GUIDING PRINCIPLES FOR BOARD RISK COMMITTEES

November 2018

The Directors and Chief Risk Officers Group
Leaders of the global risk governance community.

the DCRO
Directors and Chief Risk Officers Group

ABOUT THE DIRECTORS AND CHIEF RISK OFFICERS GROUP (THE DCRO)

The DCRO was formed in 2008 to focus on the top-level governance of risk in practice. Bringing together leading board members, chief risk officers, and other c-level officers whose jobs include a fiduciary responsibility for governance and risk management, the DCRO counts more than 2,000 members from large and mid-size for-profit and nonprofit organizations, coming from over 115 countries.

DCRO members participate in facilitated meetings, conference calls, benchmarking research, and governance councils that allow them to compare current practices with those adopted by fellow members, those being required by regulatory bodies, or those expected by investors.

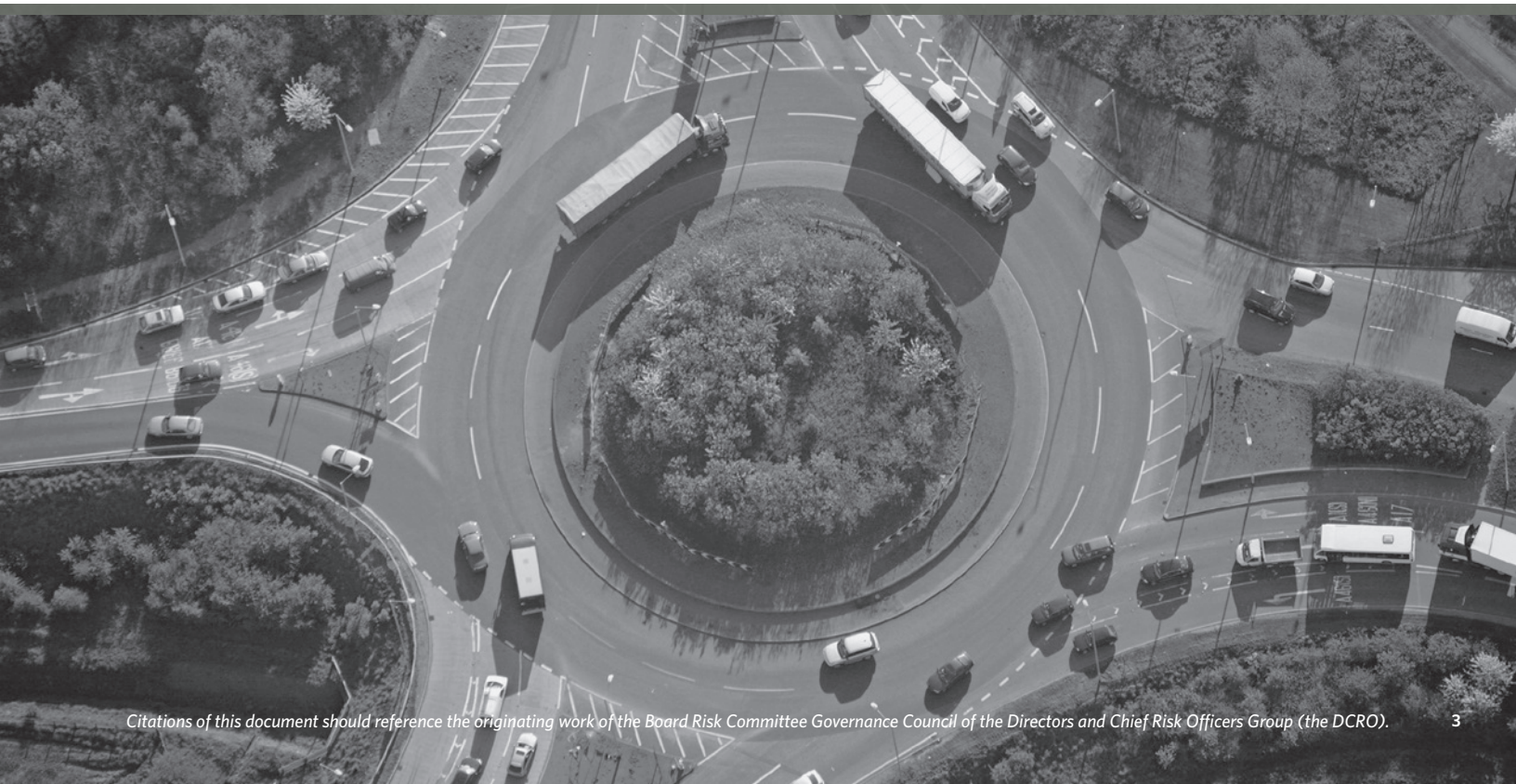
Membership in the DCRO is strictly limited to active or recently active, board members, chief risk officers, or c-level executives with risk governance responsibilities.

For further information, or to provide comments on these guiding principles, please contact:

The Directors and Chief Risk Officers Group
e) info@dcro.org
w) www.dcro.org
t) +1-917-338-6631

the DCRO
Directors and Chief Risk Officers Group

TABLE OF CONTENTS



DCRO GUIDING PRINCIPLES FOR BOARD RISK COMMITTEES

THE GUIDING PRINCIPLES

Board risk committees are of growing importance in best practice corporate governance. We provide these Guiding Principles and the associated discussion to further the development of risk governance processes via board risk committees at organizations of all kinds. These Guiding Principles have also been written to give external stakeholders a view of what should be expected from the boards of organizations on which they depend for their success.

Principle 1: At any organization, the full board has the overall responsibility for risk governance. In many cases, the full board will benefit from the focused and specialized support of a well-structured and competent board risk committee.

Principle 2: The focus of a board risk committee is to link the risk-taking activities of an organization with its strategic objectives. It provides the full board with the capacity to evaluate the risk management infrastructure and capabilities of the organization and to challenge the effectiveness of management's pursuit of strategic objectives from a return-on-risk perspective.

Principle 3: Board risk committee meeting agendas should be guided by best practices, stakeholder expectations, and regulatory requirements. Agendas should cover topics that include a review of risk culture, strategy, tolerance for loss, and both internal and external communications.

Principle 4: Regular meetings with key executives and independent information gathering from stakeholders are both essential for the board risk committee to develop a full narrative of a company's risk-taking activities.

Principle 5: The board risk committee must interact with other board committees to ensure full coverage of the organization's risk profile and the interdependencies across its risk and performance drivers.

Principle 6: Board risk committees should be populated with *Qualified Risk Directors* who are competent to govern the risks to which the organization is exposed.[1]

Principle 7: The board risk committee should provide sufficient guidance and information to allow the full board to issue a simple-language disclosure about the organization's risk culture and control processes. Further, and only if warranted, the full board should issue a statement that the organization's risk philosophy, infrastructure, processes, and capital base are "fit for purpose."

1 Download the DCRO Qualified Risk Director Guidelines for more details on these qualifications

BACKGROUND

As political and economic interactions become more complex, and as disruptive technologies and processes make innovation cycles massively shorter, boards of directors are paying more attention to risk. Risk is defined as the absence of certainty – a two-sided concept, describing both positive and negative deviations from expectations.

Most board members are quite adept at and familiar with risk-taking. But experience in taking risk and understanding risk are not equivalent. Board-level risk governance is a process that involves dynamic analysis of an uncertain future, development of internal resilience, allocation of risk-taking capacity, establishment of measurable levels of tolerance for loss, and envisioning things that may never have been considered relevant to a business discussion, but which might have highly disruptive potential. This type of analysis is the realm of directors with a special understanding of risk and is the genesis of board risk committee inclusion in best practice corporate governance.

