improve director oversight of the firm, noting that, during the period of compliance breakdowns, they did not meet supervisory expectations.

Concurrently with the Fed's enforcement action, Wells Fargo will be replacing four of its board members. [9]

Notably, the board appeared to have the necessary experience and skills as well as diversity: the board included top corporate executives, former high-ranking U.S. government officials, an accounting expert and an academic, with diversity in gender (40% women) and ethnic background. [10]

In our experience, boards would never overtly approve any illegal or improper activity. So why did the firm behave as it did? One could question whether the board members failed to comprehend their stewardship role, or whether they believed that the behaviours were in fact not material, or whether they were willing to compromise on controls and compliance in favour of aggressively pursuing growth.

Perhaps the fact that the CEO was also the Board Chair resulted in less transparency and discussion around risks, with directors less likely to probe management to root out potential issues as a result of the dual role. Perhaps they did not think to question the company's aggressive sales targets or consider how the firm was able to materially outperform its peers.

8 *Business Insider, 'The Federal Reserve has done nothing', (2017)*

9 *Federal Reserve System, "Responding to widespread consumer abuses and compliance breakdowns" (2018)*

10 *New York Times, "By Taking Back Money, Wells Fargo's Board Seems to Recall Its Role" (sept 2016)*

Other examples that made headline news [11] raise questions as to whether board members were willing and able to meaningfully engage in their governance role vs. a "form over substance" board. In some cases it appeared that directors were not sufficiently independent so that they could (and would) effectively challenge management recommendations and decisions. In others, it appeared that the board did not understand the business' operations and the fundamental operating risks.

The examples emphasize the importance of:

- *having a strong, independent and engaged board with directors that understand and take seriously their stewardship role. Strong credentials are not enough.*
- *having directors that understand how the business is achieving its goals, particularly when they are aggressive, and where firms have vulnerabilities due to risk / return trade-off decisions.*
- *having directors that understand fundamental operating risks, such as technology risks, and are tuned in to the potential vulnerabilities in managing them.*
- *having directors that know how to guide management during times of crises, whether internally or externally created. Cyber threats in particular are increasing in frequency and severity and all firms are vulnerable.*

11 *Examples include Home Capital, Volkswagen, Carillion PLC and Equifax*

"FORMULA" FOR BOARD EFFECTIVENESS

Taking into consideration the guidance from regulators and our observations from the examples of risk governance failings, we conclude that for boards to be effective, all members need to make a conscious and deliberate effort to understand and fulfill their obligations.

Directors must be vigilant, diligent and persistent in their approach to risk identification and assessment. They must foster a collaborative, mutually respectful environment with management so that risks, and management recommendations, can be discussed openly in order to recognize vulnerabilities, assess risk/return trade-offs, and guide management under both "business as usual" and crisis conditions.

The **right people, structure and information** are the key elements for effective oversight. Our "formula" for effective governance is illustrated below, followed by our perspective on each of the three key elements, including complexities and dynamics that must be considered.

THE RIGHT PEOPLE

Fundamental to achieving effective oversight is having the right people.

The **right people** will:

- *bring a mix of skills and experience as well as perspectives to drive a thoughtful assessment and discussion around strategy and risk;*
- *be aware of and knowledgeable about the challenges, as well as the emerging risks and trends, affecting the industry;*
- *take their stewardship role seriously. They will be well prepared for meetings, having reviewing reporting with an eye for any areas of concern that may or may not be identified;*
- *be open to providing, hearing and considering different points of view;*
- *be constructive in their tone and approach, recognizing that questioning management, or expressing disagreement, can come across as doubting their capabilities which can lead to a defensive, counterproductive reaction; and*
- *be free of any relationships that could create a conflict of interest.*

THE RIGHT PEOPLE
Mix of skills and expereince;
Diversity of perspectives;
Engaged, Collabortive, Respectful;
No conflicts of interest

