Bank Governance Leadership Network
ViewPoints

January 12, 2012

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Progress on the risk governance journey, but key challenges remain

Risk governance has evolved rapidly, and tremendous energy and investment have gone into implementing policies and processes to improve banks' ability to identify, monitor, and manage risk and to improve regulators' ability to monitor systemic risk. Most banks and regulators have made significant changes to the manner in which they oversee risk, including changing out some of the directors, executives, and supervisors involved. Risk committees have been established or reconstituted, and many chief risk officers (CROs) are relatively new to their roles (some firms are on their second or third CRO in as many years). Many of the officials involved in setting or monitoring risk are also new or have new roles.

Are these investments in improvements paying off? Questions remain regarding how banks and supervisors should assess risk governance effectiveness, what level of further investment is appropriate, how coordination with and among supervisors can improve, and, ultimately, how banks can determine if they are striking the right balance between risk and reward. Answers to these questions are key to achieving the desired final goal of executives, board directors, and supervisors alike – stronger, more stable institutions.

During the past three years, the Bank Governance Leadership Network (BGLN) has worked extensively to enable a dialogue on risk governance. We have conducted hundreds of discussions on risk with chief risk officers, directors,[1] and regulators[2] through the BGLN, and at all of the 16 BGLN meetings held to date, risk has either been a topic or has been raised in discussion.

This *ViewPoints* offers five discrete sections on progress on risk governance in the banking industry. It draws on over 120 discussions in 2011, as well as several meetings in which we brought CROs, directors, and supervisors together to discuss risk.[3] The following key themes emerged from the discussions:

- **Risk appetite frameworks remain hard to implement, and the industry and supervisors debate the degree of progress made.** Many were initially skeptical about the practical value of risk appetite statements, but most now agree they have enabled better board and management dialogue. Significant implementation challenges remain, including incorporating operational and reputational risks, communicating the statements effectively, linking them to existing risk limit structures, and linking risk appetite statements to returns and capital allocation decisions. Convincing supervisors progress has been made remains challenging, too.
- **Instilling and monitoring a risk culture that supports the risk appetite is essential.** Ultimately, no risk appetite statement can take every situation into account. Institutions must have strong risk cultures that actively support their chosen risk appetite. Industry participants advocate a focus on the mosaic of behaviors exhibited across the bank. Key ingredients include a consistent tone at the top,

[1] In this document, "director" refers to non-executive, non-employee board members on a firm's unitary or supervisory board.

[2] In this document, "regulator" refers to any agency responsible for the development and implementation of rules-based regulatory regimes, and "supervisor" refers to any agency responsible for oversight of management and board actions within those regulatory regimes.

[3] All discussions were held under a modified version of the Chatham House Rule that encourages sharing of perspectives but absolutely forbids attribution to individuals or institutions. All comments from BGLN participants are italicized. A complete list of interviewees and discussion participants can be found in the Appendix, on page 29.

proper metrics, properly monitored, established escalation processes, an open culture, and consistent enforcement.

- **Boards and supervisors have a central role to play driving necessary upgrades to bank risk IT systems.** Discussion of risk inevitably has IT infrastructure implications. Ideally, banks need risk IT systems that can gather risk information quickly and comprehensively, producing global, cross-product, cross-legal entity estimates of their exposures within hours. But many banks fall short of that ideal. Many directors and executives acknowledge the need for a step change in the magnitude of investment and oversight of risk IT, and they agree that supervisors could play a critical role in assuring improved risk IT systems are put in place.
- **Ultimately, banks have to invest more in identifying and reacting to emerging risks.** Directors are not entirely convinced that banks are better positioned to spot emerging risks now than they were prior to the financial crisis. Directors, executives, and supervisors cite a range of approaches to ensure banks remain focused on identifying new emerging risks, including stress testing and scenario analysis to improve the dialogue on risks, improving institutional agility, and spending more time on industry risk blind spots.
- **Risk committees have proved a success, but are challenged to define their role, ensure the CRO is effective, and get the right information.** While everyone agrees risk committees have an important role in bank control systems, differences of opinion exist as to what risks they should oversee and how much input they should have on risk decisions. Regardless, regulatory and supervisory pressures are making it hard for risk committees to avoid being drawn into approving too many decisions. The committee also has to assiduously ensure the CRO has standing in the boardroom and management suite and the right overall skill set so that the CRO can be deeply engaged in key risk decisions. Even after several years of progress, banks are still challenged to get the right amount of information to directors.
- **Conclusion: the journey continues.** While there has been progress, improvement opportunities exist for all banks. There is no achievable final destination, only an ongoing risk management journey.

We hope this summary of candid discussions among some of the banking industry's leading directors, CROs and supervisors helps you as you continue along your own journey to improved risk governance within your institution.

Lawrence "Hank" Prybylski
Global Practice Leader, Financial Services Risk Management
Ernst & Young

Mark Watson
Partner
Tapestry Networks

January 2012

Risk appetite frameworks remain hard to implement, and the industry and supervisors debate the degree of progress made

A significant agenda item for risk committees and CROs over the last few years has been the definition and implementation of a firm-wide risk appetite. In 2008, many bank executives and boards questioned the role of the board in defining or setting risk appetite. They asked what risk appetite statements should look like, the appropriate metrics to include, and whether the focus on risk appetite would yield practical benefits. Most practitioners now agree that establishing a firm-wide risk appetite has enabled more robust discussions of risk tolerance and strategy. A debate emerged in the boardroom about which should come first: risk appetite or strategy. That is, should risk appetite be set first and used to guide strategy, or should strategy be determined first and risk appetite defined in relation to it?

While bank strategies have always been rooted in risk management, formalized risk appetite statements have now become the primary driver of strategy discussions. One director stated, *"We see risk appetite as driving strategy – a constraint. It is not that you can develop a strategy and then risk appetite falls out of that."* Whether strategy drives risk appetite or risk appetite drives strategy, the two have become intertwined in boardroom discussions. BGLN members credited discussions of risk appetite with helping the board decide *"what type of bank we want to be,"* while also and with encouraging a focus on core rather than peripheral activities or geographies.