In 2014, advisory organization Deloitte Touche Tohmatsu Limited conducted a global survey of publicly traded companies across eight countries. They found that nearly 40% of these organizations utilized board risk committees or hybrid committees that included risk in their title and focus.[2] That percentage is higher than surveys from just a few years earlier and suggests a growing adoption of board risk committees as a best practice.[3,4]

2 As risks rise, boards respond: A global view of risk committees, Deloitte Touche Tohmatsu Limited, 2014
3 The Relationship Between Boards of Directors and their Risk Management Organizations: Are Standards of Best Practice Emerging?, in Corporate Boards: Managers of Risk, Sources of Risk, Wiley-Blackwell, 2010
4 Emerging Governance Practices in Enterprise Risk Management, Conference Board Research Report, February 2007

THE PURPOSE OF A BOARD RISK COMMITTEE

Formal and effective implementation of a board risk committee fosters a corporate environment in which the most value can be created from an organization's limited risk-taking capacity. Garnering the most benefit from risk-taking requires both an understanding of downside risks, from either action or inaction, as well as an understanding of the drivers of success.

We can distinguish the functions and responsibilities of a board risk committee as the following:

- Having the directive to look forward, not backward in time
- Developing a deep understanding of the drivers of success in achieving corporate goals
- Building an awareness of any threats to those drivers of success as well as any opportunities for their enhancement
- Overseeing the organization's tolerance for loss relative to its objectives and accountabilities
- Ensuring that the organization has the necessary infrastructure, expertise, and capabilities to identify emerging changes in the risk landscape and to provide early warning of corporate performance that materially deviates from expectations
- Ensuring that the organization's infrastructure, culture, policies, and procedures foster resilience
- Ensuring that the components of enterprise risk management are in place and that the overall program is working effectively
- Driving the corporate risk culture throughout the organization
- Conveying to external stakeholders and potential partners that management and the board understand risk and its potential for positive and negative impact

To be clear, a board risk committee is not responsible for risk management. It's focus is on the governance of both risk-taking and risk management by employees of the organization in their pursuit of strategic goals. Its specialized focus and skills serve as a source of enhancement to the risk governance responsibilities of the full board.

DETERMINING THE NEED FOR A BOARD RISK COMMITTEE

The full board's responsibility for risk oversight and governance mirrors its responsibility for oversight of strategy and the evaluation of results. The question arises as to whether a board risk committee can help the full board to more ably fulfill its duties in this realm and whether board risk committees are now becoming an expectation.[5,6,7] Aside from regulatory requirements, which most commonly affect financial institutions, there is no clear demarcation between an organization at which it is acceptable for the full board to be the *de facto* risk committee and one that is more effective when directors are informed by the focused work of a board risk committee.

We suggest a few strategic and contextual tests for boards considering the benefit of a board risk committee:

Size, Dispersion, and Complexity – Highly complex organizational structures increase the possibility of risk amplifications, or knock-on effects that may not have been anticipated via normal executive or board discussions. Disparate geographic locations, rapid employee or revenue growth, and complex regulatory environments all suggest a likely benefit from the creation of a board risk committee.

Investor or Regulatory Concerns – Communication from investors or regulators indicating a concern that the board is not allocating sufficient time or has not acquired sufficient skills among its members to fully consider the impact of risk on the organization is also a likely indicator that it is time to establish a board risk committee.

Pricing Risk is a Core Function – If a business is specifically about pricing risk – insurance, banking, investing, or trading, for example – it is incumbent upon the board to create a specialized committee to ensure that the pricing of risk internally is as good as it is for external clients.

Dependence on Vendors, Outsourcing, and Offshoring – If an organization depends on numerous third-party vendors, not just in technology but through business process outsourcing, or the legal environment of operations is effectively outsourced for regulatory convenience, it likely needs the specialized knowledge that a board risk committee can provide.

Cyber and Privacy Risks – If the compromise of key digital assets or non-digital processes and information related to confidential client information or strategy would create an existential crisis, a board risk committee is probably warranted.

Real Assets and Human Safety – If an organization is predominantly involved in managing real assets and human safety is a key risk, it likely needs a board risk committee.

Board Focus and Time Management – If a board, in practice, is predominantly spending its time reviewing outcomes, management reports, and past performance rather than being prospective in its analysis, it probably needs a board risk committee to shift more of its attention to subjects of "what might be."

5 Should your board have a separate risk committee?, Tonello, Matteo, Harvard Law School Forum on Corporate Governance and Financial Regulation, February 2012

6 Are board risk committees a fiduciary expectation?, Koenig, David R., Conference Board of Canada, Risk Watch, December 2010

7 How your board can decide if it needs a risk committee, Governance Insights Center, PwC, 2017

It is well understood that good risk-taking results in a more effective use of capital in all forms – human capital, political capital, equipment capital, financial capital, reputation, and any other scarce input to the organization's success. Even a very modest improvement in return-on-capital translates into significant enhancements in market valuation for publicly traded companies and lower costs of all other forms of capital. A board risk committee helps the full board to evaluate if the organization is taking risks that will truly generate value after accounting for their costs, both actual and prospective. It further helps to focus the full board's attention on the organization's most critical risks and risk management capabilities.

Beyond these contextual evaluations, we provide a detailed list of questions in the Appendix to help boards determine whether their specific organization can benefit from the establishment of a board risk committee.

THE FORM AND FUNCTION OF A BOARD RISK COMMITTEE

If a board risk committee is being planned or is already a part of an organization's governance practices, proper structure, process, and population of the committee is essential for its success. A diligent routine of information gathering and interaction with key personnel, like that which is outlined below, forms the foundation for this success. In the end, implementation of these best practices will allow the full board to more ably fulfill its Duty of Care.

Charter of the Board Risk Committee

Since there will be some overlap of a board risk committee's work with the work of other committees, the full board must clearly define its goals and boundaries by charter. The charter of the board risk committee should, at a minimum, include the statement that its work is about ensuring the company has strategic risk-taking plans, risk management infrastructure, and capabilities that warrant the holding of investor capital. Simultaneously, it must ensure that these risk-taking plans are within the capacities that such capital allows.

It must take a holistic approach that is not just focused on financial risks that are easier to measure on a relative basis. The charter should direct the board risk committee to consider the value of capital like public trust, human safety, and how the organization is best putting its precious non-financial capital to use.[8]

Board Risk Committee Meetings and Discussions

Board risk committees should meet quarterly or monthly, depending on the complexity of the organization and overall cadence of full board meetings. The focus of the conversations should be on linking the organization's risk-taking activities with its strategic objectives and evaluating whether the return on risk-being-taken is sufficient to support strategic goals.

Several questions should be asked and answered at every meeting of the board risk committee:

- Are the risks being taken by the organization likely to foster the achievement of strategic objectives?
- How is the organization identifying, managing, and monitoring the risks it chooses to take?
- How might the organization do better by strategically taking more risk? Less risk?

8 Please see the Appendix for links to sample board risk committee charters

- In what cases has non-core risk been transferred or mitigated? What might cause these approaches to underperform or fail?
- What disruptions might cause expectations not to be met?
- How are changes in the environment in which the organization operates affecting its strategy and risk profile?
- How is the organization structured to respond and adapt to unexpected disruptions or events?[9]
- How is revenue gathered?
- Is the approach to incentivizing revenue generation consistent with the core philosophies of the organization?
- Are there any activities in which the organization is engaged that could significantly impact its reputation and ability to do business?
- Are there any operational aspects of the organization's work that could cause its "sudden death?"
- Are the organization's risk-taking activities consistent with its stated risk tolerances and risk appetite?
- Are there any third-party contracts or key employee agreements up for renewal that could disrupt the organization if they cease?
- Do the CEO and the board have enough information to have a bias towards confident, intelligent risk-taking?