+

THE RIGHT STRUCTURE
Roles clearly defined and explicitly acknowledged;
Directors held accountable for performance

+

THE RIGHT INFORMATION
Unbiased, timely, accurate;
Summary Report focusing on top and developing risks, conclusions and action plans;
Areas for discussion clearly indentified

=

More robust discussion, with consideration of various perspectives, leading to more informed decision making

Consistent across the body of regulatory guidance was the requirement for directors to have relevant and up to date experience in the firm's significant business operations and expertise in areas of material risk exposure. We would add that it is particularly important for the board mix to include expertise in areas of new or emerging risks, and to enhance coverage of developing/escalating risks. Guidance on identifying, assessing and managing new, emerging or growing risks could help the firm avoid unnecessary missteps.

As an example, many boards of financial institutions have responded to increasing technology risks by enhancing board of director competency requirements in this area. It is important to recognize that expertise for all technological risk areas, such as operational risks associated with systems, cyber security risks and risks associated with technological change, may not be held by one individual.

Where boards have gaps in their understanding of existing or developing risks, they should seek out independent experts for "teach-ins" or advice. Director education sessions, provided by management or third parties, into areas of significant risk or complexity, may be appropriate to facilitate a more detailed understanding, particularly where a firm's practices, or risk levels, are changing.

In addition to experience and expertise, diversity of perspectives is also important to facilitate thorough and robust discussions. Looking at opportunities, challenges or information through different lenses will reduce the potential for "group think" and "confirmation bias". [12]

GROUPTHINK:

The practice of thinking or making decisions as a group, resulting typically in unchallenged, poor-quality decision-making.

CONFIRMATION BIAS:

The tendency to interpret new evidence as confirmation of one's existing beliefs or theories.

12 *Definitions are from Webster's Dictionary.*

Diversity regarding gender has been receiving a lot of attention, and for good reason: studies show that firms with women on boards perform better financially. [13] Diversity should be considered in a broader sense, consistent with the view put forward by the IFC in its "*Standards on Risk Governance in Financial Institutions*":

> *"It is also believed that representation of different social, cultural and educational backgrounds among directors can contribute to a more complete understanding of the different environments in which the bank operates."*

Another important factor is independence. Directors must be free from relationships (with the firm, its management, or each other) that could compromise their ability and/or willingness to question management, or offer a differing perspective. As stated by the IFC:

> *"The avoidance of any form of conflict of interest is an absolute requirement of sound risk governance. A well-developed process of assessment should be in place for new board members, executives, and employees, including standard disclosures and signed statements of compliance."*

Tenure of directors should also provide a mix of "new" and "old". While long standing directors will develop relationships and trust with management that will facilitate collaboration, this may detract from their ability to critically evaluate management's opinions and recommendations. Newer directors may be more objective, and also be able to ask questions about the company's practices without appearing to be challenging them, simply because they are new to the board.

13 *The CS Gender 3000: Women in Senior Management report by Credit Suisse, published in 2015, demonstrates that companies with more women in the boardroom lead to better returns and outperform on the stock market.*

Ensuring the right people are chosen for board positions can be challenging.[14] Competency matrices are commonly used to identify the skillsets and perspectives needed. These should be reassessed in light of business changes and/or changes to the operating environment. Candidate screening through interviews and references does not always translate to an effective "fit" or desired performance. Behavioural assessments can add insight to improve the likelihood of fit.

THE RIGHT STRUCTURE

As set out in the regulatory guidance (and summarized in the Appendix), the right structure includes clarity of roles and responsibilities, typically documented via mandates, as well as clear reporting lines and authorities; it also includes sufficient stature and authority, as well as resourcing, for risk management. Most regulatory guidance stipulates that the chair of the board should not be an executive of the firm.

Our view is that it is important to clearly document, and have directors and senior management explicitly acknowledge, that they are jointly accountable for the corporation's wellbeing and long term viability. They should also share a commitment to pro-actively identify and manage risks for the benefit of the firm and its stakeholders.