A director observed, *"[Risk appetite] has become pervasive in the board dialogue,"* and a CRO said, *"[Risk appetite] is the right way to start a discussion between the board and management."* Engaging in this dialogue, rather than perfecting risk appetite models, is what provides real value, directors say. Risk appetite statements have provided a framework for strategic decisions that have led some banks to make dispositions or exit businesses as a result, but this is *"an iterative process; it is never perfect."* BGLN members stated that risk appetite is discussed at virtually every risk committee meeting and regularly with the full board.

For the past 12 to 18 months, however, BGLN members have increasingly focused on properly embedding risk appetite statements throughout the organization. Several difficulties arise:

- Finding appropriate operational and reputational risk metrics
- Overcoming the practical challenges to implementation in large, complex banks
- Debating with supervisors whether progress has been made or not

Finding appropriate operational and reputational risk metrics

Most banks are now working through the inevitable implementation challenges associated with large-scale process and system changes within complex institutions. In a 2011 Ernst & Young survey on risk management in financial services organizations, 91% of respondents found determining the right metrics for risk appetite to be particularly challenging.[4] One director said, *"There are some risks that do not map well to the traditional measures of risk, especially operational risk. There isn't a neat distribution."*

[4] Ernst & Young, *Making Strides in Financial Services Risk Management* (Ernst & Young Global Limited, 2011), 25.

Regulators are looking for progress in this area. In June 2011, the Basel Committee released *Principles for the Sound Management of Operational Risk*, which stated, "Sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems."[5] In a statement to the press, the Basel Committee noted, "Supervisors expect banks to continuously improve their approaches to operational risk management."[6] BGLN research in 2010 highlighted that firms are struggling with incorporating operational and reputational issues into their risk appetite frameworks.[7] One CRO admitted they continue to struggle with this: *"We have not gotten that far because we don't know how to do it well."* BGLN research participants echoed Ernst & Young's survey respondents in identifying the development of credible metrics that can be appropriately monitored as a primary challenge.

BGLN discussion participants more recently highlighted a more fundamental challenge: the complexity of developing preventive measures to address operational risks. One risk chair asked, *"How do you mitigate these risks in a reasonably practical way?"* He went on to say that, in practice, banks can only really focus on *"recognizing there will be issues. How good is your response plan? How do you react?"* One CRO shared a similar perspective, using corruption to make his point: *"Our tolerance for [Foreign Corrupt Practices Act] compliance [failures] is 0.0. Even that is more of a statement of values, rather than an objective, hard tolerance. It shows where we need good limits, checks and balances, and a means to escalate issues quickly."*

Reputational matters are even more complicated. Numerous times in recent years, the industry has suffered reputational damage and litigation costs when products, services, or fees have been reclassified, in hindsight, as onerous to the customer. Recent examples include credit card and overdraft fees and payment protection insurance. Directors are increasingly concerned about similar potential risks in their firms' product and service offerings, and some mentioned that new reputational factors that are being incorporated into product approval processes and audit committee oversight thereof. However, directors do not wish to hamper innovation or become uncompetitive. Moreover, few have mastered the art of using early-warning metrics that relate to the firm's reputation.

Overcoming the practical challenges to implementation in large, complex banks

CROs and directors acknowledge that additional risk appetite implementation challenges remain:

- **Communicating risk appetite across the businesses.** The largest banks are actively converting risk statements into measurable actions that can be more easily communicated to the front line. Even in those instances where risk-appetite statements are relatively comprehensive, communicating them across very diverse workforces is a major obstacle to progress. As such, these statements are increasingly viewed as a *"communication platform"* for broadcasting and reinforcing the bank's strategy throughout the organization. One CRO explained, *"We need our employees to understand*

[5] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk* (Basel: Bank for International Settlements, 2011).

[6] Jim Brunsden, "Basel Seeks to Curb Banks' Risk From Rogue Traders, Fraud," *Bloomberg*, June 30, 2011.

[7] Tapestry Networks and Ernst & Young, "Strengthening the Board-Management Dialogue on Risk and Strategy," *ViewPoints*, November 15, 2010, 7–8.

how the risk issues fit into our ongoing journey as a company." This CRO's initiatives include creating informative booklets and sponsoring events, followed by road shows in support of the message. Directors also want the top-level framework to remain comprehensible. Noted one, *"It has to be such that the non-executive directors could talk confidently about it in front of regulators around the world."*

- **Linking risk appetite and broad limit structures.** One regulator described the problem vividly: *"As banks get bigger and more diverse, to roll up limits becomes challenging … They have it all nailed down at the bottom, calculating limits on the trading business, etc., but they don't know how to roll it up by line of business or at the top of the house into something like a statement of the amount of earnings or capital at risk."* A CRO asked, *"How does risk appetite get reflected in the early-warning system? There should be triggers to action. The limits are important, but as important is what you do about them when triggered. Risk controls are, by nature, backward looking; the risk appetite weaves the limits together."* One CRO pointed out that not only is it difficult to summarize risk, but moving from broad understandings to specific actions is also hard: *"How do you manage the balance sheet and earnings to ensure volatility is not too high? You develop some metrics in … lending, trading, etc. But translating that down into the business is difficult."*

- **Determining what to do about exceptions.** When board members on one director's board were asked what would happen if a risk limit was broken, a variety of answers were offered: it wouldn't happen (because a limit is a limit); it would get escalated to a superior; it would spark a dialogue. This example shows the uncertainty that can exist within the organization (or even in the industry as a whole) regarding how risk limits can or should work. One CRO said, *"We use [exceptions] as a trigger to spark dialogue, but the regulator views them as a sign the process is not working."*

- **Linking risk appetite to dynamic capital allocation.** One way for firms to deal with the current intense downward pressure on returns on equity (ROEs) is to more dynamically reallocate capital, taking into account the firm's changing risk profile and market and client opportunities. However, firms continue to struggle with aligning risk appetite and capital allocation. Indeed, global policymakers have indicated privately that they may examine the industry's approach to this issue in due course to see where practices need improving. A director noted, *"It is linked to risk appetite because if capital is a scarce resource, becoming more so, we need mitigants to reduce risk-weighted assets."*

- **Linking risk and returns.** One executive observed that ultimately risk appetite is about the age-old concept of risk and reward – it's just that today firms must be *"more scientific"* in their approach. Unfortunately, only 37% of Ernst & Young's survey respondents reported a strong ability to track adherence to the risk appetite, making efforts to link risk to reward tremendously challenging.[8] For now, many banks have adopted pragmatic approaches. One CRO said, *"Where we take incremental risk, I try to make people show us the return. What are the parameters, what elements are in our strategy versus those that are not? What pieces are going to cause an offside?"*

[8] Ernst & Young, *Making Strides in Financial Services Risk Management,* 25.

