North American
CRO Council

Risk Governance and Culture

Principles and Practices in the Insurance Industry

February 2014

North American CRO Council

This publication was sponsored by members of the North American CRO Council. The content of this article reflects the view of the majority of the Council and not necessarily the opinion of every member.

ACKNOWLEDGEMENT

The North American CRO Council would like to thank Oliver Wyman for their support, guidance, and coordination throughout the development of this work product.

TABLE OF CONTENTS

North American CRO Council

Section I: Executive summary

The global financial crisis was marked by several high-profile failings of risk management across the financial services sector and particularly amongst banks. The insurance industry fared relatively better, largely due to structural differences in the underlying business model and the illiquid nature of insurance liabilities, but it was not left entirely unscathed. Weaknesses in governance and/or an unhealthy or unbalanced culture were cited as common contributory factors in many such risk failings, although we note that in some cases the firms' risk management practices were generally considered reasonable and the firms had emphasized aspects of risk governance and culture. These events highlight the need for consistent and continued emphasis on governance and culture in order to ensure the effectiveness of risk management and a well-functioning insurance industry.

In the years since the crisis, the entire financial services sector has faced heightened regulatory scrutiny, with particular emphasis on bolstering enterprise risk management (ERM). Today, multiple stakeholders including investors and policyholders expect a higher form of risk management capabilities. Rating agencies are also enhancing their focus on ERM capabilities, and in some cases explicitly include ERM reviews within their rating processes for insurers. Given the lessons learned from the crisis as well as the enhanced focus from regulators, shareholders and rating agencies, the insurance industry has been hard at work strengthening risk management capabilities, with a strong focus on risk governance and culture.

The North American CRO Council ("Council"), representing 30 insurers across North America, seeks to develop and promote sound practices in risk management. This paper, which was developed in collaboration with Oliver Wyman, is intended to highlight key considerations that we hope will assist the industry in further strengthening risk governance and culture. Importantly, we acknowledge that there are many approaches to implementing sound practices in risk management; business requirements and implementation may differ meaningfully across organizations due to factors such as business complexity and strategy, organizational size, risk tolerance and target risk positioning. Indeed, in our research we find that practices vary considerably across the industry. Notwithstanding these differences, looking ahead, we believe there are several principles which serve as a guide for our industry, each essential for ensuring effective risk governance and building and sustaining a healthy risk culture.

there are **many approaches** to implementing sound practices in risk management

Sound principles of risk governance

1. **Boards, in their mandate to oversee risk, strike the right balance between ensuring risk is managed prudently and allowing for strategic risk-taking within a specified and agreed risk appetite:** Boards need to play a critical role by actively shaping the questions that are being asked, while still encouraging management to pursue the agreed risk-taking strategy.

2. **Boards have the resources to deliver on their mandate:** Boards need to have the expertise, skills and up to date information to provide effective challenge. Regular and extensive risk-focused discussions are needed to provide a forum for the Board to discharge its risk-related duties. A well-defined risk appetite and set of risk policies should be maintained and enhanced, and business decisions and strategies should be evaluated against these policies.
3. **Risk management is a shared executive priority:** Risk management should be an explicit executive priority and part of the formal goals of the entire executive team, not just the domain of the Risk Management function.
4. **Risk Management function is independent, effective and influential:** Independence of the Risk Management function is critical. Risk Management professionals should be enabled to effectively deliver on their mandate to manage risk and need to have unfettered access to senior leaders and the Board.
5. **Risk organization is well aligned to the risk-taking units:** Risk Management is sufficiently involved in business decisions to allow for the possibility of identifying emerging risks or changes in the risk profile beyond what is detectable in tracked metrics.

Sound principles of risk culture

The global financial crisis made it clear that risk governance mechanisms need to be complemented by a robust risk culture, especially within front-line risk-taking units. We believe that, in its simplest form, risk culture amounts to the shared understanding and behavioral attitudes of an institution's people towards risk-taking. It can, rightly, be unique to a given firm and should be consistent with the firm's business strategy and risk appetite. It is essential for firms to assess their risk culture on an ongoing basis, proactively target preferred cultural practices and celebrate behaviors and individuals that reinforce the desired cultural state. We believe the following principles are essential in order to establish a healthy risk culture:

1. **Board and Executives prioritize effective risk culture:** "Tone from the top" is a critical factor in instilling a healthy risk culture. Furthermore, firms need to emphasize risk awareness and include risk-adjusted metrics in their performance measures and incentive structures. Prudent risk-taking should be encouraged and respect for the wisdom and validity of risk limits instilled. Firms should recognize that their understanding of risks may be flawed and should prohibit make or break bets.
2. **Risk-taking units are key actors in a risk-aware culture:** Risk culture concerns the cultural and behavioral practices related to risk management across the entire organization; it is crucial to emphasize a risk-aware culture within front-line risk-taking units. The Board and Senior Management must remain mindful of attitudes towards risk-taking throughout the organization.
3. **Risk education, communication and transparency are emphasized:** Important elements in strengthening risk culture are effective communication, education and training on risk-related topics; this is a key role for the Risk Management function.

We hope that these principles and the examples of sound practices described herein serve as a useful reference for the industry on matters of risk governance and culture. Firms should take heed from the recent high-profile failings, and the governance and cultural weaknesses they exposed, in deciding how to prioritize and invest. Although each of these principles on its own will strengthen institutional risk positioning, the collective impact of these principles would be greater than the sum of the parts and therefore should be considered the goal.

North American CRO Council

Section II: Introduction

The global financial crisis exposed multiple pressure points with respect to risk governance and culture across a range of financial institutions, with the banking industry highlighting particular inadequacies. Since the crisis, a number of high-profile incidents such as JPMorgan Chase's "London Whale" or Barclays' LIBOR scandals[1] clearly underscored risk governance and cultural weaknesses, shifting regulatory, shareholder and media focus towards these topics. Interestingly, we observe that many of the firms impacted by these incidents were well-reputed and were considered to have reasonable practices across key dimensions of risk management, which further highlights the need to continuously reinforce risk governance and culture. Today, even the firms with the strongest risk management capabilities can't afford to become complacent as governance failings or a sub-optimal culture can develop in isolated pockets and precipitate high-profile incidents at, otherwise, sound and prestigious institutions. Although insurers remained predominantly on the periphery of the crisis, risk governance and cultural aspects have nonetheless gained importance as the industry was impacted by the subsequent prolonged economic stress, including historic low long-term interest rates and volatile equity markets.

The global regulatory landscape has evolved considerably since the crisis. In the context of insurance, these regulatory changes are partially driven by emphasis placed on risk governance and culture topics by the global insurance standard setting body – the International Association of Insurance Supervisors (IAIS). The IAIS has developed a set of twenty six insurance core principles (ICPs), a number of which focus on establishing sound governance and cultural practices. The IAIS is also in the process of developing a common framework (ComFrame) for the supervision of internationally active insurance groups (IAIGs), placing extensive focus on governance, Own Risk and Solvency Assessment (ORSA) and ERM topics[2] (Box 1). In addition to continued focus on risk governance, global regulatory bodies and industry groups are placing heightened emphasis on risk culture. For example, both the Institute of International Finance (IIF) and the Financial Stability Board (FSB) have identified risk culture as a key priority, described common risk

Box 1: IAIS guidelines

Within IAIS Insurance Core Principles (ICPs), ICP 7 emphasizes corporate governance, focusing on the structure and governance of the Board in risk management, executive remuneration and ensuring reliable and transparent financial reporting. Similarly, ICP 8 highlights Board responsibility for risk management and internal controls systems, including actuarial, compliance and internal audit functions; and ICP 16 deals with enterprise risk management requirements for solvency purposes, risk responsiveness, and mandates ORSA.

Furthermore, within the forthcoming IAIS ComFrame supervisory requirements, modules focus on group governance frameworks, management structures and assessment of business mix from the perspective of managing risk. Other modules emphasize principles of the corporate governance framework, particularly with respect to the establishment of group-wide risk management frameworks and internal controls systems appropriate to a firm's organizational structure.

1 Risk governance and culture failings were identified in the report of the Review Committee of the Board of Directors of JPMorgan Chase on the Board's Oversight Function with respect to Risk Management (Jan 2013) and by the Salz Review: An Independent Review of Barclays' Business Practices (Apr 2013). In addition, failure of control was identified as the proximate cause during the investigation of JPMorgan Chase's role in the Madoff scandal (Dec 2013).