This joint accountability and shared commitment sets the foundation for collaboration. Specific language should be incorporated into mandates (and/or job descriptions) for directors as well as senior leaders, and reviewed and acknowledged annually to reinforce this essential role. This recommendation goes beyond what is currently covered in regulatory guidance.

There should also be an explicit, shared understanding between the board and senior management regarding the board's role to constructively challenge management to ensure that risks have been fully identified and considered from a variety of perspectives. This conscious agreement should facilitate more robust discussions, diffusing the potential for active questioning to be perceived as mistrust or lack of confidence. The board's obligation to constructively challenge management should be set out in the board's mandate, and specifically reviewed and reinforced annually in conjunction with mandate updates.

We emphasize that the role and the performance expectations for board members must be clearly defined (with the concepts above incorporated). Further, board members' performance should be regularly assessed against expectations. 360 reviews, incorporating feedback from the chair of the board, other directors and management, can be useful in this regard.

The board should be clear in its role to help management effectively balance risk and reward, noting that this necessitates probing management to understand their motivations, and expressing any concerns. The key is to do so in a respectful, non-confrontational way. Directors should contribute to the dialogue by leveraging their own experience and expertise, explaining the basis for their views.

Having the right people in the roles of board chair, risk committee chair, chief executive officer and chief risk officer is particularly important as these people set and reinforce the expectations for conduct and behaviours. They also lead discussions, set the tone and can encourage questions and robust dialogue. These leaders must consciously establish, communicate, model, recognize and reward the desired behaviours and take prompt action to address undesirable behaviours, creating the right tone for board and senior management interactions, and establishing the foundation for the firm's broader organizational culture.

14 *Having the right people also applies with respect to senior management. In addition to having the necessary job specific competencies, leaders need to be strong communicators. They also need to be open to hearing the views of others, and willing to engage in robust, meaningful dialogue.*

THE RIGHT INFORMATION

It must be recognized that directors are at an inherent disadvantage when it comes to information: they are dependent on senior management to provide the board with the right information to effectively oversee senior management. Further, the director role is not full time, meaning board members have a time disadvantage as well.

The goal is for boards to obtain informative reports that provide an unbiased view on risk levels, both actual and potential, current and developing, to facilitate performance of their stewardship role. The importance of timely, accurate, unbiased, clear and concise information from management is incorporated into most of the regulatory guidance, along with cautions about volume of information.

The right information will clearly identify the most important areas for discussion, as well as any decisions to be made, providing supporting views on vulnerabilities and capabilities as well as risk and return trade-offs.

When reviewing recommendations for material business changes (e.g., acquisitions, divestitures, strategic changes), directors should ensure that management provides sufficient information to assess the associated risks, including the likelihood and impact of potential downside (and upside) scenarios, available risk mitigation strategies, and alternative strategies that were not chosen.

For downside analyses, directors should ask, “what could go wrong, how bad could it get”, keeping in mind that it is human nature to underestimate risks (and complexity) and to overestimate our capability to manage them, and that deteriorating situations may be exacerbated by market conditions. Directors can use their past experiences to help management identify plausible scenarios and realistically assess potential outcomes.

We recommend that reports to the board comprise two key components: an executive brief and supplemental reports. The executive brief will clearly and concisely highlight top risks and trends, along with management’s conclusions and action plans and supporting rationale. It will not merely summarize information. The supplemental reports will provide backup information, allowing directors to dive deeper where they deem it appropriate. Additional information should be requested as needed, whether to give directors a deeper understanding, or to substantiate positions expressed by management.

Regular discussions between the risk committee chair and the chief risk officer, as well as the risk committee chair and the chair of the board, are necessary to ensure an appropriate agenda and focus for meetings. Time must be prioritized for the top risks and areas where risk return trade-off decisions are being made.