- One director said, *"Risk appetite is about risk-adjusted returns. Where the board plays a role is guiding management, e.g., saying, 'We don't expect you to hit the expected return right now because we need to focus on the risk side and not get hung up on the return side.'"* Within this context, the industry has also been struggling to properly risk-adjust compensation.

Debating with supervisors whether progress has been made or not

Late in 2010, the regulatory community stressed the importance of this risk appetite work. The Senior Supervisors Group (SSG) made the following observation: "Considerably more work is needed to strengthen those practices that were revealed to be especially weak at the height of the crisis. In particular, we have observed that aggregation of risk data remains a challenge for institutions, despite its criticality to strategic planning and decision making."[9]

Around the same time, the Financial Stability Board published a report on intensive and effective supervision, in which it stated that "supervisors … should be asked to consider more stringent SIFI [systemically important financial institution] assessment criteria when it comes to the setting and monitoring of risk appetite, aggregating data to feed the risk control and oversight functions, and in finding ways to make the complex firms more able to be overseen by boards and supervised by authorities."[10] Supervisors also indicated that they were soon going to start evaluating each firm's culture, particularly as it related to risk.

Overall, the industry is relatively comfortable with its progress. Banks have stepped up their efforts in this area: most have completed a lot of the top-of-the-house dialogue on the overall risk appetite. One CRO said working through the process of articulating risk appetite in recent years was his proudest achievement.

Many supervisors, by contrast, remain critical of the industry's progress. One senior regulator said, *"Only one of the top 15 banks has a good handle on their risk appetite. Most want to be shown what success looks like. Many are floundering."* Another noted the industry *"has a ways to go … The areas of remaining challenge [include] operationalizing the statements – or connecting the statements effectively to the risk limit frameworks."* A director observed, *"Regulators are OK with risk appetite as to the risks we want to take. They are not comfortable with risks that get to 'who's watching the store?' e.g., technology risk, reputational risk, etc. There is pressure on the risk committee to focus on these."* In addition, supervisors are seeking greater consistency among firms' risk appetite statements.

Directors and executives acknowledge that there remains room for improvement. Several participants asked, *"Just how far do you go with a risk-appetite statement?"* Few are truly confident that they have achieved a fully operational, fully integrated risk-appetite statement and framework. Some banks have opted for completeness, developing hundreds of risk limits. Others reject a detailed approach, with one CRO suggesting, *"Shouldn't all banks have a single-page overview of their institution's risk appetite?"* And indeed, some banks have focused on developing a brief statement at the top of the organization.

---

[9] Senior Supervisors Group, *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure* (New York: Senior Supervisors Group, 2010), 14.

[10] Financial Stability Board, *Intensity and Effectiveness of SIFI Supervision: Recommendations for Enhanced Supervision* (Basel: Financial Stability Board, 2010), 13.

CROs and directors often express concern that regulators will select the *"gold-plated one and say, 'Everyone should have a gold-plated one like this.'"* Yet as one CRO noted, *"A challenge with pushing risk appetite too far is it moves from a desire to a requirement … [Once written down] it becomes a compliance matter, and we tick the box … It removes the flexibility that's required."*

The divergence in perspectives may arise from differences in the way bankers and regulators describe things: some risk officers claim that regulators conflate the narrow risk appetite approach with the broader and more complex limit structure and framework that each firm has in place. CROs and directors outlined three factors they believe contribute to supervisors' more negative view of the progress that has been made:

- **A focus on technical models.** Part of the challenge, according to one director, is that regulators and institutions may focus on different priorities when it comes to improving risk appetite statements: *"The people within the regulators discussing risk appetite tend to be technicians, not people with expertise about how we think about risks. We end up in a debate about what the model should look like."* One director predicted, *"The test will come in the next crisis: will the guy who got the gold star for having the best risk appetite model perform better? I doubt it."*
- **Zero tolerance for operational risks.** Many directors and CROs believe regulators do not understand the trade-offs involved in mitigating operational risks.
- **Shifting goalposts.** Some say that regulators have been too vague and inconsistent in their expectations and accuse them of moving the goalposts. At one BGLN meeting, a director said, *"Speaking of [going] from 'satisfactory' to 'strong,'*[11] *how do we know when we have gotten there?"* A regulator responded, *"It is incumbent on supervisors to be as clear as possible. But, there were strong institutions before the crisis that all had near-death experiences. The result is a crisis of confidence, so everyone becomes more conservative."* A CRO then asked, *"Are [you] saying that the target is never going to be achievable?"* And indeed, with challenges such as risk, it seems likely that more progress will always be required: there is no finish line to cross, and there are always areas for improvement.

Implementing risk appetite across organizations with thousands, or in many cases hundreds of thousands, of employees will be an ongoing journey as the external environment changes and the board and management adapt their strategies and risk appetite as a result.

Boards, risk officers, and supervisors may wish to consider the following questions:

- ? In what areas have banks been most challenged in implementing risk appetite frameworks? How can banks successfully overcome the common implementation challenges?
- ? How can banks better incorporate operational and reputational risks in their risk appetite statements?

[11] "Satisfactory" and "strong" are ratings used by some regulators to assess risk management and governance in regulated financial institutions.

- How can risk appetite statements be communicated effectively across organizations?
- How should the industry address supervisors' perception that financial institutions have not made sufficient progress on implementing risk appetite?