9 For an interesting look at governing disruption in health care, see *Health Care Governance on the Eve of Disruption*, American Hospital Association, August 2018

Information Gathering

The aforementioned discussions are critical for developing a sound narrative and understanding of how risk is taken at any organization. To ensure that the information that reaches the board risk committee is accurate and has integrity, mechanisms must be in place to ensure that these conversations and associated analysis are supported with reliable and verifiable data as well as a diverse set of perspectives.

A significant portion of the information gathering process involves regularly scheduled meetings (no less frequently than once per quarter) with key executives including the CEO, CFO, Chief Risk Officer (CRO), Chief Audit Executive, CTO/CISO, the Head of Human Resources, and as appropriate, the heads of key business units. While it is important that these sessions be independent, executive sessions, we suggest that there is significant value to occasional open roundtable discussions that include all of these parties.

At least annually, the committee should independently gather information from key stakeholders in their supply chain, from customers, line employees, securities analysts, investment bankers, and regulators. The committee may go even further and create a stakeholders committee to advise it on external perceptions of the organization for alignment with the representations made by internal sources. To be clear, this is not intended to be a two-way flow of information, but rather a way for the board risk committee to receive additional perspectives on the work of the organization.

The committee should always consider ways to avoid barriers that prevent risk information from reaching the highest levels of an organization. Regular meetings with randomly selected line employees from key business and operational units may provide additional perspective on emerging risk or cultural issues that have not yet garnered the attention of senior management or that may contradict the representations they are making to the committee. These types of conversations can also help to identify obstacles to the free flow of critical information to the board.

The committee has a special relationship with the Chief Risk Officer, where one is present. This relationship may include that individual reporting indirectly to the committee (in addition to the CRO's direct reporting to the CEO). To supplement this, the committee should make liberal use of external risk advisors, much in the same way that the audit committee uses an independent audit firm. This is especially important if the organization does not have a CRO. The committee should not be afraid to challenge the assumptions and methods of the CRO, risk advisor, or any executive presenting evaluations of risk to the committee. At the same time, as appropriate, the board risk committee should make its backing and support of the CRO, where present, very clear to the senior administration of the organization.

The leaders of all compliance functions, including the General Counsel, should have direct access to and regular interaction with the board risk committee.

There must be sufficient risk infrastructure within the organization, as well as enough expertise on the board risk committee, to properly assess the organization's use of its risk capacity. In the process of information gathering, the committee should be able to determine and convey to the entire board the following information at the ensuing board meeting:

- The key findings of the organization's overall enterprise risk assessment and what actions are being taken to address any shortcomings
- Near-misses that have occurred recently and the lessons learned from them
- Avenues by which the organization might consider taking more risk
- A comparison of the organization's return on risk and cost of capital to that of its competitors

The process being used to validate that the culture of risk-taking at the organization is consistent with the board's articulated tolerance for prospective loss

We suggest that in the committee's review of the information it gathers, it pays special attention to any places where dysfunctional behavior in the organizational culture is becoming normalized, especially around incentive compensation. This includes a regular review of all escalation and whistleblower reports, whether made anonymously or directly to the committee.

The committee should gather enough information, both quantitative and narrative, to know where risk is "owned" within the organization and what kinds of risk assessments are being done on an ongoing basis.

Finally, the committee should establish certain trip wires that mandate the reporting of incidents to the committee. We suggest that the committee limit its use of "heat maps" as a process for identification of emerging issues and, instead, focus on the narrative provided via its regular conversations with key parties. Heat maps and other data can provide some context for the discussion but should not be considered the primary source of early warning.

Interaction with other Board Committees

The board risk committee should have regular interactions with other key committees of the board to discuss where their charters have overlapping interests. The focus of the compensation (remuneration) committee should be on the way in which compensation plans direct risk-taking behavior and any unintended messages that compensation plans convey. We refer readers to the DCRO Guiding Principles for Compensation Committees for a more detailed discussion of those risks.

The board risk committee should review the audit committee's report on the effectiveness of internal controls and address any material issues raised therein that relate to effective enterprise risk management.

It should review cyber risk issues with the technology committee or other appropriate body where a technology committee does not exist. Here we direct readers to the DCRO Guiding Principles for Cyber Risk Governance as a guide.

For non-financial organizations, it is essential to coordinate with the health and safety committee, focusing on physical risks that are typically not present at most financial organizations.

And since the skills to interpret risk and think forward are essential to the success of the board risk committee, it should work with the nominating/governance committee to fill any skills gaps that it identifies on the board or the board risk committee, ensuring that risk can be discussed by the full board in an effective manner. The DCRO Qualified Risk Director Guidelines provide detailed guidance on the skills and attributes required for members of a board risk committee. The discussion with the nominating/governance committee may also include any issues that the board risk committee identifies with the organization's governance structure that may contribute to an ineffective use of risk-taking capacity.

Finally, an annual board committee chairs' meeting may help to facilitate the coordination of respective agendas and a focus list for upcoming discussions of mutual interest.

Education

Because of the evolving nature of risk – expanding complexity, rapidly disruptive technologies, and the greater potential for risk amplification via broad and connected networks to occur, the board risk committee must also engage in ongoing education to ensure that it is implementing the best practices of risk governance. We recommend requiring that board risk committee members attend at least one or two outside risk courses each year, or, ideally, that case studies and reviews of emerging best practices be part of each board risk committee meeting. Committee members should not limit themselves to lessons from their own industry but should also seek out opportunities to learn risk lessons from other sectors as well.[10]

Additional Considerations

The committee should engage in an annual assessment of its own function, including the gathering and analysis of feedback from other committee chairs and the chair of the board, to evaluate how the committee functions along with the performance of individual members.

The committee should plan an annual meeting where specific areas of discussion and review are covered. In the Appendix, we provide a detailed list of items that should be covered in such an annual meeting.

We note that the need for and application of a board risk committee at financial and non-financial institutions is likely to be different. Both types of organizations can learn from the best practices of the other and we provide some discussion of this in the Appendix.

Ultimately, as a final act to demonstrate the commitment and effectiveness of the board risk committee, we recommend that the chair of the board risk committee communicate to the full board that the committee has reviewed the organization's risk philosophy, infrastructure, processes, and capital base, conveying to the board the shortcomings and steps being taken to address them.

THE ROLE OF A BOARD RISK COMMITTEE IN COMMUNICATIONS

Clear communication of an organization's philosophy around risk and its management is central to the effective use of risk-taking capacity within the organization as well as for the attraction of all forms of capital from outside of the organization. The full board should communicate this message in a positive and affirming manner, conveying a true understanding of the drivers of risk – the variance in expected outcomes.[11] This type of communication can reduce uncertainty and, therefore, reduce the cost of attracting human and financial capital, customers, and suppliers. It can also reduce the regulatory or legal drag that will inevitably develop from an inability to communicate such an understanding. It is likely that such an inability will convey a sense of a lesser practice of risk governance meaning that as board risk committees become more prevalent, the cost of that regulatory drag is likely to increase.

A board risk committee must drive the institutionalization of risk management and risk culture, as both will only be robust and sustainable if they become part of the organization's DNA. Sound and clear communication increases the implementation of a consistent risk culture.