2 Insurance Core Principles, Standards, Guidance and Assessment Methodology (Oct 2011; updated Oct 2013). Common Framework for the Supervision of Internationally Active Insurance Groups; Consultation Draft (2013). International Association of Insurance Supervisors.

culture issues and emphasized key concepts such as "tone from the top", accountability, effective challenge and the role of incentives.[3]

Supervisory approaches to these topics vary across regulators. For example, risk governance and culture are a key focus for the U.S. National Association of Insurance Commissioners (NAIC), and corporate governance is a core component of its Solvency Modernization Initiative (SMI), which provides relatively high-level guidance on these topics. In contrast, the Canadian Office of the Superintendent of Financial Institutions (OSFI) and the Bermuda Monetary Authority (BMA) have issued more detailed requirements over the past few years. For example, OSFI's recent guidelines emphasize a number of governance mechanisms, including the role of the Board of Directors and the Audit committees, as well as broad governance mechanisms, such as the risk appetite framework and the role of risk committees and risk officers.[4] Similarly, BMA has issued extensive guidelines regarding governance topics, group supervision rules and group responsibilities.[5]

Going forward, insurance regulators are broadly converging around the principles of ORSA, which is based on the notion that each firm needs to tailor an effective risk management framework in order to internally self-assess and effectively manage enterprise risk. Risk governance and culture are key components of the ORSA framework; for instance, ORSA includes specific emphasis on embedded risk culture, risk accountability and responsibility, as well as identifying lines of defense for compliance, risk management and audit.

3 Reform in the Financial Services Industry: Strengthening Practices for a More Stable System (Appendix A). Institute of International Finance (2009). Increasing the Intensity and Effectiveness of Supervision: Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. Financial Stability Board (2013).

4 The Office of the Superintendent of Financial Institutions Canada: Guideline on Corporate Governance (Jan 2013).

5 Bermuda Monetary Authority: Insurance (Group Supervision) Rules (2011); The Insurance Code of Conduct (2010).

These insurance sector developments are complemented by trends within the broader financial services regulatory landscape. For instance, the Dodd-Frank Wall Street Reform and Consumer Protection Act[6] highlights the role of the Board in risk governance for financial institutions. These regulations will require certain non-bank financial institutions to establish a Board committee – comprising a number of independent directors and at least one risk management expert – responsible for oversight of enterprise-wide risk management practices.

In addition to the regulatory scrutiny afforded to these topics, rating agencies, academics and industry thought leaders are increasingly focused on promoting sound practices regarding risk governance and culture, as highlighted by a number of recent publications.[7] Some rating agencies explicitly include ERM reviews within their rating processes for insurers; for instance, in its rating reviews, Standard & Poor's formally evaluates the strength and capabilities of the ERM function across five key sub-factors which include risk management culture.[8]

The combination of each of these factors underscores the need to strengthen governance and cultural aspects across the insurance industry. We note that there are multiple approaches and mechanisms to enhance a firm's positioning and as each firm seeks to strengthen their practices, consideration should be given to invest across the range of attributes which enable risk governance and culture.

6 Dodd-Frank Wall Street Reform and Consumer Protection Act (2010).

7 For example, "Let's Stick Together". Oliver Wyman (2012). Also, "Risk culture in financial organizations: An interim report". The London School of Economics and Political Science (2012).

8 Five sub-factors include risk management culture, risk controls, emerging risk management, risk models and strategic risk management. Standard & Poor's Insurance ERM-Commentary & Criteria: Enterprise Risk Management (May 2013).

North American CRO Council

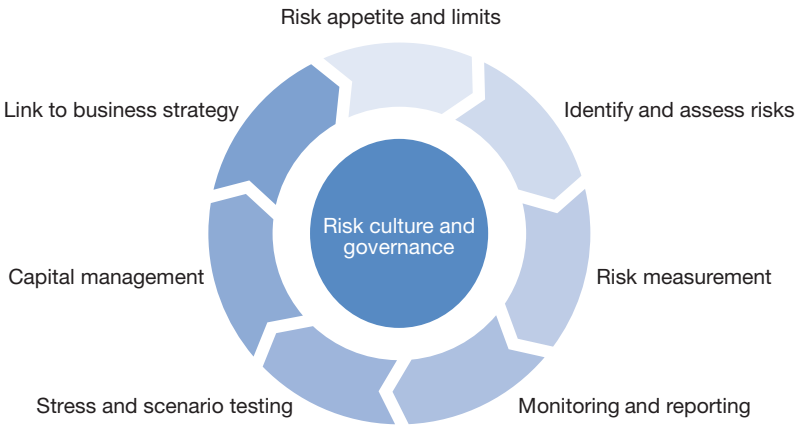
Section III: Aligning risk governance, culture and business objectives

The Council's members believe that sound risk governance and cultural practices form the cornerstones of an effective ERM framework. A comprehensive ERM framework has many interrelated components, including risk appetite and limits; mechanisms to identify, assess, measure and monitor risks; and capabilities to effectively manage capital and link risk to business strategy. As highlighted in Exhibit 1, risk culture and governance underpin the entire ERM framework and provide the foundation for effective risk management.

We believe it is important to emphasize risk governance and culture across organizational layers and require active participation from the Board, Executive Management, Risk Management, and those in risk-taking roles. Each of these stakeholders has an important and distinctive role to play in strengthening enterprise positioning, and consistent engagement is required across the organization to reinforce governance and cultural practices.

Post crisis, in their efforts to strengthen their risk management practices, financial institutions are placing higher reliance on governance and/or cultural aspects depending on their risk profile and the strength of the relationship between the Risk Management function and risk-taking units (Exhibit 2). Emphasizing culture or emphasizing governance mechanisms each have their merits; however, care must be taken to proactively address organizational challenges associated with excessive reliance on either dimension, and to ensure that the strengthening of governance mechanisms such as oversight structures, guidelines and processes is balanced with emphasis on culture.

EXHIBIT 1: COMPONENTS OF AN EFFECTIVE ENTERPRISE RISK MANAGEMENT FRAMEWORK



Source: North American CRO Council.

EXHIBIT 2: POST-CRISIS EFFORTS TO STRENGTHEN RISK MANAGEMENT

High reliance on governance

Characteristics

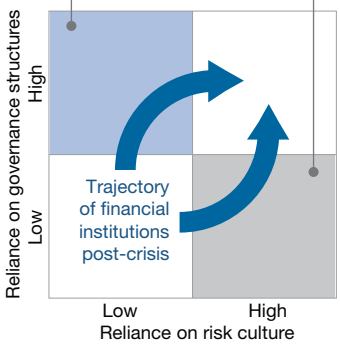
- Clearly communicated and consistently implemented "three lines of defense"*
- Comprehensive and robust policies and limits
- Powerful Risk Management function, "policing" the business
- Enforced through job descriptions and compensation

Strengths

- Clarity around roles and responsibilities
- Tangible framework for communication to external stakeholders, e.g. regulators

Vulnerabilities

- Risk management becomes a "tick box" exercise, with staff following the rules without understanding the principles
- Difficulties when encountering new risks or business conditions – no framework or rulebook can cover all possibilities
- Requires significant governance "overheads" (staff, policies, controls, etc.)



High reliance on culture

Characteristics

- Institutional risk taking philosophy is consistently understood across all parts and levels
- "Hearts and minds" aligned – staff actions and behaviors reflect risk taking philosophy
- Typically "lighter touch" Risk Management function, as business lines require less "policing"
- Enforced through management communications, actions and compensation

Strengths

- Staff empowered to apply principles to new risks or business situations
- More "slimline" Risk Management function and governance framework
- More harmonious "partnership" relationship between risk and the business

Vulnerabilities

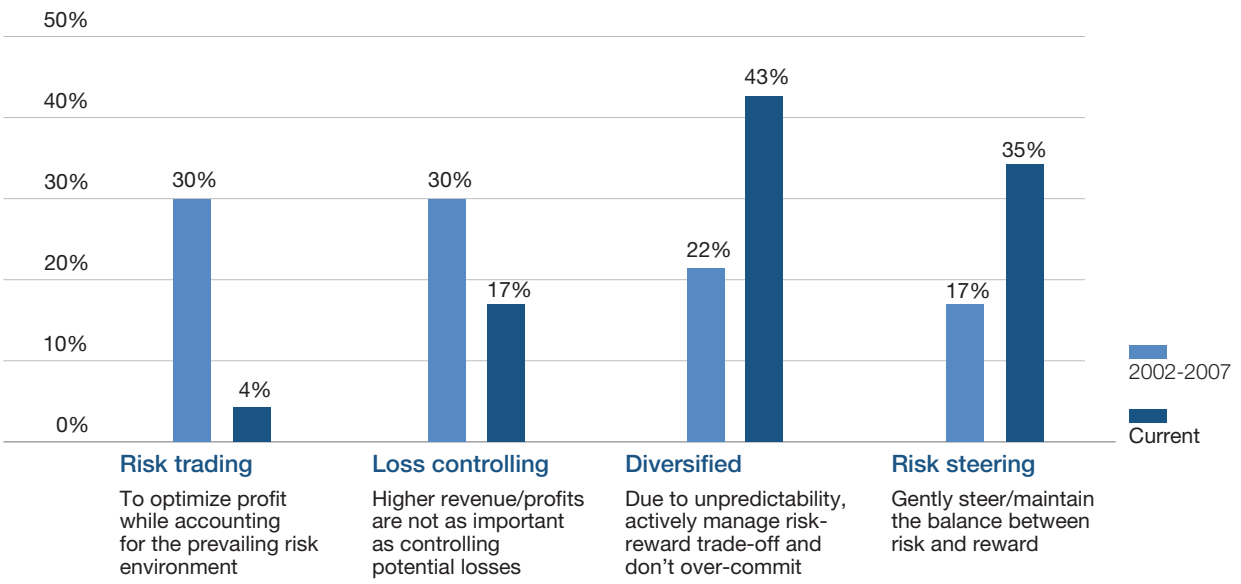
- Newcomers (new hires, staff in acquisitions, etc.) take time to assimilate, resulting in potential risks
- Can be intangible to external stakeholders, e.g. regulators

* For a more detailed description of the "Three Lines of Defense" model please refer to Box 2.