FIVE AREAS FOR ENHANCING BOARD OVERSIGHT

We have also identified five specific areas where boards could up their oversight: strategic risk, longer term thinking, corporate culture, crisis management and technology risk management. Our key recommendations for each are set out below.

1. Strategic risk

Approval of a firm's business objectives and core strategies to achieve them is a long standing and fundamental role of a board. Explicitly approving a firm's risk appetite was added to the board's role in response to shortcomings identified during the 2008 global financial crisis. The challenge is to thoroughly and effectively integrate risk considerations into strategic decision making to ensure fully informed risk/reward decision making.

Boards could improve their understanding and consideration of risk implications of strategic choices in both the near and longer term, better integrating the decisions made in the pursuit of earnings with the assessment of downside risks.

For example, a potential acquisition is often assessed for its revenue add, operating synergies and resulting bottom line contribution. Ability to integrate organizational cultures, systems and processes are often secondary considerations, and considered "risk free" in that they are seen as manageable. Consider, however, the potential damage if a significant risk event or scandal occurs as a result of a much less rigorous risk and control environment. HSBC's 2012 agreement to pay US$1.92 billion in fines for laundering drug money through a bank it had acquired is a good example.

Increasing risk appetite to facilitate achieving financial objectives that have been put under pressure as a result of a more challenging operating environment should also be carefully considered. Downside risks should be understood, with close monitoring as well as use of key risk indicators to ensure course correction if risks start heading offside.

2. Longer Term Thinking [15]

Our system of quarterly financial reporting means that often companies are more focused on the short term. This is reinforced through markets that emphasize recent performance (as exemplified by share price movements that reflect release of quarterly or annual results. Mandate durations and compensation structures also contribute to a myopic view (e.g., executives that put the company at risk to elevate performance during their tenure rather than taking a longer term view).

Boards should ensure sufficient focus on identifying, assessing and planning for risks and trends that could impact longer term sustainability. Examples where companies faced catastrophic outcomes as a result of failure to effectively adapt to trends, such as the move to digital photography and smartphones and changes in consumer preferences for shopping.

GRI's Global Risks and Trends Framework provides a systematic and robust process for pro-actively identifying and evaluating risks and trends most relevant to the firm's future success.

Discussing emerging risks and trends and evaluating "what if" scenarios will help the firm assess and prepare for different possibilities. Directors can be particularly helpful

15 *This recommendation is not directly tied to the regulatory guidance or lessons learned from the examples cited in this report, but is a result of our research into the governance topic*

in developing plausible scenarios, including identifying correlations and combinations of events that would pose material risk. Asking "What could go wrong" and "How bad could it get" is a good place to start in assessing probability, severity, and timelines.

For plausible threats with material impacts, boards should ask management to establish early warning indicators to trigger reassessment of the risks. Potential mitigation strategies should also be evaluated, including the cost/benefit to taking early action.

3. Corporate Culture

A strong corporate culture can enhance reputation and performance; it can also reduce the potential for undesirable behaviours. Boards should therefore ensure that sufficient attention is paid to corporate culture. As with risk appetite, corporate culture needs to be defined at the top of the house and cascaded throughout the organization. This involves defining what it means for each group. There are guiding principles that apply to everyone, but there are also desired behaviours that need to be more specifically defined at the business or infrastructure unit level.

Firms should emphasize having a fair and ethical culture. A "do the right thing" culture, fostering trust mutual respect, helps attract and retain the right type of employees (and is of particular importance for "millennials") and it minimizes the occurrence of negative incidents that can cause reputational harm. A rules-based approach that emphasizes compliance may be seen as a "check the box" approach, and more rules alone will not necessarily drive desired behaviour.