Publicly traded companies in many countries are now or will soon be required to include some prospective discussion of risk in the management discussion and analysis. This can include a Duty to

10 Industry associations and stock exchanges often provide formal settings for such interaction. Examples include the NACD in the United States, the Conference Board of Canada and the Directors College in Canada, the Institute of Directors in the UK, the Australian Institute of Company Directors in Australia, and the Directors and Chief Risk Officers group (global).

11 For a helpful example from the non-profit sector, see Trent University's Risk Management page.

Disclose emerging risks. For example, in the UK, beginning in 2019, it is a requirement for companies to carry out a robust assessment of emerging risks as well as principal risks, explain what procedures are in place to identify emerging risks and explain how these are being managed or mitigated.[12]

As this practice is still nascent, companies have defaulted to catch-all language that bears the imprimatur of legal counsel. We believe that it is more helpful when a company clearly communicates a view explaining its culture and processes, rather than through complex or defensive language. Engaging in a clear communication of risk allows organizations to more ably demand the same from their suppliers, subcontractors, and service providers. Knowing that these critical partners are also well-engaged in risk governance can give an organization greater assurance that external issues which disrupt operations are less likely to emerge or will be less severe in their impact. This is especially important for non-financial organizations.

Since 2011, the Securities and Exchange Commission (SEC) in the United States has required quantitatively heavy disclosures around cyber risk. Its interpretive guidance notes that if cybersecurity risks are material to a company's business, the nature of the board's role in overseeing the management of that risk must be disclosed. This is consistent with the disclosure this Guiding Principles document recommends.[13]

While quantitative disclosures are helpful to some, they likely convey a false sense of the accurate measurability of large risk exposures. And they are also likely to be incorrectly understood by many critical parties, including the board and senior management. Carefully considered statements regarding the organization's sensitivities in economic terms and the material risks to achieving its objectives are needed by the board. Further, companies have an obligation to make this transparent to investors (owners) for an effective capital markets system to function. We note that this discussion can also include the impact of positive risk realization.

We recommend wrapping these quantitative disclosures in simple descriptive language. In making this suggestion, we rely on the adage that if you really understand something you should be able to communicate it in a way that everyone else comprehends. If the organization cannot do this in a public disclosure about risk and risk culture, then maybe the board doesn't really understand it either. Investors may rightfully conclude the same.

The process of drafting external statements about the risk culture and control processes can begin with the board risk committee. The first draft should be evaluated by the committee to ensure that it says what the committee wants to convey. General Counsel can then review the statement to ask how it might be misinterpreted and recommend adjustments. These adjustments should not overwhelm the first priority of communicating what was intended about the organization's understanding and effective governance of risk. Ultimately, the full board should approve and issue the statement.

We believe that if it accurately conveys the organization's understanding of risk and the ability of the organization to capitalize upon its risk-taking capacity this disclosure can conclude with the statement by the full board that the organization's risk philosophy, infrastructure, capabilities, processes, and capital base are "fit for purpose." Such a statement would solidify the trust that key parties need in any organization that affects their well-being.

12 2018 UK Corporate Governance Code and new legislation, Ernst & Young, July 2018

13 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 26, 2018, U.S. Securities and Exchange Commission

BOARD RISK COMMITTEE MEMBERSHIP

The duties and responsibilities of a board risk committee are broad and require substantial and specific skills and experience.[14] In 2013, the DCRO issued its Qualified Risk Director Guidelines to help boards identify the people most likely to be effective members of a board risk committee. Included in the Qualified Risk Director Guidelines are some of the key attributes, such as business acumen, risk management acumen, interpersonal skills, and education necessary to fulfill this role. For example, key attributes from the Qualified Risk Director Guidelines include:

Business Acumen

- The ability to evaluate different kinds of strategic options, including financial, operational, technological, or market-based investments
- The ability to keep risk strategically relevant, "at the board level" of discussion
- The ability to see both the upside and downside of risk-taking
- The ability to take the "long view" – to think about the effects that something will have in the future as well as in the present
- Expertise in the subject matter from which the organization's risks emanate and an understanding of the environment in which the organization operates, including identifying stakeholders, international networks, economic inter-relationships, and other external influences on the ability of the organization to achieve its goals

Risk Management Acumen

- Experience managing the types and complexity of risk the organization faces
- An understanding of how risks can be amplified or attenuated
- An understanding of the regulatory environment in which the organization operates, if any, and prospective changes related to risk governance
- An understanding of how risk relates to integrity, ethics, and ultimately to success
- An understanding of the broad scope of risk, risk terminology, the tools of risk management, and how to assess their proper application to the organization
- An inventive mindset akin to that of an engineer with failure analysis training

Personal Attributes

- Independence, integrity, honesty, and ethical conviction, with the determination to act above personal interests in the conduct of their role, and to engage and challenge the leaders of the business and risk infrastructure of the organization
- Having the ability to assess multiple potential outcomes concurrently – to think dynamically and about the likelihood of non-linear outcomes
- Assertiveness and the ability to manage conflict with strong personalities
- Healthy skepticism, balanced with earned trust – allowing one to probe and challenge without becoming unnecessarily antagonistic

14 In the United States, the Securities and Exchange Commission issued rules for audit committees that require a company to disclose whether it has at least one "audit committee financial expert" serving on its audit committee. See https://www.sec.gov/rules/final/33-8177.htm for more details.

- Having the ability to challenge a "group think" mentality, along with the awareness of common cognitive biases present among groups and individuals

Education

- An academic education commensurate with the complexity of the organization's needs and, when practical, related to the industry or industries in which the organization operates

Any good business manager is thinking about risk all the time. Therefore, when constructing the board risk committee, there should be a bias in membership towards people who have managed a business, business line, or risk budget desiring to avoid the dominance of a control or compliance mindset on the committee. This focus is important as a board risk committee formalizes the discussions of key issues an organization is thinking about intuitively regarding its strategic direction, activities, and accountabilities. Those without risk-taking experience and accountability might not use the same language or have the same intuition and experience as the type of people qualified to serve on a board risk committee. Nevertheless, the board risk committee should still include representation from both the audit and compensation (remuneration) committees for balance and to further enhance the committees' joint work on overlapping areas of interest and responsibility.

ALTERNATIVES TO A BOARD RISK COMMITTEE

If a thoughtful evaluation of the value of a board risk committee does not lead to a definitive answer, an alternative approach may be considered. We highlight two approaches here with some notes of caution about each.

In many organizations, in addition to its duty to evaluate the internal controls, the audit committee has been assigned the responsibility for risk governance. Audit committee membership requires financial literacy but does not necessarily require risk literacy. There is a specific mindset to the forward-looking, open-ended nature of risk governance that is not innate for many audit committees either by composition, agenda, or mindset. Hence, it is common to find audit committee charters with responsibilities for risk governance enumerated near the end of a long list of accountabilities. The message that such low prioritization conveys to investors and external partners is one of less than a full understanding of the importance of risk governance. As expectations from investors increase, this will become a costlier approach for organizations to take.

Some organizations have adopted hybrid committees — often referred to as audit and risk committees. If structured well so that each area of focus is an equally dominant part of the hybrid committee's discussion, a hybrid model can be successful. Utilizing this approach more likely means that the audit committee will be a feeder of past facts regarding open risks for consideration by a board risk committee.

One suggestion under this hybrid model is to have dual chairs of the committee — one for audit and one for risk. The meeting agendas would be flipped each time it meets, with the audit chair setting the agenda in one meeting and the risk chair setting the agenda during the ensuing meeting. Or, the committee can meet twice in the same day, with the audit chair leading the morning agenda and the risk chair leading the afternoon agenda.