Instilling and monitoring a risk culture that supports the risk appetite is essential

Despite the countless hours of work invested in defining and implementing risk appetite statements, no statement, limit structure, or risk management system can accommodate every possible situation a bank will face. A bank chairman put it thus:

> *You need to enforce the risk appetite. Through values, training, and compensation – how you incentivize is important. You need strong values and integrity because you cannot set all the necessary limits for all events. Values trump opportunity. They have to ensure individuals feel empowered, they have what they need to make tough decisions, and that they will be rewarded for maintaining our values.*

Many bank chairmen have a passion for this issue. One chairman concluded, *"Culture is key to risk management. It is really about thousands of decisions made every day. You can't rely on people looking at the rules. They are conditioned by culture and how the rules are enforced."* All the chairmen noted that it takes years to do this successfully, which may explain why Ernst & Young found that while 92% of banks have increased their attention to risk culture, only 23% have reported a significant shift.[12]

A CRO observed, *"You know when you have good culture and when you have bad culture. It is somewhere in the middle of the continuum that is difficult. Gradations are tough."* Most agree that developing tangible metrics is more challenging. Furthermore, because large banks have *"very heterogeneous"* workforces, forging a single culture is difficult, if not impossible, and in fact may be counterproductive. Indeed, BGLN participating banks are so large that one has to assume that there will be mistakes in the areas of risk and controls at some point. One CRO noted, *"People will always try to game the system. You need to have multiple mechanisms in place to ensure adherence to policy."* The challenge is that *"every firm's culture is different,"* and it is often difficult to get past platitudes when considering how to adopt and maintain a strong risk culture.

Directors, CROs, and supervisors noted four components that are necessary for a strong risk culture:

- Consistent tone at the top
- Proper metrics that are regularly monitored
- Proper escalation processes and an open culture
- Consistent enforcement

Consistent tone at the top

Participants said the CEO and senior management create the tone at the top through their words and deeds. A supervisor observed, *"Successful organizations drive [culture] through the business."* Another noted, *"The key factor is the CEO's vision and where the board wants to go … That's nine-tenths of what shapes culture*

[12] Ernst & Young, *Making Strides in Financial Services Risk Management*, 9.

… [The rest] is details." A CRO agreed, noting, *"If you don't have the tone at the top set by the CEO with consistency, no matter what risk management says, people will just get around it."*

While no panacea, tone at the top is an important element of culture. Non-executive directors are well placed to monitor and evaluate tone at the top, given their significant exposure to senior management. One director said, *"Risk is not a function, it's an attitude. It must start with the board, the CEO, and then you get down into metrics."* Directors feel *"completely responsible for the culture"* and believe that *"the board should understand the culture and have a view."*

But directors should also spend time in the operations *"to [confirm that] … the words that are spoken are the same as those used at the board level."* They should be sensing if the words and messages are getting through. One director went so far as to say, *"For the robust culture you are looking for, tone at the bottom is more important than tone at the top."* Often, the officially communicated messages and policies can be different from the implicit messages being delivered to revenue producers, so management and the board need mechanisms to understand if employees are receiving the right messages across the organization. One director said his bank had adopted a novel approach: *"We have employed a behavioral psychologist in our internal audit department. Do messages get consistently driven down?"*

Some directors and CROs believe that regulators are in a good position to monitor behaviors deep in the organization now that they *"are putting more people on-site than ever before, having more informal conversations than ever before, to triangulate [a sense of the organization's culture] from the front line, management and the board."* Directors believe the external auditors are also well placed to comment on the firm's culture, particularly in the finance function. As such, directors hope regulators and auditors share their perspectives with them about the *"tone at the bottom."*

A chairman emphasized the importance of setting the right values and ensuring they are adhered to by tying them to performance evaluations and compensation: *"To reinforce it, we put together values and connected them to personal objectives. You don't even get into the balanced scorecard for compensation purposes if you are outside of the values. That concentrates people's minds."*

Proper metrics that are regularly monitored

One risk chair noted, *"An interesting question for us all is, how do we measure our achievements?"* Several CROs agreed with one who said, *"We struggle to quantitatively measure the culture."* Regulators have the same challenge: they want to observe and evaluate culture more, but struggle *"to keep it up on our agenda"* in a way that incorporates cultural insight into the supervisor's overall evaluation of the bank.

Rather than focusing discussions on culture, which, as some directors and CROs observed, can degenerate into little more than an amorphous collection of motherhood-and-apple-pie banalities, CROs recommended focusing on behavior instead. As one CRO noted, *"Culture can be viewed as high-level aggregation, while behavior is individual."* The latter is *"easier to measure."* The challenge is finding ways to evaluate whether actual behaviors on the ground are consistent with a broader set of agreed-upon, high-level values.

For those who are determined to measure culture, directors and executives offered an array of metrics that are *"the way you start:"*

- Employee morale surveys (though these are only directional)
- Number of risk limits that are broken and the cause, especially without prior approval
- Number of problems identified in internal audit reports, the manner in which they are addressed, and preexisting level of awareness of the problems (was management surprised by the findings, or were they already working on corrective action?)
- Percentage of self-reported control or risk problems
- The degree to which information is filtered as it is elevated up through the organization
- Degree to which people focus on information security (at the second BGLN risk meeting in 2011, this was noted as a major and undermanaged threat to the industry)
- Manner in which the company handles employees who have seriously violated company policies; equally important, the manner in which unintentional mistakes are reported and handled
- How risk and control issues – or adherence to ethical standards – are incorporated into the bank's ongoing people performance, evaluation, and compensation systems

One bank chairman mentioned several additional factors that are important for culture, including having strong internal audit, compliance, legal, and risk management teams, along with a core group of senior managers who not only live the culture personally, but instill it across the organization. Stability in the senior management ranks is also important. Working together, bank directors and executives can build a *"mosaic"* that creates a picture of the firm's culture and the direction in which it is moving.