Ensuring tone and conduct of the people managing front line employees is critical. Middle managers hire and manage the most people, and therefore have a wide sphere of influence. For new hires, firms need to recognize that people bring with them behaviours (good and bad) that were encouraged by their previous employer. Indoctrination of new employees must include training on the firm's culture and behavioural expectations. What managers message to their employees, what expectations they communicate, how they recognize performance and behaviour, and how they deal with their employees' concerns, will affect the firm's culture. Compensation systems need to balance management of goals with management of culture, keeping in mind that "what gets measured gets done".

Corporate culture should be measured and monitored for the organization as a whole, as well as for different geographies and units, recognizing the potential for differences within the firm. In addition to metrics such as employee turnover and other job satisfaction measures, there are ways to use technology to monitor culture, as identified in the GRI white paper, The Secret Life of Culture: Unveiling Culture Risk in the Age of Machine Learning.

4. Crisis Management

Every business will face a crisis at some point. Boards should therefore ensure that management have developed a robust crisis management plan, including a crisis response communication protocol that covers all relevant stakeholders, including regulators, government, the Board of Directors, customers, employees, material suppliers, and the media.

When communicating problems, ensure communication is timely, be forthright and honest, and demonstrate a bias towards action, even when the nature, scope or action plans are not yet clear. Do not attempt to minimize the issue or play down its significance. The full extent of the problem may not be known in the early stages. Admitting to a problem in a timely manner and showing swift action to address it will mitigate the associated reputational damage. Several recent examples show how ineffective communication around a cyber security incident can hurt a company. Arguably, the negative publicity associated with how the company handled the breach, was more damaging than the breach itself.

Senior leaders responsible for plan implementation should be trained, and the plan should be tested and kept up to date.

Boards should oversee management's crisis response: problem identification, investigation, communication and remediation. A follow up review should be conducted post crisis to identify areas for plan enhancement.

5. Technology Risk Management

Technology risks include operational risks associated with system performance, cyber security risks, and risks to the business model arising from technological advancements. In addition, large scale technology projects involve a high degree of risks.

Technology risks have been increasing due to the growing dependence on technology as well as the increasing scale and sophistication of cyber attacks. As a result, technology risk management is a critical area for board oversight.

Cyber security ranks at or near the top of the list of key risks identified by senior leaders. It was the highest ranked risk identified in GRI's annual member survey of risks for both 2017 and 2018. Prevention, detection and response preparation are all important areas for management of security risks. Best practices for cyber security preparedness includes conducting simulation exercises to test out response plans.

It is important to recognize that cyber security risks include both internal and external threats. Employees can unintentionally allow system protections to be breached as a result of poor security habits, including responding to phishing emails. Employees also have access to private customer information as well as material non-public firm information relating to the scope of their work, and "bad actors" can expose the firm to information breaches. Technology risks include associated with use of third parties also need to be considered: directors should assess their firm's approach to initial and ongoing assessment of third party technology controls (prevention and detection controls as well as business continuity plans for outages), as well as contract specifications regarding security incidents.

Oversight of operating risks, such as system maintenance practices, is also important, as exemplified by the Equifax security breach, attributed to the delayed implementation of a security upgrade.

Lastly, recognizing the high degree of risks associated with successful delivery of large technology projects, boards should designate a director, with the requisite skills, to lead oversight of such projects.

RECOMMENDATIONS

The operating environment is becoming increasingly challenging, with new and heightened global risks and trends requiring a more pro-active approach to strategic planning and risk mitigation.

The competitive environment is also more challenging. Technological innovation has and continues to give rise to new entrants and challenges to existing business models; increasing cyber dependence and cyber crime are heightening operating risks. As revenue growth becomes challenged, the focus on cost reductions will intensify. Regulatory expectations are not expected to diminish.

With heightened challenges in the operating environment and to the business model, risk governance will play an increasingly important role. Effective risk governance will reduce risk at the firm level; this will in turn reduce the risks to the financial system.

Below are our top five recommendations for effective risk governance.