Even with this structure, we note that audit committees already have very full and crowded agendas and the prioritization of risk discussions, even in these ways, is likely to give risk governance less than the needed attention. One additional drawback to the hybrid approach is that the size of the committee may need to be expanded to ensure sufficient expertise in both audit and risk subject matter. This may be counterproductive to efficient deliberations.

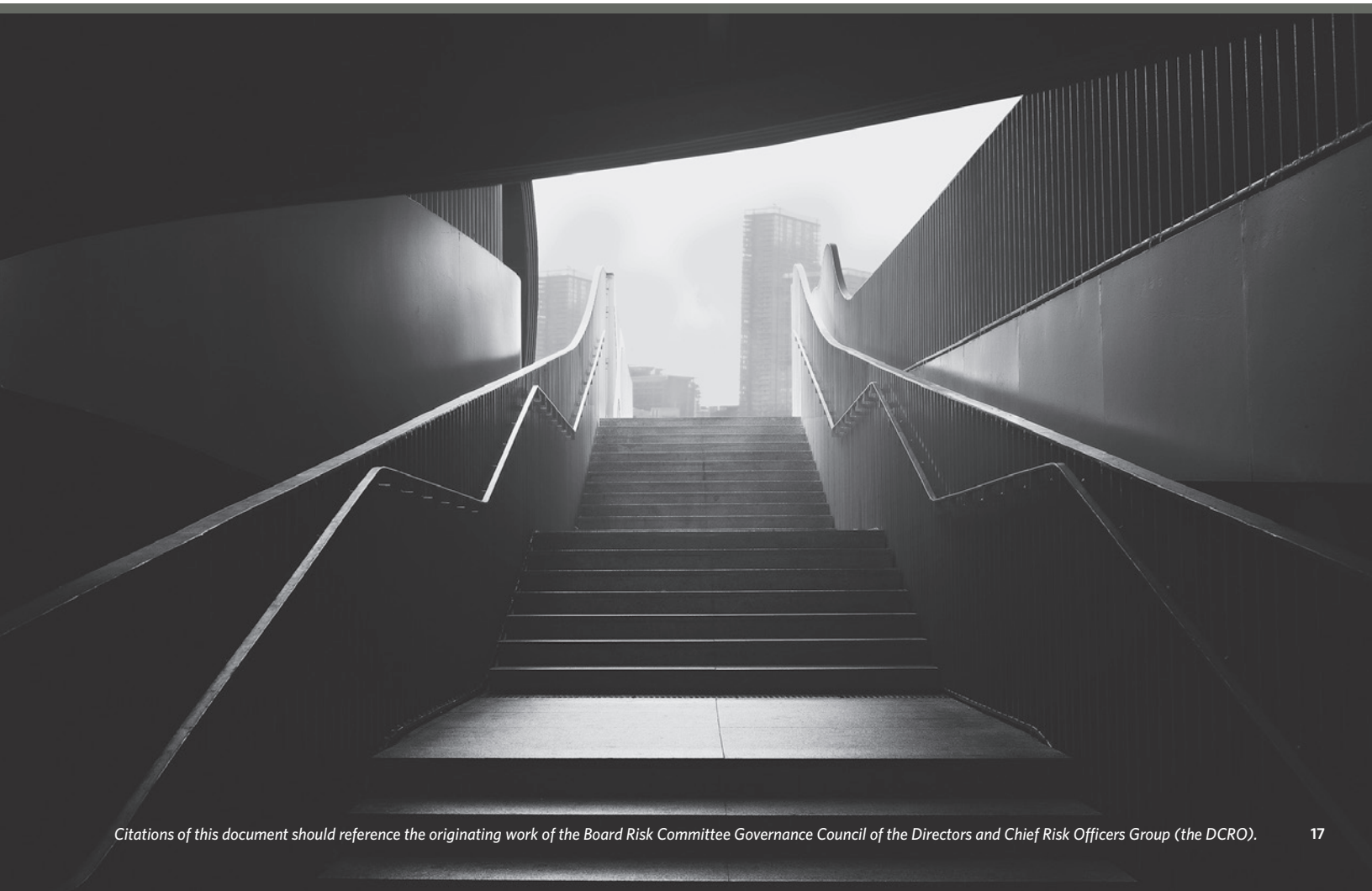
CONCLUSION

Effective risk governance adds value to any organization by improving the likely return on financial capital and reducing the cost of attracting capital in all its forms. Further, proper risk governance provides a higher level of certainty regarding the sustainability and viability of any organization.

Risk is complex and the interaction among various types of risk is increasing in complexity and velocity. While boards of directors remain accountable as a whole for the governance of risk, ably fulfilling the Duty of Care for which each individual director is responsible is difficult without the focused skill and analysis of a board risk committee. The work of a board risk committee will inevitably overlap with the duties of other board committees. That overlap simply provides an opportunity for discussion between the board risk committee and other committees, whereby the board risk committee brings its focused efforts to bear, further improving the organization's overall risk-taking and risk governance.

Forward-looking organizations are likely to be rewarded for adopting specialized risk governance at the board level. Board risk committees are likely to be most effective when they are created by positive choice. In the financial sector, the directive to create board risk committees came following an existential crisis. It behooves one to consider why an organization should wait until its industry experiences a calamity to begin a more focused look at the future.

An investment in the governance of risk-taking can be quite positively impactful and is wisely undertaken using these Guiding Principles.



APPENDIX

Reference Documents

Best Practice Documents

- Risk and Viability Reporting
- Build Your Board's Situational Awareness
- Risk Committee Resource Guide
- The Three Lines of Defense in Effective Risk Management and Control
- Risk Management and Corporate Governance (OECD)
- Standards on Risk Governance in Financial Institutions (IFC)
- Risk Governance: Evolution in Best Practices for Boards
- Financial Stability Board: Thematic Review on Risk Governance Peer Review Report
- Financial Stability Board: Principles for An Effective Risk Appetite Framework

Sample Board Risk Committee Charters

- Suncorp Group Limited (Australia)
- Prudential plc (UK)
- AMP Limited (Australia)
- Fonterra (New Zealand)
- Woolworths Holdings Limited (South Africa)
- Sample Risk Committee Charter (Deloitte)

Helpful Books

- Implementing Enterprise Risk Management: From Methods to Applications
- Governance Reimagined: Organizational Design, Risk, and Value Creation
- Risk Governance: Coping with Uncertainty in a Complex World
- The Law of Governance, Risk Management and Compliance
- Risk Culture and Effective Risk Governance
- A Short Guide to Risk Appetite
- Governance, Risk Management, and Compliance: It Can't Happen to Us

Education and Reference

- North Carolina State University Enterprise Risk Management Initiative Library
- IMMPC – Instituto Mexicano de Mejores Prácticas Corporativas

QUESTIONS USED TO EVALUATE THE NEED FOR A BOARD RISK COMMITTEE

The full board should be able to answer the vast majority of the following questions without significant sacrifice of the time it would dedicate to other strategic discussions. If it cannot, it is likely that the organization would benefit from the establishment of a board risk committee.