Proper escalation processes and an open culture

Large, complex banks with geographically dispersed operations depend heavily on open communications up and down the organization. As one risk chair observed, *"The problems often come a couple of layers down. We need a system that teases that out for the board."* There are no easy answers. One CRO summed up his bank's approach: *"We have [hundreds of thousands] of employees … How do you expect them all to make the right decisions? We assume people will make mistakes … so we talk about 'raising your hand and asking for help' … It's about creating a culture of risk identification and escalation."* Culture determines *"the manner in which we encourage colleagues to raise and highlight concerns."*

Many directors and executives advocate a no-surprises approach. One CEO said, *"I have a simple philosophy: I don't like surprises. If there is an issue, tell me before it grows into something bigger."* CEOs say they and their management teams have to share their concerns openly, and in a timely fashion, with the board, as only then can directors *"understand the issue and provide input"* or direction. This approach extends well down into the organization. Such an approach requires executives and employees to *"bring bad news forward"* and not hide it, said a chairman. Only if management elevates problems quickly and

early can the board gain confidence in it, and the same goes for others further down the organization. One executive said a good open approach means *"management, the CEO, the chairman, and the board discuss bad news in more detail than good news."*

To engender such an open atmosphere, boards and managers *"need to be tolerant of mistakes and of honest attempts to do the right thing,"* as one chairman put it. Said one CEO, *"When things go wrong, it's not about finding backsides to kick; it's a diagnostic process to identify what went wrong. Do people lack the support they need? Training, knowledge? How do we get it right the first time, and if not, how do we correct for it and identify whether it is something systemic?"* Another CEO said the worst question a director or executive can ask is *"why did we let that happen?"* Rather, the right questions are *"what can we do about it?"* and *"what did we learn from it?"*

Consistent enforcement

Sanctions have to be used and be seen as being used without discouraging openness or the appropriate escalation of errors or issues when they arise. As one executive observed, *"Culture without reinforcement through action is not worth the paper it is written on."* Similarly, it is important that traders who exceed their limits are penalized the same way, whether they make money or lose it: *"There is a perception [in the media] that if someone produces unexpected profit, that is good. That perception needs to be culturally dismissed."*

Boards, risk officers, and supervisors may wish to consider the following questions:

- What steps should banks take to evaluate risk culture?
- What changes can they institute to monitor or change that culture?
- How can the board more effectively monitor the tone at the top and bottom of the organization? Have you sought out the views of external audit and your lead supervisors on tone within the organization?

Boards and supervisors have a central role to play driving necessary upgrades to bank risk IT systems

Inevitably, discussion about risk and other information quickly turns to the IT infrastructure implications. This issue emerged in a BGLN discussion in 2010. Brian Peters, then senior vice president for risk management at the Federal Reserve Bank of New York, remarked, "As boards think about risk appetite, they also need to think about the quality of the infrastructure the firm needs in order to grow – especially IT. In banks, the front office always has the latest and greatest, but the core infrastructure does not get the level of investment that is required."[13] One director asked, *"How do we make our systems better for the business and also respond to regulators?"* Ideally, banks need risk IT systems that can gather risk information quickly and comprehensively, but few are satisfied with their current capabilities.

The SSG highlighted this concern:

> Inadequate IT systems hindered the ability of many firms to manage broad financial risks as market events unfolded rapidly and intensely. The [2009 SSG] report endorsed the need for firms to build "more robust infrastructure systems [that may] require a significant commitment of financial and human resources on the part of firms."[14]

Ernst & Young's research supports the SSG's view: 80% of survey respondents said that inefficient, fragmented systems made it hard to extract and aggregate data across the firm for stress-testing purposes.[15] Similarly, only 37% could aggregate counterparty exposures across business lines within a day, and a significant majority (81%) required manual intervention to do so.[16]

The situation is made more urgent by the number of demands being placed on financial institutions. In some jurisdictions, financial institutions must deal not only with multiple regulators, but also with international organizations, such as the organizations within the Bank for International Settlements and the International Monetary Fund, and new entities, such as the European Banking Authority, the European Systemic Risk Board, and the US Financial Stability Oversight Council, which continue to broaden the nature and frequency of risk information requests. One CRO said, *"It is a huge burden on the risk infrastructure to develop and deliver the materials that the risk committee and regulators now expect."* Data must be pulled from across the organization and often must be pieced together from legacy systems, which greatly increases the potential for errors. One chairman explained the problem facing the industry: *"Over time, [banks] increased IT processes, upgrades, adding parts – both hardware and software. [But] they ended up with thousands of programs, silos, a huge amount of spaghetti. It creates problems, a mess."*

---

[13] Ernst & Young and Tapestry Networks, "Risk Appetite, Strategy, and Regulatory Reform," *Insights from the non-executive director dinners,* June 16, 2010, 8.

[14] Senior Supervisors Group, *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure,* 10.

[15] Ernst & Young, *Making Strides in Financial Services Risk Management,* 30.

[16] Ibid., 33.

Problems associated with inundating banks with regulatory requests for data

- **Distracting firms from managing risks.** Several CROs commented on the potential risk introduced by complying with disjointed regulatory obligations: the risk organization may become absorbed in responding to regulatory requests and may not have the capacity to focus on forward-looking risks. One said, *"We spend more time showing that we are managing risk than actually managing it."* Another said, *"Regulators should care that the [ongoing, ad hoc data request] is distracting people from managing risks."*
- **Misunderstanding existing risks.** Several CROs shared examples of instances where they felt that providing the requested data was not practical or useful. One described the requested data as often *"theoretical and disconnected from the day-to-day."* Another was more specific: *"Supervisors want us to submit the bank's balance sheet on a daily basis … I am not sure it is even possible to close the balance sheet every day."* To some degree this comes from a lack of understanding as to why the information requests are being made. Noted one CRO, *"We should be having a dialogue about whether they are asking the right questions. Instead, it's very dictatorial."* Several CROs provided examples related to requests for information about legal entities.
- **Creating unintended effects on behaviors.** One CRO suggested regulatory scrutiny might change behaviors, but not in the way regulators intended. For example, if the regulator questions the number of exceptions to a risk policy, the bank may simply change the policy. Another said, *"The simple fact that we share information with regulators changes behaviors."*
- **Introducing additional compliance risks.** Several CROs noted that the scale of regulatory requests, especially given their novelty and short deadlines, is necessitating a lot of manual data adjustment. This introduces the potential for inadvertent data errors, which in turn increases the time management spends evaluating the data prior to submitting it.