Source: Oliver Wyman analysis.

To support efforts to develop and promote strong risk governance and culture, the Council has, in collaboration with Oliver Wyman, conducted a survey of its membership to document current practices and highlight areas of ongoing development. Survey participants represented a range of sizes, business lines and operating models, and the insights are intended to be generalizable across the insurance industry. From the survey results, we observe that attitudes towards risk-taking are increasingly balanced and are grounded in an appreciation of the need to proactively manage the institutional risk profile. As highlighted in Exhibit 3, insurers are acutely aware of the shifting economic landscape and related impacts on their risk profile and are adopting risk management approaches designed to manage the risk-reward trade-off.

EXHIBIT 3: RISK-TAKING PHILOSOPHY: BEFORE AND AFTER THE FINANCIAL CRISIS



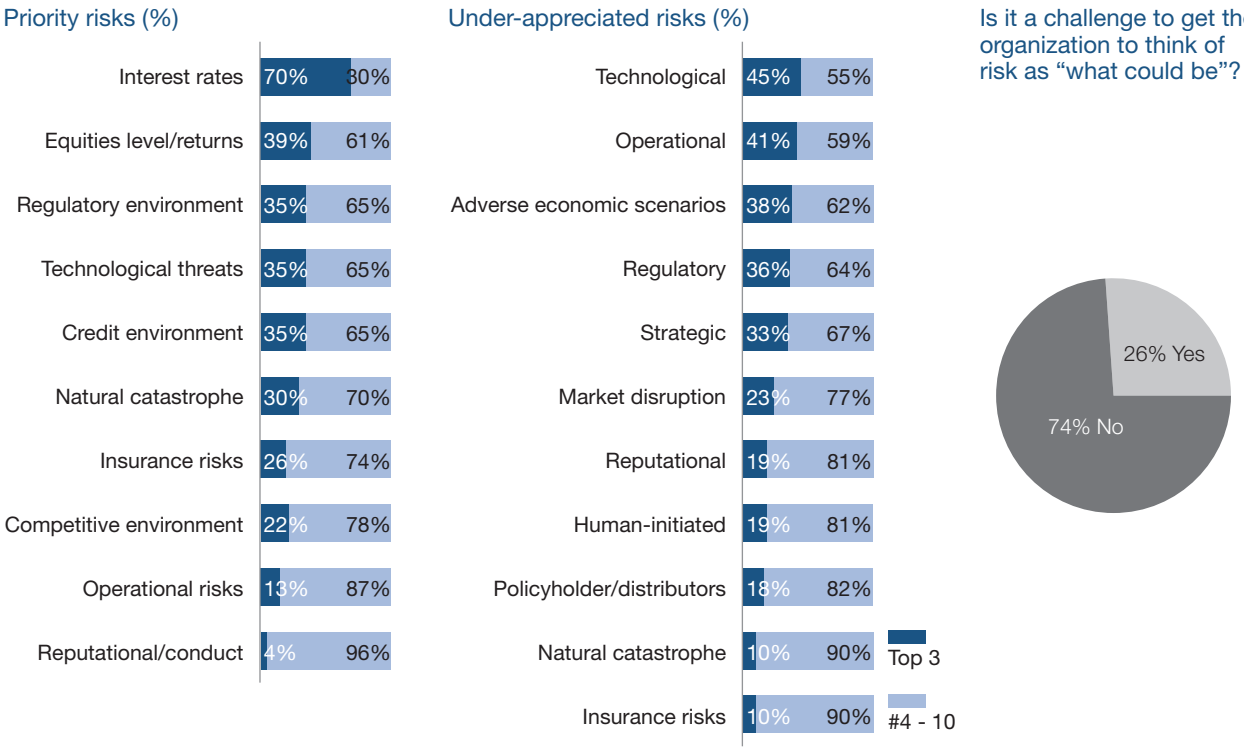
Source: North American CRO Council survey on risk governance and culture.

Since the crisis, insurers' efforts to strengthen risk management have helped to enhance risk awareness. Indeed, as highlighted in Exhibit 4, firms indicated a generally high level of risk awareness and convergence along key risks. As expected, a number of CROs selected interest rates, equity returns and the evolving regulatory environment as high-priority risks. Furthermore, there was a general consensus around key under-appreciated risks, which were dominated by technological and operational concerns as well as considerations of adverse tail economic scenarios.

Given the experience of the financial crisis and the ensuing efforts to bolster risk management, it is not surprising that the majority of CROs did not find it challenging to get their colleagues and the broader organization to think of risk as "what could be" rather than relying excessively on recent historical experience. We observe that heightened risk awareness, along with generally mature risk management mechanisms such as formalized risk appetite frameworks and stress testing initiatives, have enabled the industry to be better prepared to understand and manage risks; however, firms acknowledge that more work remains ahead.

This paper identifies key principles that contribute to sound risk management, including the promotion of sound risk governance practices within insurers (Section IV). In addition, it aims to provide an overview of principles which we believe can help to promote and sustain a healthy risk culture to complement

EXHIBIT 4: RISK AWARENESS AND CONVERGENCE ALONG KEY RISKS*



* Priority risks include the top concerns highlighted by Council members. For instance, 70% of Council members surveyed consider low interest rates as a top 3 risk. Similarly, Council members acknowledged a range of under-appreciated risks.

Source: North American CRO Council survey on risk governance and culture.

and reinforce governance mechanisms (Section V). We recognize that a range of approaches exist for implementing sound risk management and these approaches can vary due to differences in business complexity and strategy, organizational size, risk tolerance and target risk positioning. Despite these differences across individual firms, we believe that the principles espoused in this whitepaper will help firms enhance their risk governance and cultural positioning.

North American CRO Council

Section IV: Sound principles of risk governance

Over the past few years, the insurance industry has placed heightened emphasis on strengthening risk governance practices. Today, many firms continue to enhance their current positioning and plan to further integrate risk management into risk-taking unit processes across the organization (Exhibit 5).

We believe the following principles are hallmarks of effective risk governance:

4.1. Boards, in their mandate to oversee risk, strike the right balance between ensuring risk is managed prudently and allowing for strategic risk-taking within a specified and agreed risk appetite

Since the crisis, there has been considerable focus on strengthening the Board's risk oversight mandate. We believe that the Board plays a critical role in risk oversight and guidance of risk management, enabling pursuit of the agreed-upon risk strategy while simultaneously challenging and actively shaping risk policy.