Questions on the Appetite, Capacity, and Tolerance for Risk

- What amount of loss could the organization sustain without draining its reserves/capital?
  - How long would it take to recover this via "normal" business operations?
- What kinds of actions by the organization would the board never tolerate or never want to read about in the newspaper?
- Is the organization's risk strategy aligned with the expectations of investors, creditors, and other stakeholders and has the organization communicated it correctly?
- What are the big negative risks for the organization?
  - What risk transfers or controls does the organization have in place to address these and what are the drivers of success to those controls and risk transfers that may fail to perform?
  - Is the organization's expected net exposure after these controls and risk transfers acceptable, given its business and capital constraints?
- As the appetite for physical injury to people is zero at most organizations, is the organization making any trade-offs to reduce financial risk or to improve financial performance, that are simply transferring financial risks to operational risks that run counter to the organization's appetite for safety?
- Is the board's risk appetite clearly understood by senior management and is it communicated throughout the organization to drive the right levels of risk-taking?
- Is the organization thinking about risk in the right way?

Questions on the Risk Infrastructure, Culture, and Capabilities of the Organization

- How does the organization validate that the board's vision and policies are understood by all employees or by volunteers at a non-profit organization?
- Has the organization developed a comprehensive continuity and disaster recovery plan for all key sites, assets, and facilities?
  - If so, does the organization validate that it has been properly and successfully tested at least annually?
- Has the organization created a detailed analysis of the many drivers of performance, both positive and negative, identifying those most material and those with the greatest possibility for amplification?
- What are the threats to the primary drivers of the organization's performance?
  - If any one loss would be big enough to disrupt services, what is the organization's contingency plan?
- What would the organization like to do, but is not doing because of some fear?
  - What opportunities are the organization missing by not taking action or enough risk?
  - What could be accomplished at the organization by utilizing the benefits of a successful new idea?
- How does the organization measure its risks and know that they are of an appropriate size and not increasing?
- Does the organization have a way for concerns to be escalated to the board without executive staff interference or interpretation?
- How does the organization ensure that its employees are always growing in their risk-taking skills?
- Does the organization's compensation plan encourage risk taking at a level commensurate with its risk appetite?
- What are the organization's potential blind spots in terms of risk governance?

Questions on Process

- Does the board regularly meet in executive session (without the chief executive present)?
- Does the organization's administrative team track risk events, near-misses, actions, and outcomes for a future review by the board?
- Does the organization have a way to gather independent input from stakeholders?
- Does the board have a diagnostic of where the organization is compared to plan/expectations?

Questions on Business Strategy and Capabilities

- What are the specific measures and targets that the organization uses to evaluate its progress toward long-term and short-term goals, and are they consistent with the organization's risk appetite?
- What is the risk of being too risk-averse in pursuit of new goals or new areas of service?
- What is the quality and security of the organization's critical capital providers?
- What is the quality and security of the organization's assets?

Questions on External Influences

- What are the ethical and cultural priorities that attract stakeholders to your organization?
- How does the organization monitor changes in the external environment?
- Does the organization regularly assess, in a repetitive and comparable manner, the satisfaction with its services that customers and external influencers have?
- Could a competitor make your organization's business model obsolete or threaten your independence?

Return to Guiding Principles

SUGGESTED QUESTIONS FOR THE ANNUAL MEETING OF A BOARD RISK COMMITTEE

It is a best practice for the board to monitor the company's risk management and internal control system at least annually, while also carrying out a review of their effectiveness. As these Guiding Principles have likely conveyed, this is an enormous and time-consuming task, and one that requires very specific skills. While the board maintains the responsibility for monitoring, the board risk committee can complete an annual review of key items and summarize them for the board. We suggest that such an annual meeting include review, discussion, and reporting of at least the following items, grouped here by theme:

Strategy

- Is the organization structured to innovate in a way that fosters even better goals and, where desired, creates disruptions for competitors in the marketplace?
- How have the organization's strategy and objectives changed in the past year and what are the critical risks and assumptions inherent in those?
- What impact does a change in chosen strategy have on the risk appetite of the organization, and vice versa?

Business Environment

- How have the markets in which the organization operates changed in the past year?
- What changes over longer time horizons might impact the organization's current plans and statements?
- How and why has the organization's cost of capital changed in the past year and are these changes unique to the organization or consistent with the experience of competitors?
- Have there been any changes in the regulatory requirements or expectations around the organization's risk infrastructure? If so, what is the company doing to address those shifts?
- Have there been any changes in expectations from investors or credit providers around the organization's risk infrastructure? If so, what has the company done to address these issues?
- Have there been any changes in expectations from other key stakeholders (customers, suppliers, prospective and existing human capital, for example) around the organization's risk infrastructure? If so, what has the company done to address them?
- How does the organization know or anticipate its customers' future needs?
- What is different about the organization's current situation in comparison to that of its key competitors?

Infrastructure

- How has the organization's risk management infrastructure changed in the past year and is it sufficient, given the risks the organization is taking?
- Does the organization have an effective escalation policy and whistleblower hotline?
  - Have they changed in the past year?
  - What are the details of their use in the past year?
- Have there been any changes made in the reporting line of internal audit and risk management and do those changes enhance or hamper the risk governance of the board?
- Is the risk management function adequately staffed and does it have access to sufficient risk infrastructure?
- How is the organization's critical data stored and protected, and how can it be accessed during a crisis?

- How effective have risk transfer programs – including hedging and insurance – been and are they adequate?
- How do we plan to ensure a consistency in the organization's risk appetite and philosophy across new administrations when organizational leadership changes?

Culture

- Are the current internal risk appetite statements, risk limits, and risk philosophy statements consistent with the state of the markets, political environment, organization's strategy, objectives, and risk-taking capacity?
- Are these statements and limits accurately understood by senior executives and their staff?
- Is the company actively discussing and addressing changes in expectations around work environment, safety, sources of harassment or disparate impact?
- Do we clearly link performance management and risk and is the organization's defined risk appetite consistent with expected employee behaviors?
- What is the organization's policy on sustainability and other Environmental, Social, and Governance (ESG) issues and are they consistent with external expectations?
- What does the organization do to ensure that it is compliant with its own sustainability and ESG goals?
- How does the organization evaluate whether its compensation plans drive behaviors consistent with the organization's desired culture?
- When managing risks, is the business balancing the proper commercial aspects versus operational and functional aspects?

Resilience

- Does the organization have an empowered committee to quickly respond to emerging risk events (Problem Response Team) and how often, for what reasons, and to what effect has it been used over the past year?
- Has the authority of this Problem Response Team been changed in the past year and do those changes enhance or hamper the ability of the organization to respond quickly to emerging risk events?
- Are the technical skills and leadership resources of the Problem Response Team congruent with the organization's key risks?
- Does the organization have a robust business continuity plan and was it tested, utilized, or changed in the past year?
- If so, what were the results, and will the changes enhance the organization's ability to respond to emerging risk events?
- Does the company have a robust succession plan and how is the board monitoring it?
- What changes are planned to address any discovered shortcomings?

Return to Guiding Principles

BOARD RISK COMMITTEES AT FINANCIAL VERSUS NON-FINANCIAL ORGANIZATIONS

At all types of organizations, both positive and negative variations from plan will impact current performance and the ability to pursue larger goals in the future. But that ultimate linkage does not mean that financial and non-financial organizations have the same agendas or areas of focus for a board risk committee. There are, of course, both financial and non-financial sources of risk at each type of entity. However, the cultural risk environment in which they operate and the focus of attention in risk governance are quite different.

For example, health and safety matters rank substantially higher on the risk agendas of most organizations that deal with the interaction between physical assets and people as an integral source of value creation. Financial organizations, while arguably having substantial physical assets like technologies and physical space, do not have the same kind of interaction between the physical and human assets. At non-financials this interaction often has health and safety implications for both employees and communities in which they operate, sometimes as matters of life and death.