Addressing this challenge may require front-to-back, multiyear risk and finance data system improvements, which in turn requires two things:

- A step change in the magnitude of investment and oversight of risk IT
- Input from supervisors regarding improvements

A step change in the magnitude of investment and oversight of risk IT

One CRO commented that in light of a surge of inbound requests from various agencies, his resources are simply not available to undertake an IT overhaul right now. He quipped, *"You can't build a fence and paint it at the same time."* Another executive pointed to budget dollars recently allocated: *"We got a significant investment in risk systems, so it would be hard to go back and ask for another $100 million. There is a big trade-off. You have got to survive in the short term even though the long-term investment might have*

been beneficial." Meanwhile, risk systems are part of a broader infrastructure that includes finance systems, customer data, and other systems that all require upgrade investments.

Nevertheless, some CROs said IT investment should experience a step change, with funding spread over time to maximize returns. One predicted, *"The bar will soon be reset."* Another foreshadowed, *"The amount of time and focus that has been spent on risk appetite will transition to IT infrastructure. [Regulators] will benchmark very quickly, so I need to understand where I am relative to this. It will be the top issue this year, and the board is asking."* One CRO admitted what many in the industry say behind the scenes: *"The real question is, [in the end] have we underspent on infrastructure?"*

A director said, *"The IT spend issue has to be thought of differently … There's the ongoing investment in IT infrastructure [that's needed to run our business] – this is a sunk cost, where talk of a [return on investment (ROI)] is meaningless … Then there's the IT investment we should be making to understand our customers and develop products that meet their needs … The problem is, management often tries to have an ROI in all IT."* Another director said, *"We are always behind what we would like to have as a platform. As you face cost problems, how much complexity can you have? Can the systems deal with the complexity? Do we want them as complex as we have been? It becomes a strategic issue."*

With expenditures of such magnitude, governance is even more important than ever. Who at the board level is evaluating management investment in IT? Typically, it would fall to the audit committee. However, a director said, *"We set up a separate board committee to spend enough time to really understand these issues."* Such a committee may improve the focus on IT among the board by taking an aggregate, strategic view of IT investment across risk, finance, customer, and other data needs and ensure an integrated approach to investment is adopted.

Input from supervisors regarding improvements

Directors and CROs recognize the need for communicating more timely, accurate, and fulsome information to regulators, but pointed out that the sheer weight of data requests creates challenges that extend well beyond a heavier cost burden. A chairman acknowledged that regulatory coordination has improved, but commented, *"We send 2,800 reports to regulators worldwide. Perhaps it is good for those who have to say, 'We asked for it,' but what they do with it, I have questions about … Naturally, [the lack of coordination] bothers us. If you have different structures to the same reports, etc., it is inefficient. The major regulators should come together and say, 'These are the kinds of things we should demand of banks.'"*

Many participants in the BGLN's meetings suggested a constructive dialogue with regulators and supervisors on improving coordination, in which all the parties could discuss *"how [to] do this in a sensible way, recognizing that banks have more to do than respond to regulators."* While there is broad recognition that the supervisors are often responding to political pressures and requests from above, participants said they still see clear opportunities to improve the process for managing and sharing information, including the following:

- **Coordination on timing.** At present, information requests come from multiple sources, in different forms and often with strict deadlines. This creates real pressures within banks.

One CRO observed, *"The ad hoc requests … just chew up a lot of time … I spend close to 30% of my time on reporting on ad hoc requests. We were doing six quantitative studies at one point for Basel."* Another noted, *"Many regulators [who make information requests] have no concept of time period or priorities … We get shopping lists as long as your arm."* Another said, *"The lack of coordination is at the micro level as much as the macro … between the senior executives and those who sit in our offices … between the examiners and the centralized policy and model teams."*

- **A shared taxonomy.** CROs agreed that *"supervisors are using assumptions or definitions that are markedly different."* Likewise, regulators noted that firms use different definitions across the industry. While each firm and regulator may have good reason to adopt specific data items, the lack of a shared taxonomy creates a significant burden on the industry and regulators. Similarly, risk disclosures are not standardized, which limits transparency regarding systemic risk and interconnectedness among banks and non-bank financial firms. One regulator said, *"If we had a common standard for terms, it would save the banks billions."* Another regulator noted, *"It has been difficult to engage the industry in this dialogue – they should benefit."* He went on to say that while a shared taxonomy would be highly beneficial, *"banks have a tendency to want to rush to an answer so they can build their systems; they need to realize sometimes we need more time to figure out if the information meets our needs."* Several participants wondered whether the European Banking Authority and newly formed US Office of Financial Research would be the natural agencies to spearhead a common taxonomy or, alternatively, whether the industry and individual regulators could expedite the process.
- **Standardized reporting.** Risk executives highlighted that regulators frequently ask for information that their peers have previously requested, but in different formats. One observed, *"Every time a regulator asks me for a country exposure in a prerequired format, they are always different."* Another complained, *"We have two different regulators asking for the same information in two different formats, neither of which do we actually use in the business."* Reformatting data creates additional work and a higher likelihood of errors. CROs would prefer standard reporting requests so *"the information can be piped routinely to the supervisors, error free."* That said, one CRO cautioned, *"Generally, there is a benefit to standardization … but we could go too far … If we all have a common view on risks, it will influence behavior."*

Directors agree that both regulators and boards need to press management to embark on sustained investment in IT over the next couple of years. Boards and management will also have to reconsider how they evaluate and oversee such investments, and supervisors will need to find ways to obtain data from the banks in a way that does not require quick fixes that actually stall the necessary long-term investments.

Boards, risk officers, and supervisors may wish to consider the following questions:

- **?** What level of risk IT investments does your bank require? How many years would it take to properly overhaul legacy systems to ensure risk data is as robust as finance data?

- ? How well do boards understand the magnitude of IT infrastructure challenges? Where must critical progress be made?
- ? In what ways have the information requests from regulators had a deleterious effect on firms' ability to manage risks, or on supervisors' ability to understand risks? How can the industry and regulators make progress on issues such as standardized reporting, taxonomies, and coordination on data requests?