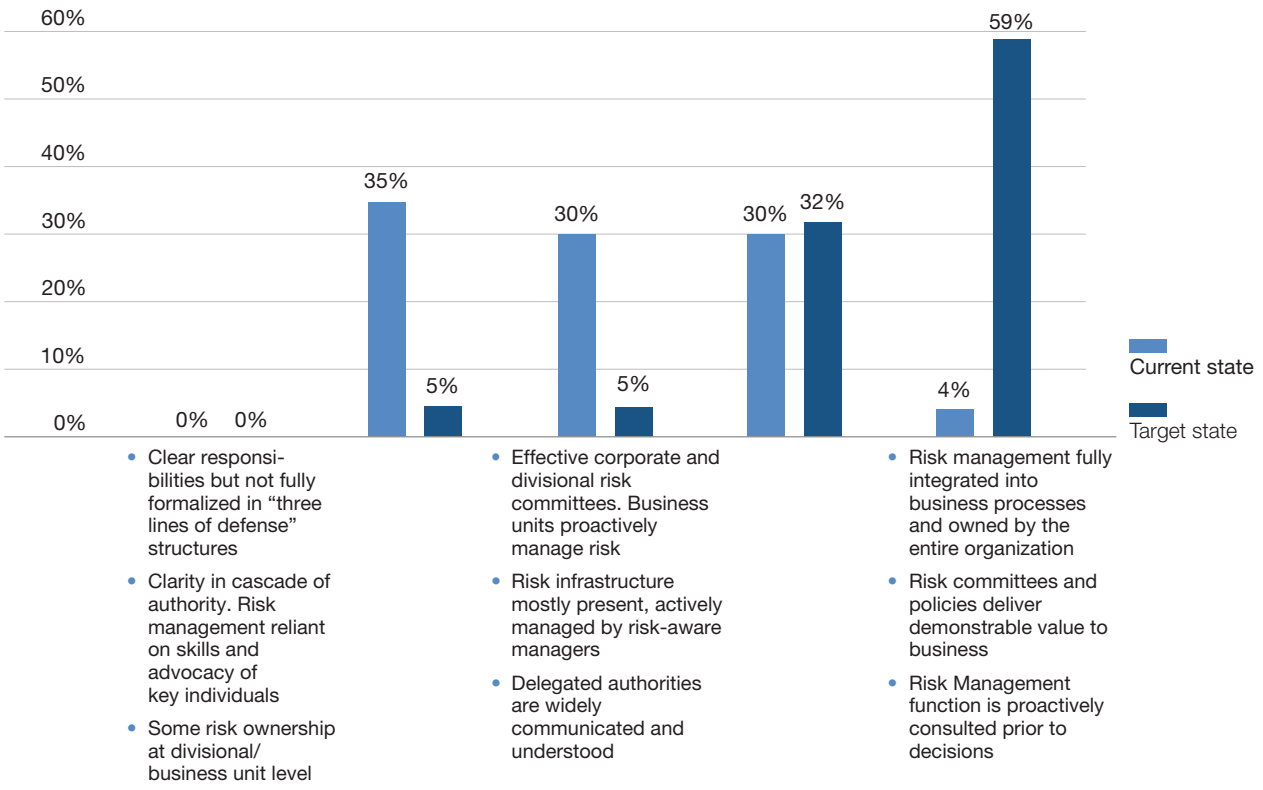
This view is supported by a number of industry publications which articulate and reinforce the importance of the Board's role in risk governance. For instance, the Walker review[9] recommends that the Board must ensure that risks taken by the institution are in line with Board and investor expectations. Similarly, FSB in its review of risk governance[10] recommends that the Board should ensure that Executive Management has sufficient processes in place to ensure firm's adherence to approved risk policies.

We note that effective Board involvement can take different shapes depending on the individual needs of the organization and the characteristics of the Board. Industry practices range across insurers, with some of our members preferring to engage the entire Board on risk topics. Alternatively, a few of our members mandate individual Board committees to manage specific risk components (e.g. investment committee manages investment risk) while others mandate a single Board committee to oversee enterprise risk issues (i.e. Board Risk Committee). We believe all of these constructs have merit as long as they ensure sufficient Board attention towards and engagement on risk topics.

9 Walker Review, A Review of Corporate Governance in UK Banks and Other Financial Industry Entities (Nov 2009).

10 Financial Stability Board, "Thematic Review on Risk Governance" (Feb 2013).

EXHIBIT 5: RISK GOVERNANCE PRACTICES: CURRENT AND TARGET STATES



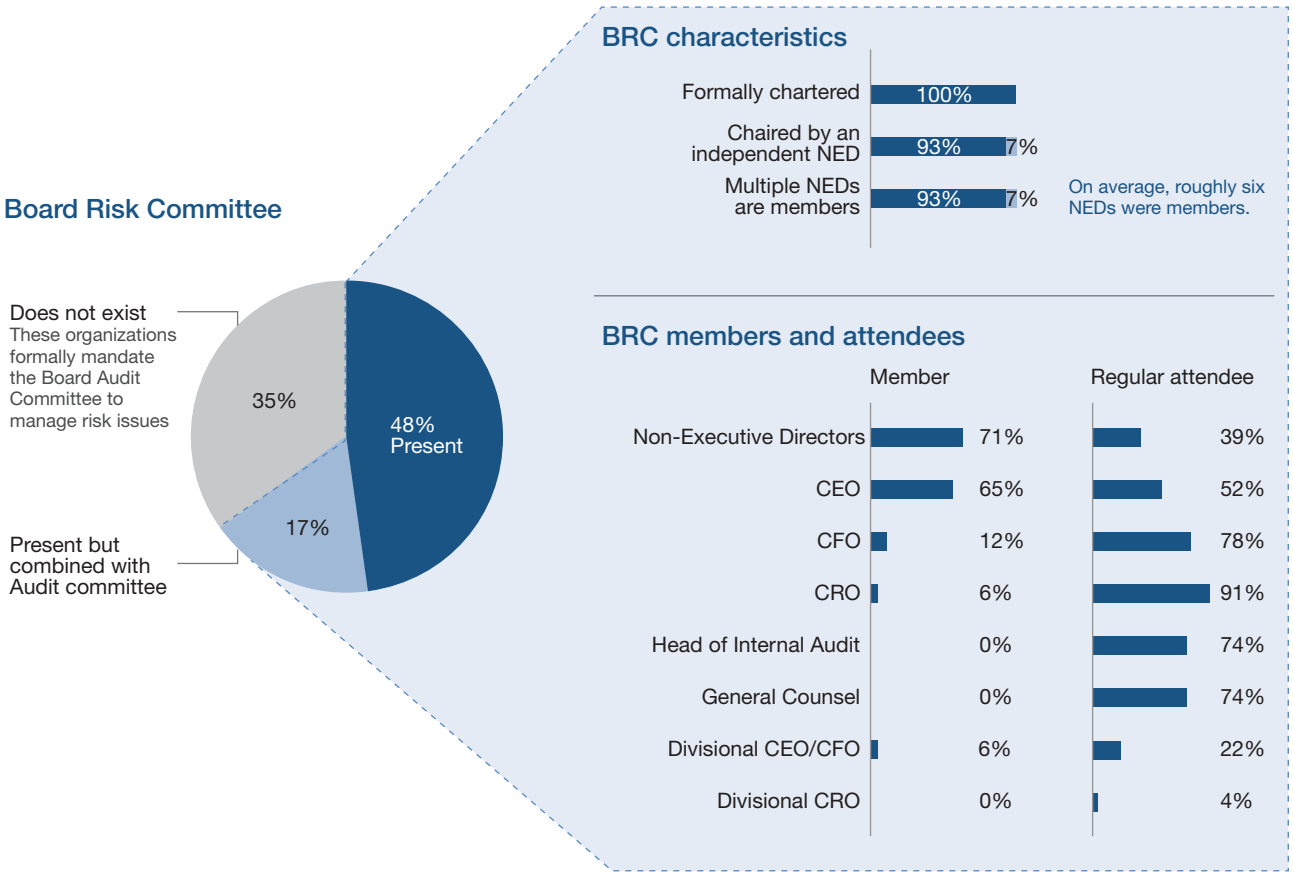
Source: North American CRO Council survey on risk governance and culture.

In practice, an increasing number of our members find it helpful to create dedicated Board Risk Committees (BRC). In fact, BRCs were present across roughly 65% of firms surveyed (Exhibit 6). For those which did not establish BRCs, Board Audit committees were formally mandated to manage risk issues. BRCs, when present, were typically chaired by an independent Non-Executive Director (iNED) and comprised of the CEO and several iNEDs, ensuring their independence and ability to provide oversight of risk topics.

4.2. Boards have the resources to deliver on their mandate

Insurers should create the right conditions for the Board to be in a position to effectively deliver on its risk oversight mandate. In terms of Board membership and skill set, we note that there is value in diversity of expertise at the Board, and Board members should embody a balance between business and risk expertise. However, there is a minimum level of fluency in risk topics which is critical for Boards to

EXHIBIT 6: BOARD COMMITTEES MANDATED TO DEAL WITH RISK TOPICS

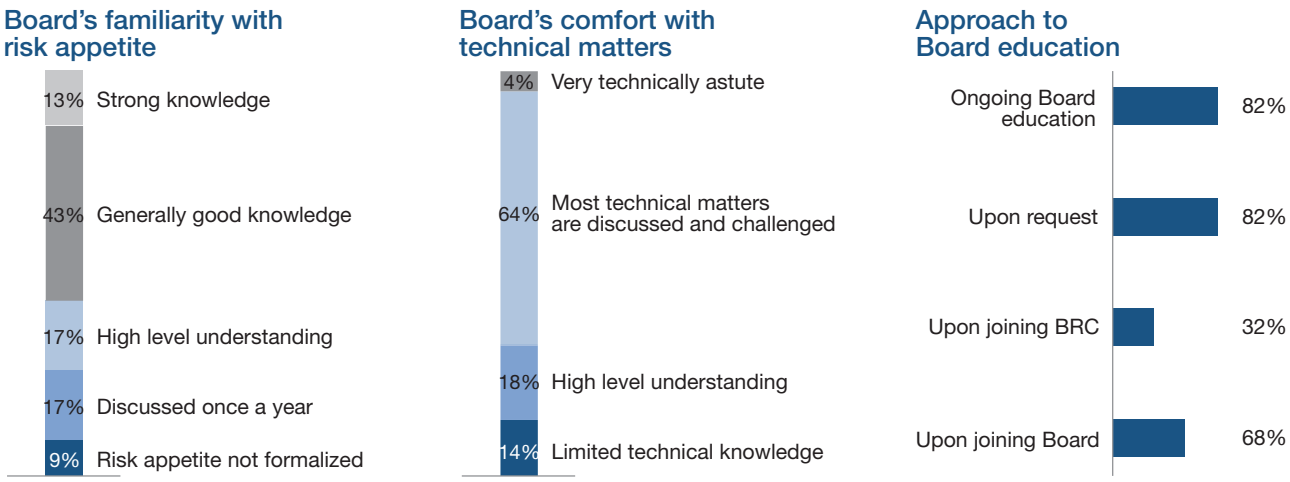


Source: North American CRO Council survey on risk governance and culture.

evaluate the implications of management decisions on the institutional risk profile. Since the crisis, an increasing number of our members have added Board members with proven expertise in risk management to enable the Board to effectively discharge its oversight mandate.