Another example is the difference in counterparty risk. Suppliers in the physical chain of resource provision have long lead times, may have significant capital investments to make to service the non-financial client, and their resilience in the face of negative risk events could affect production of the non-financial for extended periods of time. While financial capital is also a flow, the focus on maintaining that flow is concern over immediate and catastrophic interruption, akin to what Lehman and Bear Stearns faced during the 2008 financial crisis. Or, the failure of a counterparty to meet the terms of a financial contract could begin a cascading series of events for the financial organization. The response of each type of entity to its specific forms of counterparty risk means that it has a different approach to resiliency matters, such as the speed, visibility, and externalities of amplification.

A third example is a focus on resilience due to negative physical risks that come about by the actions of the non-financial company, as was the case with the Bhopal gas leak or the Deepwater Horizon oil spill. Financial instruments can be quite complex to analyze and understand, but non-financial organizations typically have significantly more complexity to their risk issues because they cut across multi-faceted exposures like cultures, political boundaries, varying regulatory environments, safety, and more. They need to operate more infrastructure in the communities which necessitates a greater focus on the goodwill they have with these communities than do financial corporations.

And a final example is that managers of non-financial organizations are more often faced with the choices referred to as *real options*. These are projects that involve physical rather than financial assets. Expanding or closing a production line, running a pilot project, identifying potential opportunity costs of a choice, failure to account for the value of possibilities that move from potential to real in the event of successes now are all examples of real options that are more relevant to governance discussions at non-financial organizations.

Despite the clear complexities of governing risk in the non-financial sector, we find a much higher prevalence of board risk committees within the financial sector. Much of this is due to recent regulatory emphasis and not because of some broad, industry-driven initiative.

Financial, non-financial, and even non-profit or governmental agencies, share a common need to understand the drivers of their success and should include at their board risk committees a review that encompasses discussion of their objectives, measurement of achievement of those objectives, potential drivers of both positive and negative variance from those objectives, tolerance for those variances, and plans for resilience in the event that a variance has the potential to move outside of tolerances. These common needs suggest there is no less importance to the establishment of a board risk committee at non-financial entities than at financials and that both types of organizations could benefit from implementing risk governance review practices common at the other.

Return to Guiding Principles

DCRO BOARD RISK COMMITTEE GOVERNANCE COUNCIL MEMBERS

Mazhar Bashir Ahmad (Norway) | Partner, Head of Risk in Norway, Financial Compliance Group (FCG); Former Head of Group Risk Management, Gjensidige Group

Florence Anglès (Switzerland) | Chief Risk Officer, REYL & Cie Ltd; founder of a Risk Manager Association in Switzerland: GIROS; member of Club de lecture et de Présélection du Prix Turgot (Paris, France)

Laurie Brooks (US) | Board Member and Chair, Board Risk Committee, Provident Financial Services; Former Director, NACD New Jersey; Former Chief Risk Officer, PSEG; Former Chief Risk Officer, PG&E

James Brown (US) | Senior Vice President and Chief Risk Officer, Progress Bank and Trust; Former Field Examiner, Office of Thrift Supervision

Martyn Brush (UK) | Chief Executive Officer, ePanoptes; Former Chief Risk Officer, Global Markets and Global Head Market and Pension Risk, RBS Group

Maria Paula Calvo (Mexico) | Vice President Service and Global Technology and Operations Lead Mexico, MetLife; Former Chief Operating Officer and Member of the Executive Committee, AXA; Former Board Member and member of the Risk and Audit Committee, Credito Familiar S.A. de C.V. (Citi)

Richard Daingerfield (US) | Member, Board of Directors, Peapack-Gladstone Bank; Adjunct Professor, Boston University School of Law; Former Executive Vice President and General Counsel, Citizens Financial Group, Inc.; Former Executive Vice President and Chief Legal Officer, NatWest Holdings, Inc.

Todd Davies (Australia) | Board Member, Independent Chairman and Member, Audit and Risk Committees (multiple), New South Wales Government; Board Member, Independent Chairman and Member, Audit and Risk Committees (multiple), South Australia Government; Former Member, Board of Directors, Australian Conservation Foundation

Luis Franco (Portugal) | Chief Risk Officer, Companhia de Seguros Tranquilidade (Seguradoras Unidas); Former Chief Financial Officer and Mandatario, Commercial Union Assurance Plc in Portugal

Carol Gray (Canada) |Board Member and Member of Board People and Remuneration Committee, IFM Investors Pty (Melbourne); committee member of IFM Board Responsible Investment and Sustainability; Governor, Trent University and member of Pension and Investments and Endowment Lands Committees; Board Member, ISPT/IFM International Property Management; Board Member and Chair, Board Risk Committee, Amex Bank of Canada; Former President, Equifax Canada; Past Board Member and Chair Ontario Realty Corporation; Past Board Member and Chair, Board Risk Committee, Infrastructure Ontario

Darlene Halwas (Canada) | Board Member and Chair, Audit Committee, Commissioner for Complaints for Telecom and Television Services; Board Director, Canada Development Investment Corporation; Board Member, Watt Consulting Group; Board Member, Alberta WaterPortal Society; former Corporate Director, Aquatera Utilities Inc.; and past Head of Risk Management for three companies

Michael Haralabidis (Greece) | Chief Risk Officer, Hellenic Financial Stability Fund; Former Group Chief Risk Officer, Piraeus Bank; Former Deputy Director — Group Risk Management, National Bank of Greece; Former Chairman and Member, Audit Committee, European Investment Bank, Luxembourg; Former Chairman and Member, Audit Board, European Investment Fund, Luxembourg

Craig Jimenez (US) | Board Member, NACD North Texas; Former Board Member, EcoCentri, LLC; Former Board Member, OGE Energy Resources, Inc.; PRMIA Subject Matter Expert — Risk Appetite and Executive Compensation

Robert Karreman (UK) | Chief Risk Officer MARLO Technologies (U.K.); Former Chief Risk Officer, East-West United Bank S.A.(Luxembourg); Former Chief Risk Officer, Alfa Bank (Russia)

Christy Kaufman (US) | Risk Analytics and Insights Director, American Family Insurance; Faculty Member and Senior Lecturer, University of Wisconsin; Former Head of Enterprise Risk Management and Chief of Staff to the General Counsel, Marsh & McLennan Companies

David R. Koenig (US) | Chair, DCRO Board Risk Committee Governance Council, Founding Principal, TGF Analytics; Founding Principal, (b)right governance; Founder, The Directors and Chief Risk Officers Group; Former Board Member and Chair, Professional Risk Managers' International Association; Former Board Member, Northfield Hospital & Clinics; Author, *Governance Reimagined: Organizational Design, Risk, and Value Creation*

Lloyd Komori (Canada) | Board Member, Chair Audit, Risk and Investment Committee ETFO — ELHT, Board member, Former Chair, Governance and Nominating Committee, Toronto Central Local Health Integration Network; Former Senior Vice President, Risk Management, OMERS Administration Corporation; Former Board Member, OMERS Administration Corporation; Former Chief Risk Officer, Ontario Power Generation; Founding Faculty Instructor, The Directors College

Council member organizational affiliations are listed for identification purposes only and do not imply the formal endorsement by said organizations of these guidelines.