1. Emphasize accountability.
Directors must understand their stewardship role and take it seriously. They must be free from relationships or potential conflicts that could impede their judgment or willingness to express their views openly and honestly. Expectations for directors must be made clear, and directors should be subject to regular assessments to ensure they understand and are fulfilling the expectations.

2. Cover all material risks.
Boards need to have sufficient risk expertise to oversee all material risks of the firm. Boards need to understand changes and challenges in the operating environment and ensure they can provide effective oversight of new or evolving risks as well as risks associated with strategic choices. Gaps need to be addressed, bringing in new directors with the appropriate expertise.

3. Foster open and honest dialogue.
Directors need to be collaborative, non-confrontational, and respectful in their tone and approach when probing management to assess their recommendations, and when offering their views and guidance to management. Directors should look out for the "too good to be true" and be aware of the natural bias to underestimate risk and overestimate capabilities.

4. Spend time wisely.
Focus on the most significant risks and issues. Makes sure there is time to have a robust discussion with management regarding action plans and alternatives. Make time for thorough consideration of risks associated with strategic choices, and for forward thinking that gives consideration to risks and trends that could affect longer term viability.

5. Be ready for a crisis.
Whether it's a cyber security breach or a natural disaster, firms should have a communication plan at the ready, in addition to a business recovery plan. Managing a deteriorating situation or stress event is enhanced where options and outcomes have been discussed in advance, without the pressure of the moment.

APPENDIX

Below we provide a summary of the main topics covered in regulatory guidance for risk oversight.

Board Composition and Structure:

Commonly, regulators stipulate that the size of the board and its structure, including whether it should have a dedicated risk committee, should reflect the size of the firm, nature of its business and its risk profile. On whether a bank needs to have a specific risk committee, the Basel Committee on Banking Supervision (BCBS) specifies this is required for systemically important banks. Similarly, the Bank of England's Prudential Regulation Authority (PRA) adds that the potential impact of failure should also be a consideration. Other common requirements include documented mandates specifying roles and responsibilities, plus regular meetings. The U.S. Federal Reserve is alone in specifying quarterly risk committee meetings.

Independence:

Guidance is generally consistent regarding the need for a majority of independent directors, without conflicts of interest, and that the Chair of the Board should not be an executive of the firm. The Office of the Superintendent of Financial Institutions (OSFI) requires all risk committee members be independent.

Director Qualifications:

Regulators agree that directors should have a mix of skills and experience, including industry knowledge and competency in risk management. OSFI states that the risk committee should include individuals with the technical knowledge in risk disciplines that are significant to the firm; OSFI also recommends an annual skills competency evaluation process for directors. The PRA emphasizes being up to date as well as being able to provide effective challenge.

Director Attitudes:

Some regulators go beyond experience and competencies to include director attitudes. The BCBS states that director attitudes should facilitate communication, collaboration and critical thinking. The PRA recommends a culture for the board that is cooperative and collegial and supportive of management, but not inhibiting effective challenge of management decisions and plans. Effective challenge is a recurring theme in the PRA guidance. The U.S.'s Office of the Comptroller of the Currency (OCC) provides the most comprehensive list of attributes for directors, including being willing and able to exercise independent judgment and provide credible challenge to management's decisions and recommendations.

Diversity:

Most regulators recommend that directors collectively bring a variety of skills and experience relating to the firm's business and its risks. The OCC goes further, stating: "Diversity among directors is another important aspect of an effective board. The board should actively seek a diverse pool of candidates, including women and minorities, as well as candidates with diverse knowledge of risk management and internal controls."

Risk Appetite:

All of the regulatory groups state that the board is responsible for establishing risk appetite and strategy and for ensuring alignment; the Board is also responsible for monitoring risk levels in the context of risk appetite. The PRA includes specific reference to board oversight of prospective risks in addition to actual risks. The BCBS includes that risk appetite should take into consideration the long term interests of the firm and the ability to manage risks effectively.