Boards should receive the relevant training, insights and thematic updates to enable them to provide effective risk oversight. Encouragingly, across survey participants we observe that the majority of Boards have a good understanding of technical topics and actively discuss and challenge technical matters. Nonetheless, firms are actively seeking to strengthen their Board's capabilities, and roughly 80% organize on-going Board education and training programs to ensure that Board members possess sufficient understanding to effectively discharge their risk oversight mandate (Exhibit 7).

EXHIBIT 7: BOARD RISK CAPABILITIES AND APPROACH TO BOARD EDUCATION



Source: North American CRO Council survey on risk governance and culture.

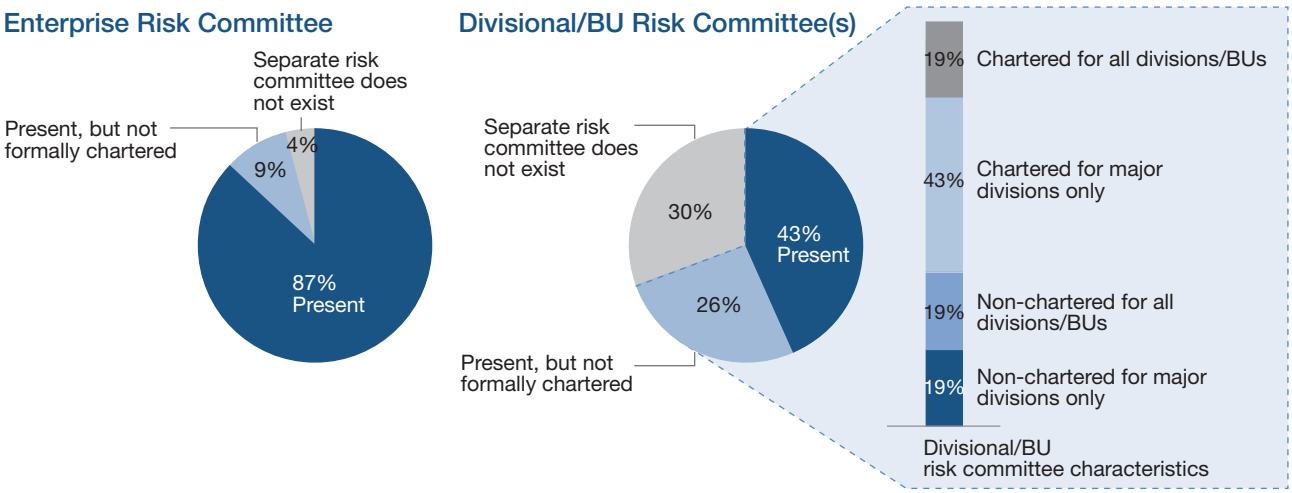
Our members are increasingly supporting Boards through access to senior executives and with timely, well-structured risk information, enabling and encouraging regular risk-focused discussions. Furthermore, insurers recognize that clearly defined risk appetite and risk policies are essential as they allow the Board to evaluate business decisions and strategies from a risk standpoint.

4.3. Risk management is a shared executive priority

We believe risk management should extend beyond the domain of the Risk Management function to be an explicit executive priority. Emphasis on the importance of sound risk management practices should not be limited to Risk Management professionals, and there should be a broad appreciation amongst risk-taking unit leaders that risk management is a critical enterprise objective. Good examples include efforts to formally articulate the institutional risk appetite and cascade quantifiable risk limits, efforts to ensure effective partnership between the Risk Management function and risk-taking units, and structures and processes which ensure that the Risk Management function's stature is sufficient to execute its mandate. We note that firm-specific emphasis on particular enablers varies depending on the business model and risk-taking philosophy.

Amongst our members, the Executive Risk Committee (ERC) is widely considered to be the primary platform for risk-taking unit leaders and Risk Management officers to discuss risk topics and align on organizational approach to risk management. Today, almost all Council members have ERCs, a majority of which are formally chartered and are designed to ensure sufficient executive focus on risk issues at both the enterprise and divisional levels (Exhibit 8). ERCs had

EXHIBIT 8: PREVALENCE OF RISK COMMITTEES



Source: North American CRO Council survey on risk governance and culture.

significant executive participation and included risk-taking unit leaders, the CRO and key executives such as the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Investment Officer (CIO).

4.4. Risk Management function is independent, effective and influential

Independence of the Risk Management function is critical. Risk Management professionals should be enabled to effectively deliver on their mandate to manage risk and need to have unfettered access to senior leaders and the Board. It is critical that the stature and organizational placement of Risk Management professionals, including the CRO, be commensurate with the importance of their role and reinforces their ability to escalate risk issues.

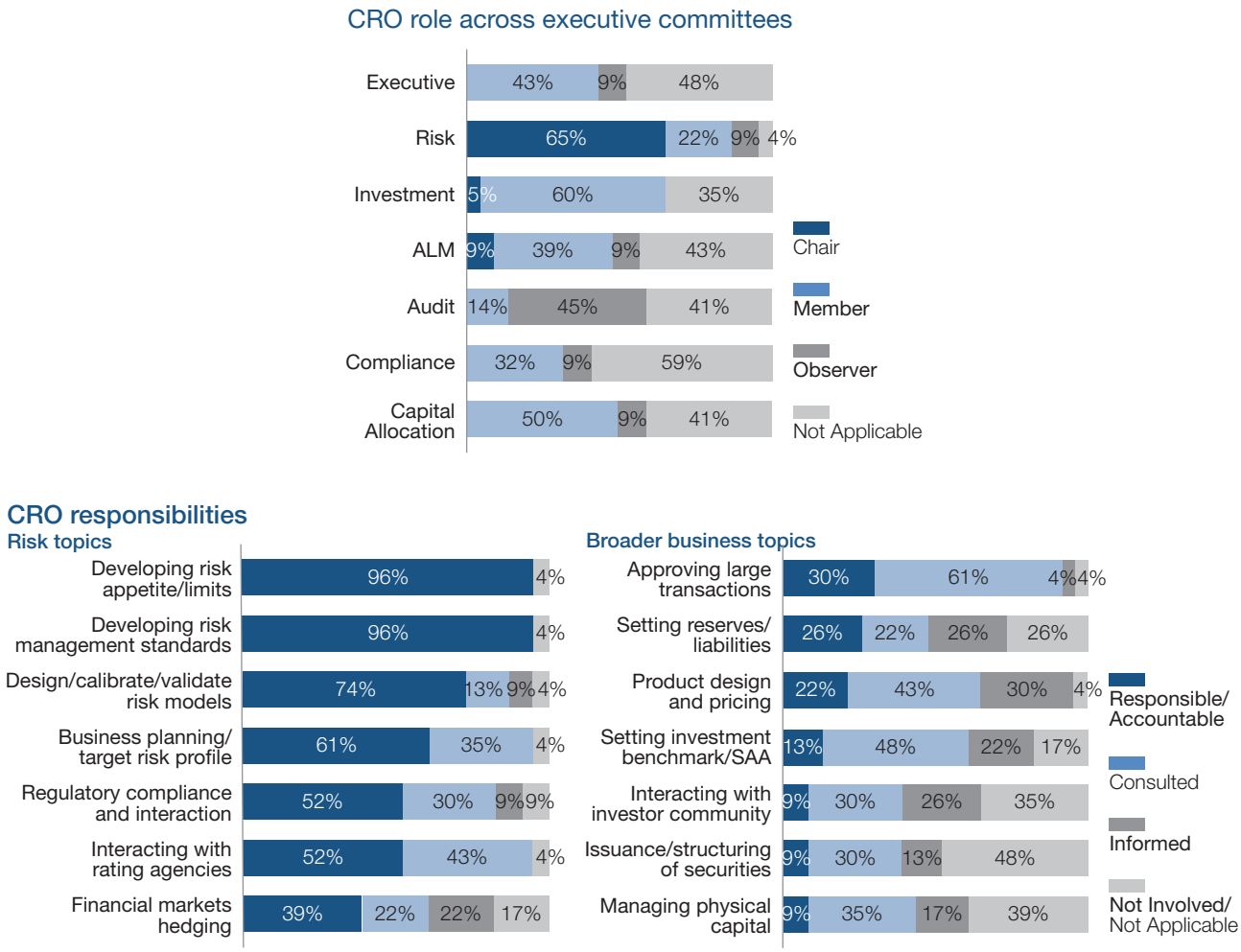
We observe that the corporate CRO position is now ubiquitous within Council members. Many firms identified the ideal corporate CRO reporting structure as a dual report to the CEO and to the Chair of the BRC, so as to strengthen the independence and influence of the Risk Management function. In practice, corporate CROs typically report to the CEO and/or CFO and hold quarterly meetings with Executive Management including the CEO and Chair of the BRC. Today, the majority of corporate CROs at our member firms have regular access to the Board and issue regular risk reports to the Board and ERC.