James Lam (US) | Board Member and Chairman, Risk Oversight Committee, E*TRADE Financial; Independent Director, RiskLens Inc.; President, James Lam & Associates; Former Partner, Oliver Wyman; Former Chief Risk Officer, Fidelity Investments; Author, *Enterprise Risk Management* (Wiley, 2014) and *Implementing Enterprise Risk Management* (Wiley, 2017); NACD Directorship 100 (2017, 2018); NACD Board Leadership Fellow and Faculty; Inaugural GARP Risk Manager of the Year (1997)

David X. Martin (US) | Co-managing director of cybXsecure; Former founding Chairman, Investment Company Institute's Risk Committee; Former Co-Chair, Buy Side Risk Committee; Adjunct Professor, New York University's and Fordham's Graduate Schools of Business, author of *Risk and the Smart Investor* and *The Nature of Risk*; Special Counselor on cybersecurity and emerging risks, Center for Financial Stability, Expert witness and former Chief Risk Officer, AllianceBernstein and Head of ERM for Citicorp

Joseph Masri (Qatar) | Head of Risk Management at GRSIA – Qatar Pension Fund; Former Head of Risk Management, Qatar Investment Authority; Former Head of Risk Management, CPPIB; Former Head of Risk Management, Barclays Global Investors

Cyril Maybury (Ireland) | Non-executive Chairman of Payac Services and Non-executive Chairman of Harcourt Life; Non-Executive Director and Chair of Audit and Risk Committee, Concern Worldwide; Pension Trustee of a number of pension funds; Former Chair, Business Law Committee, Consultative Committee of Accountancy Bodies — Ireland; Former partner in EY Ireland with various roles leading Audit, Risk Management, Fraud Investigation and Litigation Support and Expert Witness Services

Braden Perry (US) | Co-Founder, Kennyhertz Perry LLC; Board of Directors, Kansas City Securities Association; Former Senior Vice President and Chief Compliance Officer, Mariner Holdings, LLC; Former Senior Trial Attorney, U.S. Commodity Futures Trading Commission

Rupert Purser (Hong Kong) | Chief Executive Officer, Asia and the Middle East, Litigation Financing Asia ("LFA"); Past Chairman for the Asia Transformation and Turnaround Association

Tatiana Segal (US) | Partner and Head of Risk Management, SkyBridge Capital; Former Chief Risk Officer, Cerberus Capital Management; Former Chief Risk Officer, Diamond Lake Investment Group

David Streliski (Canada) | Co-Founder, Chairman of the Board and Chief Operating Officer, Koios Intelligence; Former Chief Risk Officer, Fiera Capital Corporation; Former Board Member, Professional Risk Managers' International Association (PRMIA); Co-Director, PRMIA Montreal

Leslie Thompson (Canada) | Board Chair, Architectural Conservancy of Ontario; Former Board Member, Home Trust Company; Former Board Member and Chair of Risk Oversight, Deposit Insurance Corporation of Ontario; Former Board Member and Chair of Governance, Ontario Municipal Employees Retirement System; Former Board Member, Chair and Chair of Governance, Gallery 44 – Centre for Contemporary Photography

Mark Trembacki (US) | Managing Principal, Risk Management Levers, Inc.; Former SVP, Risk Integration, COO, Commercial Banking, and Head, Enterprise Operational Risk Management, BMO Financial Group; Adjunct Professor of Enterprise Risk Management, University of Illinois; Chair, Private Directors Association Cybersecurity Initiative, Member, Audit and Risk Committee

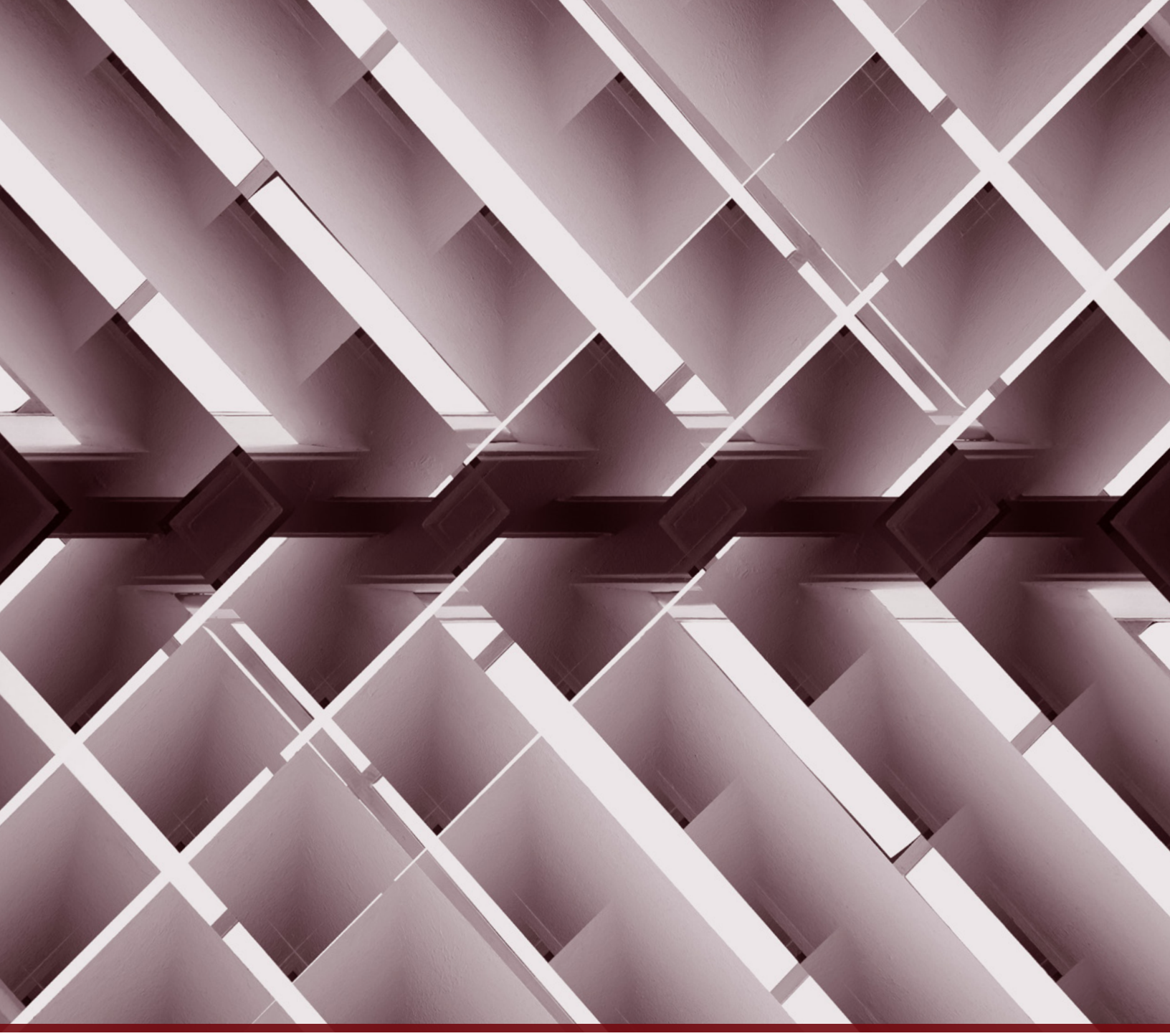
Kenneth Willems (Belgium) | Head of Corporate Risk Management Department, DEME Group

---

Thank you to the sponsors of these Guiding Principles:

T|G|F Analytics
Unique risk insights on publicly traded companies.

(b)right governance
PUBLICATIONS



The Directors and Chief Risk Officers Group

Leaders of the global risk governance community.

w) www.dcro.org
e) info@dcro.org
t) +1.917.338.6631

the DCRO
Directors and Chief Risk Officers Group