Risk Culture:

Most regulatory guidance includes board responsibility for risk culture, or "tone at the top", reflecting prudent management, risk awareness and ethical behavior. The BCBS adds monitoring of the state of risk culture. The BCBS includes more comprehensive guidance on establishing a code of conduct for ethical behavior, defining what is acceptable and what is not, with infractions to be treated seriously. The OCC specifies that the board should convey its expectations to all employees, with all employees being responsible for operating within the established risk appetite and limits.

Risk Management Function:

Commonly, the risk management function is to be independent of the business, and the responsibility for overseeing the risk management function rests with the board. OSFI stipulates that the board should approve the appointment, performance review and compensation of the CEO and other members of senior management including heads of oversight functions. Both the BSBS and OSFI, as well as the U.S. Federal Reserve, stipulate that the board should ensure the risk management function has sufficient stature and resources. Notably, OSFI also adds that boards should approve the mandates, resources (amount and type) and budgets of oversight functions. The U.S. Federal Reserve stipulates that boards should review the budget, staffing and systems of the risk management group.

Other risk management functions:

Generally, guidance covers the board's role with respect to the overall risk framework, including risk limits, policies, and reporting. Most indicate the board should be responsible for the internal controls framework; compliance management program responsibility is also set out as a board responsibility in the OCC guidance. The OCC also explicitly includes overseeing IT risks and the information security policy.

Compensation:

Regulators have a common view that boards should oversee compensation practices, ensuring alignment with the firm's risk horizon and promoting appropriate risk-taking behaviors and a strong risk culture. The BCBS adds alignment with long term objectives and financial soundness of the firm. The BCBS notes that boards should approve the compensation of senior executives, in particular the CEO and CRO as well as the head of internal audit, while OSFI includes approving the compensation of the CEO as a board responsibility in addition to reviewing the compensation policy for all human resources. The BCBS also notes that firms should have specific provisions for "material risk-takers", i.e., employees with a significant influence on the overall risk profile, that are sensitive to outcomes over a multi-year horizon so that a sufficiently large part of compensation is held back until the risk outcomes are known, and with clawbacks for inappropriate activities or behaviours.

REFERENCES

REGULATORY DOCUMENTS:

i. "Corporate Governance Principles for Banks", Basel Committee on Banking Supervision, 2015

ii. "Enhanced Prudential Standards", The Federal Reserve, 2014

iii. Commercial Bank Examination Manual, Section 5000, The Federal Reserve, updated semi-annually

iv. "Corporate and Risk Governance", Office of the Comptroller of the Currency, 2016

v. "Supervisory Statement of Internal Governance", Prudential Regulation Authority, Bank of England, 2017

vi. "Corporate Governance: Board responsibilities", Prudential Regulation Authority, Bank of England, March 2016

vii. "Guidelines of Corporate Governance", Office of the Superintendent of Financial Institutions Canada, 2013

PUBLICATIONS BY GOVERNANCE BODIES:

i. "Standards on Risk Governance in Financial Institutions", International Finance Corporation, World Bank Group, 2012

ii. "Risk Culture, Risk Governance and Balanced Incentives", International Finance Corporation, World Bank Group, August 2015

iii. "Corporate Governance and the Financial Crisis – Key Findings and Main Messages" OECD, June 2009

iv. "Corporate Governance and the Financial Crisis – Conclusions and emerging good practices to enhance implementation of the Principles" OECD, February 24, 2010

v. "Corporate Governance in Financial Institutions – Lessons to be drawn from the current financial crisis, best practices", European Commission, June 2010

vi. "Thematic Review on Risk Governance", Financial Stability Board, February 12, 2013

vii. "Risk Management Lessons from the Global Banking Crisis of 2008", Senior Supervisors Group, October 21, 2009

viii. "Observations on Risk Management Practices during Recent Market Turbulence", Senior Supervisors Group, March 6, 2008