Firms vary in organizational placement of corporate CROs, but, encouragingly, many emphasize corporate CRO participation in key executive-level committees and connect corporate CROs with core business processes affecting risk (Exhibit 9). The corporate CRO typically chairs the ERC and is an active participant across other executive committees including the

investment, asset liability management (ALM) and capital allocation committees. Not surprisingly, corporate CROs are responsible for issues such as the development of risk management standards and risk appetite/limits. Critically, corporate CROs often hold key roles in broader business activities such as strategic asset allocation, investment benchmark setting and capital management.

While we believe that there is no ideal size for the Risk Management function, it is essential that Risk Management be appropriately sized and staffed relative to the complexity of business and the institutional risk profile. Amongst our members, we observe that the size, mandate and organizational structure of the Risk Management function varies significantly. For instance, across survey participants, Risk Management

EXHIBIT 9: CROs ROLE AND RESPONSIBILITIES



Source: North American CRO Council survey on risk governance and culture.

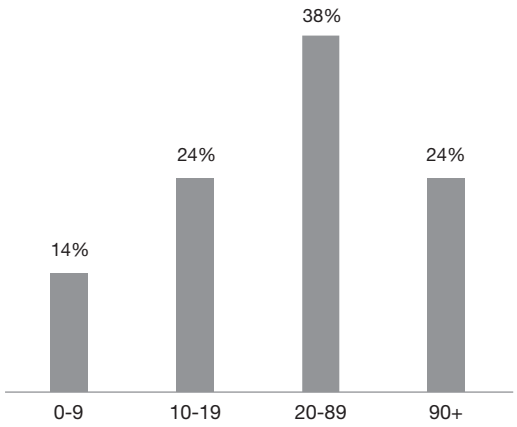
functions ranged from fewer than 10 employees to over 90 employees, (Exhibit 10). Similarly, the scope of the risk organization varied widely. For example, a few firms included actuarial areas within their Risk Management function, while others placed regulatory risk areas in the compliance organization rather than within Risk Management. Furthermore, Risk Management mandates varied due to business complexity as well as overlaps and variations within the first and second line of defense responsibilities.

4.5. Risk organization is well aligned to the risk-taking units

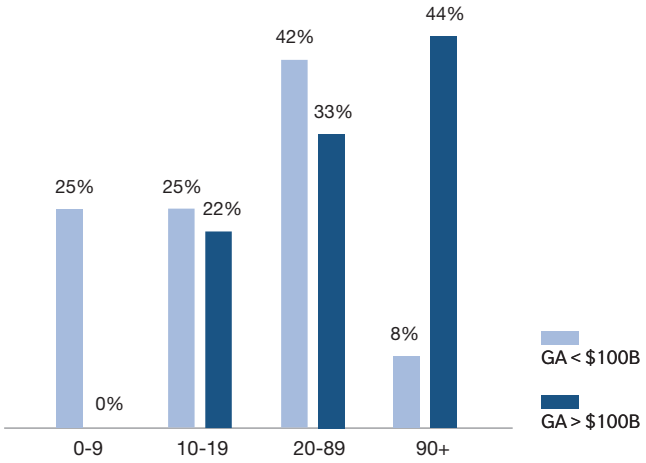
We recognize that there is no single ideal structure for the Risk Management organization and risk activities should be effectively aligned with the business model, with clear visibility into risk-taking and with timely access to risk information. Risk Management function and risk-taking unit alignment is essential along multiple dimensions including organizational placement,

EXHIBIT 10: SIZE OF THE RISK MANAGEMENT FUNCTION ACROSS INSURERS

Size of risk function
Corporate and divisional risk functions



Resourcing break down by company size
General account (GA) assets above and below $100B



Source: North American CRO Council survey on risk governance and culture.

capabilities and incentive structures. Amongst our members, the structure of the risk organization varies significantly, with companies tailoring components to best suit their business needs and risk profile; for example, a number of firms utilize sizeable divisional risk areas.

We note that our members are making progress in enhancing the organizational structures of risk management. Today, the "three lines of defense" organizational model – which emphasizes the independence of the risk organization and facilitates regulatory compliance – is increasingly commonplace (Box 2). It is essential that the Risk Management function has a strong relationship and frequent interactions with risk-taking units as well as other control functions. Indeed, roughly 90% of Council members indicated frequent interaction between Risk Management and other control functions both formally through various committees and informally through proactive consultation on key risk issues.

We do not believe that there is a single "right" answer to risk organization and governance as institutions that have demonstrated sound risk management employ a range of approaches. Depending on the company, Risk Management professionals may be ideally situated in central or decentralized departments; for example, organizations with high degree of decentralized risk taking may optimally choose to have a decentralized Risk Management function. Common organizational structures for Risk Management range from the classic "federal" model, which includes risk-taking unit aligned risk functions with solid reporting lines to the CRO, to the "holding company" model, characterized by a more distributed risk function (Exhibit 11). We believe that regardless of the organizational structure and size of the risk function, it is critical to ensure the effectiveness of risk management and to test independence, comprehensiveness of coverage, authority (stated and actual/behavioral), culture, and structural ability to outlast specific executives.

Council members are making efforts to further embed risk considerations and promote active risk management within risk-taking units. These efforts emphasize formal and on-going dialogue between the Risk Management function and risk-taking units, and are supported by increased divisional involvement in the development and application of risk limits. Along

Box 2: "Three Lines of Defense" model

The Three Lines of Defense model (3LoD) is a useful framework to assess the independence and effectiveness of a Risk Management-related organizational structure. In a traditional 3LoD structure, the first line of defense (i.e. the risk-taking unit) has day-to-day responsibility for taking and managing risk.

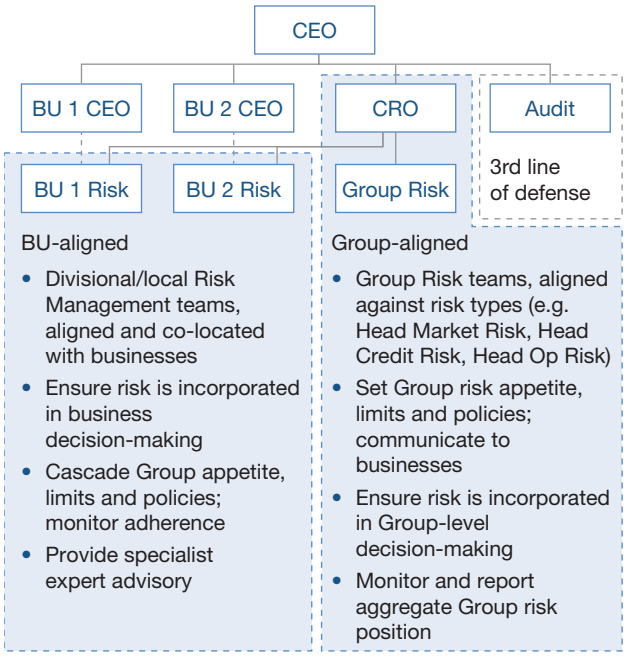
The second line of defense is an independent group (typically Risk Management) which is responsible for overseeing the risks being taken by the first line to ensure these remain within acceptable bounds and align with the institution's risk appetite. This group is also responsible for establishing and monitoring boundaries and controls which may take the form of policies, limits, usage restrictions, etc.

The third line of defense is always represented by Internal Audit. Internal Audit has responsibility for ensuring that both the first and second line of defense are fulfilling their respective responsibilities. Audit typically has its own independent reporting structure through the Chief Auditor directly to the Audit Committee of the Board of Directors to ensure that Audit receives appropriate stature within the organization.

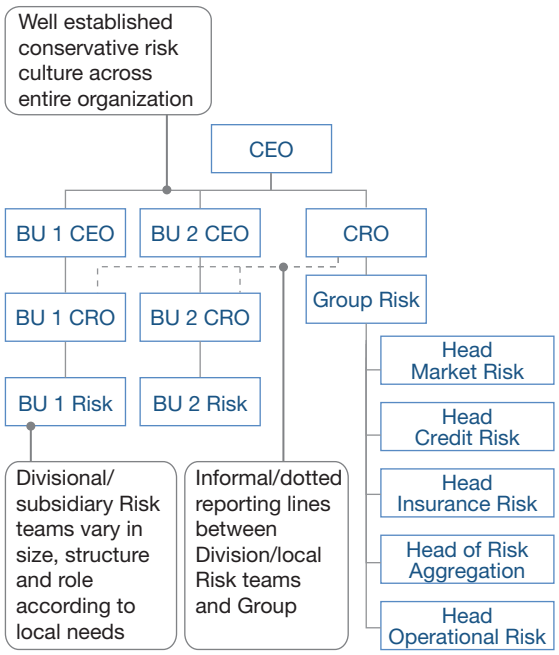
Source: Oliver Wyman analysis.

EXHIBIT 11: COMMON STRUCTURES FOR THE RISK ORGANIZATION

Example 1: "Federal Model"



Example 2: "Holding Company" model



Source: Oliver Wyman analysis.

with these initiatives, about 70% of participants have created divisional risk committees (Exhibit 8), which function similarly to the ERC but are distinctively closer to front-line risk-taking units. In addition, roughly 75% embed divisional CROs within risk-taking units. Divisional CROs, when present, typically report to divisional CEOs, with a secondary reporting line to the corporate CRO and act as advisors to divisional management and as liaisons with the corporate Risk Management function. Notwithstanding this, many corporate CROs report active involvement in appointing and evaluating divisional CROs.

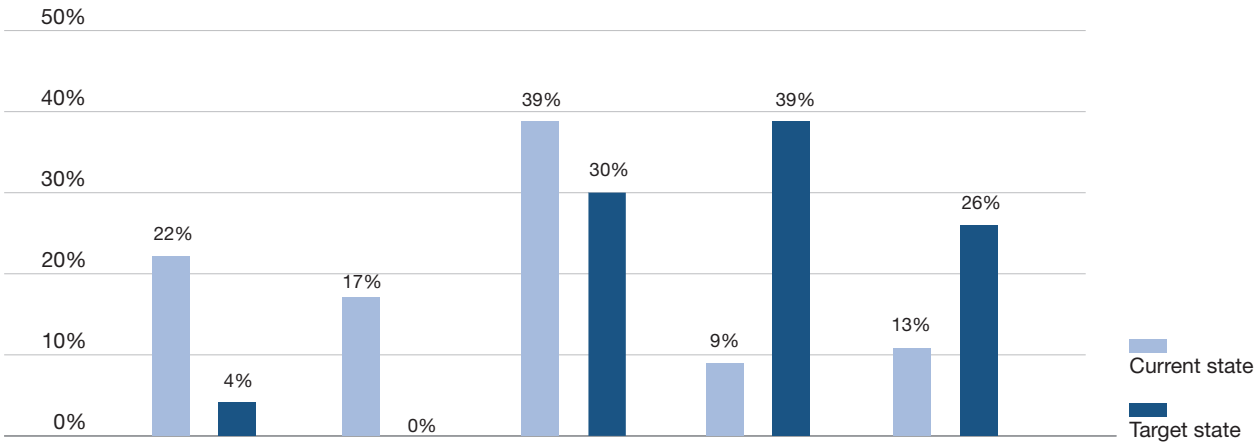
North American CRO Council

Section V: Sound principles of risk culture

Across the financial services industry, emphasis on risk culture topics has historically been somewhat less commonplace than focus on the more formal aspects of risk governance, and insurers correspondingly manifest a variety of states of risk culture development (Exhibit 12). However, there is a general acknowledgement that governance mechanisms need to be complemented with a strong risk culture, especially within risk-taking units.

Risk culture can be broadly considered as the shared understanding and behavioral attitudes of an institution's people towards risk-taking. Numerous intangible components make risk culture difficult to measure and evaluate; nonetheless, it is viewed as critical to an organization's health, and Council members acknowledge the need to proactively define and shape it. To evaluate pressure points within cultural dimensions and target areas for improvement, a number of insurers have turned to the use of diagnostic tools

EXHIBIT 12: RISK CULTURE PRACTICES: CURRENT AND TARGET STATES



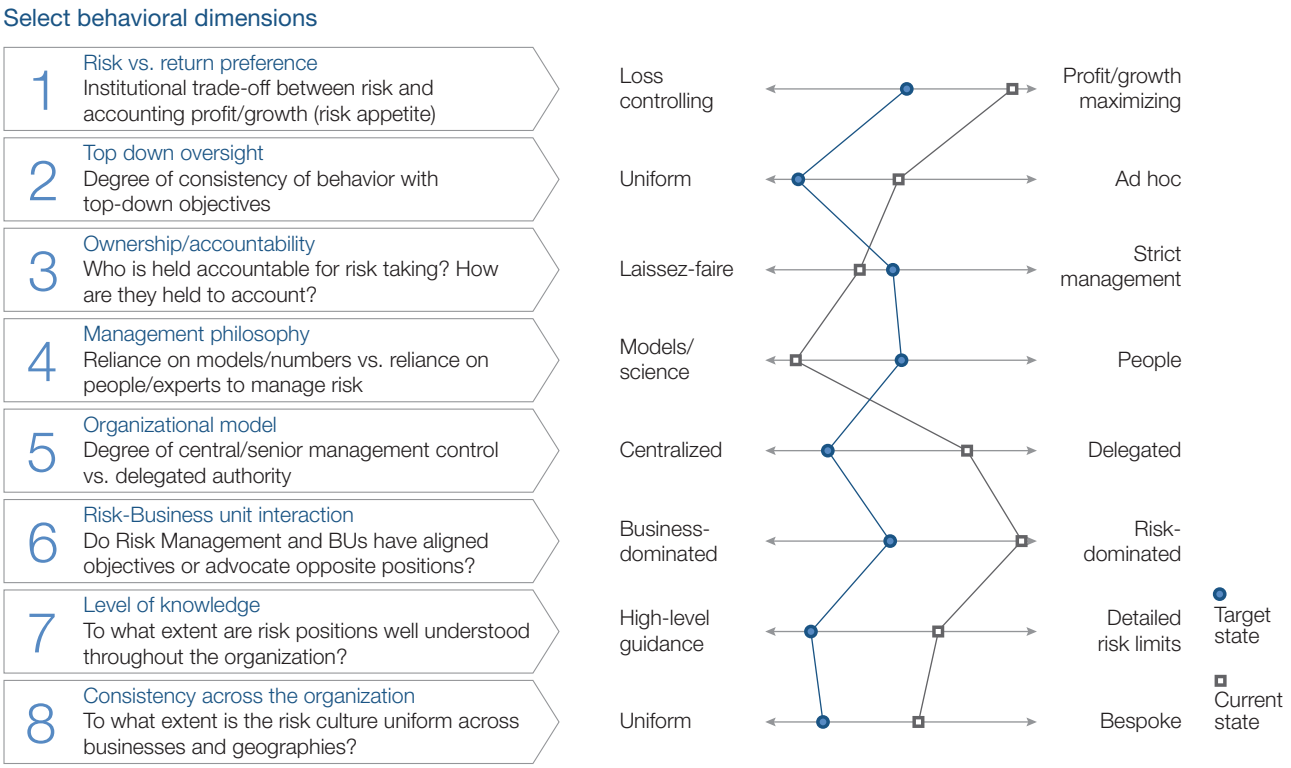
- Executives actively support risk management. BU consistently engaged with Risk or Audit
- Broad communication on detailed risk policies
- Risk performance not explicitly linked to employee incentives. Organization is risk aware and cognizant of lessons learned

- Openness and proactive participation by BU in risk management
- Executives set tone from top via frequent, high quality dialogue
- Risk performance linked to individual incentives and consistently measured. Culture reflects local differences in scale, nature

- Risk Management commercially oriented, perceived to offer competitive advantage
- Senior Management behaviors consistent with communication
- Risk performance linked to executive incentives. Underperformance in relation to risk management unacceptable

Source: North American CRO Council survey on risk governance and culture.

EXHIBIT 13: SAMPLE ASSESSMENT ALONG BEHAVIORAL DIMENSIONS OF RISK CULTURE*



* Firms utilize detailed assessment templates to evaluate current and target cultural states; this exhibit includes a high-level sample template.

Source: Oliver Wyman analysis.

and workshops (Exhibit 13). These tools help collate opinions from various stakeholders, assess attitudes and behaviors, and test participants' understanding of risk policies and the roles and responsibilities of different teams. We note, however, that even when institutional culture is well understood, it can take longer to drive cultural change purely due to the fact that it is more difficult to change hearts and minds than to change governance structures and policies.

The following principles are hallmarks of a healthy risk culture:

5.1. Board and Executives prioritize effective risk culture

"Tone from the top" is a crucial factor in instilling a strong risk culture. Indeed, roughly 70% of Council members identified Executive Management attitude

as a critical tool to strengthening risk culture. We note that the culture of an institution can be difficult for a Board or Executive Management to effectively articulate, especially at large, complex, globally operating financial institutions. Nonetheless, it is imperative that the Board and Executives clearly define attributes of their desired culture; and promote and reinforce desired behaviors through a clear, consistent and well understood risk appetite framework. To this end, although only 10% of firms have formally articulated their risk culture objectives to date, all respondents indicated a desire to define and strengthen their risk culture along key behavioral dimensions, highlighting industry trajectory.

Across a number of firms, aspects of risk culture were characterized as relying extensively on the leadership of executives. We believe that Executive Management should lead by example, be consistent within their communications and actions, clearly articulate the firm's risk appetite and desirable risk-taking activities, and lead in such a way as to demonstrate ownership of and accountability for embedded risks, as these factors significantly influence institutional risk culture. Given the importance of executive leadership for building a healthy risk culture, a number of firms are focused on raising risk awareness at the executive level. Across the industry, firms utilize a range of tactical mechanisms to raise risk awareness. Many emphasize the candor and openness required for employees to raise concerns; others focus on promoting an environment of effective challenge and collaboration in which the entire organization comes together to enable a positive, critical attitude towards risk-taking and to align around common long term interests; and a number opt to measure employee opinions through anonymous surveys and interviews. Regardless of the preferred method, it is crucial that firms avoid becoming complacent and we support the idea of utilizing a range of mechanisms to measure, monitor and strengthen key cultural aspects.

It is also important for Boards and Executive Management to have access to and make effective use of experts, be they internal or external. As noted by the Basel Committee[11] and the Walker Review,[12] independent expert advisors can provide insights into market conditions, emerging trends and evolution of risk management best practices, all of which are necessary for the Board and Executive Management to maintain risk awareness and effectively deliver on their responsibilities. Similarly, firms are strengthening their awareness of emerging risks. Today, roughly 80% of Council members have teams formally mandated to identify and evaluate emerging risks for senior leadership.

We believe that firms should further embed risk awareness through the development of risk-aligned performance measures and compensation frameworks that would guard against imprudent risk taking and strengthen risk management. In addition, we believe that a strong risk culture motivates compliance with risk limits through an understanding of their validity and utility while recognizing where the understanding is flawed. Thus, a risk-aware culture is instrumental in motivating employees towards prudent risk taking in line with organizational risk appetite.

11 Basel Committee on Banking Supervision, Principles for the Supervision of Financial Conglomerates (Sept 2012).

12 Walker Review, A Review of Corporate Governance in UK Banks and Other Financial Industry Entities (Nov 2009).

5.2. Risk-taking units are key actors in a risk-aware culture

Risk culture concerns the cultural and behavioral practices related to risk management across the entire organization, not just within the Risk Management function. It is particularly important to maintain a strong and consistent risk culture within front-line risk-taking units and to ensure that all parts of the organization maintain a manageable risk profile and do not take disproportionate risks or place outsized bets. The Board and Executive Management must encourage risk awareness and a strong risk culture across the organization, particularly within emerging, isolated or high-risk areas such as acquired businesses, international operations, or small but growing business units, as it is often in these areas that a sub-optimal culture can develop unnoticed leading to risk failings.

To this end, Council members recognize the need for a stronger relationship and balance in authority between the Risk Management function and risk-taking personnel. Given the complexity of insurance products, risk-taking units need to effectively partner with the Risk Management function to ensure that an appropriate and enabling risk appetite is established and, subsequently, risks remain within the institutional risk appetite.[13]

We observe that insurance accounting standards and the underlying product economics diverge across a number of dimensions, and there is active discussion amongst regulatory, industry and accounting bodies to resolve these differences. Nonetheless, given these differences and the complex nature of insurance products, it is essential that rules and incentives reinforce effective risk management across front-line units.

Our members identify embedding explicit risk and return objectives as one of the biggest challenges to strengthening risk culture and are converging on the view that risk-adjusted incentives across risk-taking units are critical. Today, roughly 40% of survey participants include explicit risk objectives within their performance measurement and compensation structures, highlighting a growing trend. This notion is further supported by IIF's Market Best Practices, which states that incentive compensation should be based on risk-adjusted performance and should contain a component reflecting the firm's achievement of risk management goals.[14]

5.3. Risk education, communication and transparency are emphasized

To strengthen risk culture, the Risk Management function should emphasize communication and education. Frequent and effective communication across organizational layers is critical to raising awareness of the firm's risk appetite and instilling a strong and transparent risk management framework. We believe it is imperative that consistent focus is placed on enhancing the quality of dialogue and engagement between the Risk Management function, other control functions and risk-taking units.

Effective communication and risk reporting form an integral part of the efforts to strengthen risk culture. Executive Management and the Board need timely, accurate and comprehensive reports on current and projected risks relative to the firm's risk appetite, under both regular and stressed conditions. Across the industry, Boards and Executive Management often felt that the form and content of risk reports

13 For additional details on the Council's perspective on risk appetite, please refer to "Establishing and Embedding Risk Appetite: Practitioners' View"; a joint publication by the North American CRO Council and the CRO Forum (Dec 2013).

14 Final Report of the Committee on Market Best Practices; Institute of International Finance (July 2008).

can be improved. Care must be taken to avoid risk reporting which is too detailed, overly technical or lacking actionable recommendations, all of which reduce the ability of Executive Management and the Board to provide effective oversight.

We believe that ongoing education and training should be emphasized, such that risk-takers, Risk Management professionals, Executives and the Board are all aligned in their understanding of the desired posture towards risk. Given the intangible nature of risk culture, it is critical that preferred behaviors be explicitly and consistently identified, promoted, reinforced and celebrated. The Risk Management function in particular should ensure general acknowledgement and appropriate support of individuals and behaviors that prove to be effective cultural carriers. Organizations currently utilize a variety of tactical approaches in this regard; for instance, a number of firms are making efforts to eliminate the fear that the expression of dissenting opinions would be viewed as offensive or disloyal and proactively encourage diversity of thought and challenge across the organization.

North American CRO Council

Section VI: Conclusion

We observe that the insurance industry has made strong progress since the crisis and recognizes risk governance and culture as foundational aspects of risk management. Although a number of ERM priorities, such as strengthening risk processes and embedding risk appetites, are critical and deserve immediate attention, the industry is also placing higher emphasis on strengthening risk governance and culture practices. We believe that diversity in industry's approach to risk governance and culture is important. Rules which dictate otherwise will stifle the vibrant risk management ecosystem across the insurance industry and may potentially create the kind of systemic risks regulators are working to avoid.

We believe that the heightened regulatory scrutiny, shareholder interest and the general acknowledgement amongst insurers for the need to do more will reinforce this progress. It is essential that governance and culture mechanisms are aligned with business objectives and promote and enable sound risk management. To accomplish these objectives, it's imperative that governance and cultural aspects are continuously renewed and refreshed. We hope that the principles outlined in this paper will catalyze further, positive efforts in support of a healthy and vibrant insurance industry.

North American CRO Council

Appendix: Survey methodology and contact details

The North American CRO Council is an association of Chief Risk Officers (CROs) of 30 insurers across North America and seeks to develop and promote sound industry practices in risk management. Oliver Wyman was engaged by the North American CRO Council ("Council") to assist in developing and promoting sound practices in regards to risk governance and culture. Council members represent 30 of the largest insurers across North America, including:

- 12 of the 15 largest North American Life insurers
- 12 of the 15 largest North American Property & Casualty insurers

The survey was designed to document the diversity of current practices and to identify emerging trends as well as common pressure points within the industry. Twenty three companies participated, representing a broad range of sizes, business lines and operating models.

Importantly, the survey was not intended to evaluate or judge the adequacy of risk management practices across the industry. We recognize that requirements and implementation can differ greatly across organizations due to multiple factors including organizational size, business complexity, level of risk tolerance as well as current and target risk positioning.

Further, we recognize that there is no single correct approach to risk management. Indeed, the practices highlighted within this survey do not represent all mechanisms that could be employed to enable sound risk management.

For questions or to further discuss the paper, please contact the CRO Council. The CRO Council is supported by a Secretariat. For more information please contact secretariat@crocouncil.org.