Ultimately, banks have to invest more in identifying and reacting to emerging risks

BGLN participants agreed that expectations on directors, CROs, and regulators converge in one key area: the ability to spot emerging risks: *"This is an area where we all still have work to do – we don't do enough to focus on emerging macroeconomic risks,"* noted one participant. Participants also worried that bankers may already be forgetting the lessons of the recent past: *"With the last crisis behind us, we are beginning to see the emergence of the same old behavior."*

Directors are not entirely convinced that banks are better positioned to spot emerging risks now than they were prior to the financial crisis. One said he had seen some improvement, but was guarded in his assessment: *"I do think we see aggregate risks to the enterprise better, but I am not sure we will see them sooner."* Another concluded, *"The jury is still out."* One director offered this assessment: *"I think there are emerging risks that we are aware of, but we can't quite size them yet. For example, cyber crime and IT security, dark pools. Undoubtedly, there are unexpected things, and I am not sure we would know where the weakest player would be."*

And many market participants are more pessimistic about banks' ability to foresee future risks. At one of the BGLN risk meetings, industry participants rated their firms only 5–8 out of 10 for ability to identify emerging risks. One suspects candid regulators would rate themselves similarly.

Directors, executives, and supervisors cite several ways banks can hone their ability to identify new emerging risks and enable their organizations to react better to risks when they emerge:

- Using stress testing and scenario analysis to improve the dialogue on risks
- Focusing on agility: reactions to scenarios and events
- Spending more time on industry risk blind spots

Using stress testing and scenario analysis to improve the dialogue on risks

At its core, *"the question is, do you even see the first warning signals? Then, crucially, do you have the ability to interpret those warning signals? You need a good set of aggregated risk information. Then, can you take decisions and get the institution to act?"*

Many advocate greater use of stress and scenario testing, which provide regulators with results that have horizontal equity and which are a form of testing that can be applied to all banks under regulators' supervision. Said one director, *"Regulators are heavily focused on stress testing … It helps better understanding … and makes us think about what areas we should look at."* A chairman said robust, firm-wide stress tests have enabled a real dialogue about meaningful economic scenarios, *"with a major focus on what happens if we do nothing – what's the cushion? What contingent capital do we have, and how quickly and at what price could it be sold? How quickly can we generate cash flows to get out of the trough?"* Others recommend more use of reverse stress testing, which tests the combination of factors that could cause the failure of the firm. Ernst & Young found that nearly half (48%) of banks do not utilize this approach. (One chairman suggested reverse stress testing was of limited value because *"you can stress any bank to*

death. I could give you assumptions very quickly to show you how to get [a major bank] to death. But that's not useful.")

A director described how stress testing has changed the nature of board discussions: *"We spend much more time on liquidity management: when something goes wrong, will we have the cash to withstand it?"* Others have focused on adjusting their approach to stress tests, avoiding static scenarios to *"try to make the stress tests dynamic, looking at the primary, secondary, and tertiary effects."* One participant suggested, *"One approach is to ask management to respond [to the question], 'What would you do to react if a variety of events happened?' This can spur more of an open dialogue with management about exposures versus just the risk group doing stress testing."*

Despite the benefits of discussion around stress tests, this approach has its critics. Some executives and directors suggest regulators focus a lot of attention on the detail of the scenarios, which may miss the point. One regulator said his supervisors are focused on pushing banks to ask, *"How realistic are the scenarios? How would such a stress affect the business strategy?"* But one director said, *"Stress testing is just an indicator … We could all think of a thousand stress tests. Which will be helpful?"* Others say the reliance on assumptions built into stress tests limits their value: *"How do I know whether the stress is sufficiently acute?"*

Focusing on agility: reactions to scenarios and events

A supervisor described the challenge banks and regulators face: *"There is a broad recognition that whatever will cause the next crisis will not be something we will be able to identify."* As such, several executives and directors have suggested that at some point it makes more sense to focus energy on what one CRO called *"resiliency"* – that is, focus on the bank's agility in the face of crises and exogenous shocks. A bank chairman emphasized the need to get beyond hypotheticals:

> *Stress tests, by definition, are incomplete. The last five years have been real-time stress tests, and you can observe what happened. So [knowing] how quickly the organization can react is more useful than modeling a static scenario. You have to extend beyond that. For example, if you test the cost of oil going up dramatically, you have to consider the impact on other industries, etc., not just the direct exposures, so it would be a huge test to run. So, rather than focus on that, focus on the agility to respond.*

Several BGLN participants shared similar views. One said, *"Supervisors should ask us about actual events and see how we respond – like the Middle East, Japan, Egypt. These show how we act."* Reactions demonstrate a firm's resiliency and management's aptitude in crisis.

Directors should also be sure to monitor those areas where *"things are quiet."* If necessary, they should *"create a virtual crisis to see how [management] reacts … to keep them on their toes."* A chairman said, *"If things are too quiet, you are probably on the brink of another crisis … It is the duty of the CEO to check for shortfalls in the business. Those instincts were muted in the period before the crisis. Don't get into a comfort zone when things are going well. That is not what you are paid for."*

Others noted that after the heat of the moment has passed, banks must assess how they dealt with a problem and make necessary course corrections for the future. A bank chairman said, *"Back-testing one's risk profile and risk appetite is very important. Did you stay in your chosen parameters? If yes, [was it] by chance? If you went outside, were you out of control? Or was it bad luck?"*

Spending more time on industry risk blind spots

When pressed for reasons why banks are not fully on top of emerging risks, directors, executives, and supervisors identified a list of blind spots that many feel industry participants have yet to understand fully:

- **Macroeconomic risk.** The ongoing market volatility, with daily shifts in market sentiment and consumption, makes predicting macroeconomic patterns harder than ever. One director exclaimed, *"We lack time to manage risks … How can you determine what the future macro environment will be? We always miss the one which hits us."*
- **Geopolitical risk.** With the tectonic shifts occurring in global politics, understanding political shifts has become increasingly important – and difficult. One CRO said, *"We didn't have Egypt [on our list]. We had Israel, Pakistan, Iran, etc. Absolutely did not predict Egypt. I do wonder, when Tunisia blew up, why didn't we make the connection?"*
- **Unknown potentially lethal risks.** Few directors believe their banks have a firm handle on the "lethal risks" that can bring down their firm. One lead director said, *"Good governance monitors those things that are vital to your survival to ensure they keep working … I think we should not expose ourselves to risks that could kill us. Once you have identified that which is vital, it's not that difficult to get the information. It's identifying what is vital that is challenging."*
- **Strategic creep.** Several directors and regulators noted that sometimes it is the slow changes that create problems, not the fast-paced shifts. One chairman pointed out that the risk profile of an organization often changes slowly, at the edges, and that over time, the aggregate change can be significant: *"Business models change by degree, slowly."* A new business entity might be set up for one purpose and then get used for other reasons, for example. One leading international regulator concurred wholeheartedly and recommended directors ask questions about complex organizational structures – why they exist, what the operations do, what risks they present – and consider simplification. The same could be said for complex businesses and products.
- **Outperformance.** Both directors and supervisors should be asking, *"What is creating superior returns in the businesses that are doing well? What does that tell us about concentration risk, asset quality?"* Several directors said financial institutions often miss the forest for the trees when seeking out risks. One director advocated having boards *"look at a business and ask, why are we making so much money?"* A CEO agreed, saying, *"Management and boards get excited by successes and outperformance, but outperformance should be pursued as quizzically as underperformance."* One director said that ultimately, *"if we see something increasing too much, we have to intervene as directors. But if the profitability of the bank is not competitive, what does that say about the safety of the system?"*

- **Control silos and a lack of attention to the control basics.** Across the vast number of professionals focused on control matters – which for large financial institutions can run to tens of thousands of employees – a critical concern is how well the various disciplines work together. The worst case is a set of siloed groups working independently, not sharing insight, unnecessarily duplicating efforts, and missing key risks or problems for lack of coordination. In that situation, *"internal audit, legal, compliance, are [all] asking people the same questions."* It is important that financial institutions think holistically about their control architecture.

  In this context, directors and senior executives need to ensure the basic control protocols that have been adopted are implemented effectively. Too often, when cases of rogue traders come to light, it turns out it is basic control and security protocols that have been avoided and improperly implemented. Reflecting on a control failure in his bank, one chairman said, *"Our problem was not that we didn't have controls or policies in place. It was simply that no one followed them."*

Financial institutions are hoping that their significant investments in risk governance over the past few years will enable boards, management, and supervisors to identify and react to emerging risks – though many fear a number of critical blind spots remain. More work is required. In 2012, BGLN discussions will focus on starting an industry dialogue on emerging and systemic risk issues among non-executive directors, risk officers, and supervisors.

Boards, risk officers, and supervisors may wish to consider the following questions:

- ? How has stress testing evolved and how do such tests enable better dialogue between directors and management, and with supervisors?
- ? How do banks learn from experiences in managing near misses? How can banks better improve their ability to react to risks?
- ? How would you rate your bank's ability to spot emerging risks? How can firms and supervisors improve their ability to identify and react to emerging risks? Which types of risks are hardest to identify?

Risk committees have proved a success, but are challenged to define their role, ensure the CRO is effective, and get the right information

Only a few banks have chosen not to establish a separate risk committee, and many are now required to do so. Most participants agreed that a separate board risk committee has proven to be, as one director put it, a significant part of the firm's control network, because *"it improves the focus and dialogue on risk."* Knowing issues will be reviewed by the committee, sometimes several times, *"makes risk professionals work harder."*

Several years after their establishment, risk committees still grapple with four main challenges:

- Determining the specific role of the committee
- Avoiding being pushed into approving too much
- Ensuring the CRO and risk function are effective
- Getting the level of detail and information right

Determining the specific role of the committee

In establishing their own distinct governance role in the board room, risk committees have had to determine how broad their oversight should be and how to divide responsibilities among the full board and other committees. Many risk committee chairs say they still have questions about the scope of risk committee oversight, especially as they manage packed agendas. One risk chair asked, *"Bottom line: what is the job of the risk committee?"*

Most directors agree that risk committees *"provide advice, oversight, and challenge."* They challenge by delving deeper into issues, where necessary, and by asking tough, informed questions, which in turn helps *"set the [risk] agenda."* The committee helps set the tone for risk, empowering the CRO and the risk team, and reinforcing the importance of risk throughout the organization. Most directors and risk officers agree that the board and risk committee should *"ensure the right culture is in place, that the risk appetite is right and the right stress testing is done … that the caliber of the risk professionals and risk infrastructure is appropriate … and that the non-executive directors provide the right support and investment for risk management."*

Notwithstanding the board agreement on oversight, approaches to the role still differ in two key areas:

- **Oversee all risks or just the risks we want to take?** Most directors agree that the distinction between the audit committee and the risk committee is that the audit committee is more backward looking, while the risk committee is forward looking, but some boards and risk committees have adopted differing answers as to the specifics. One risk committee chair argued for a narrow role for the risk committee: *"We should be focused on the risks we want to take, not on the risks that happen by virtue of being a big organization, like people, technology, operational risk. That is more the audit committee."* By contrast, another director said, *"The risk committee should focus on the*

actual risks, while the audit committee ensures there is a process in place with the right people to stay within the risk parameters we have adopted."

- **Involved in risk decisions or not?** There is some divergence of view within financial institutions on the risk committee's role – or the role of the board at large – in risk decision making. Most agree the risk committee, and then the board; have to approve the firm's risk appetite. It's integral to the strategy. Others see the committee as having a role in setting risk policies. One chairman said, *"The committee has to form the risk policy and risk management of the [institution]."* However, another chairman said, *"It is not the board's role to make decisions on risk."* The real differences relate to the role of non-executive directors in lending decisions. In many cases, *"the risk committee takes no decision at all. Responsibility is 100% in the hands of the CEO. The board is not to interfere, not to change the decisions of the CEO."* By contrast, several other major financial institutions explicitly involve their risk committees in lending decisions, some on a weekly basis. Where all directors and executives agree is that, overall, supervisors should not push the board or risk committee to be deeply involved in detailed risk or lending decisions.

Avoiding being pushed into approving too much

There is ever-increasing pressure for the risk committees to approve risk limits and decisions, oftentimes on matters that directors and executives view as management's role. This conflates the role of directors and management and draws the risk committee into an unhelpful level of detail and an array of compliance-related matters.

The net effect is that *"regulators are demanding that the board be much more hands-on … There can be a tension between the role of the board and executives."* One director warned, *"By forcing all decisions to the board, [regulators] will actually create a dysfunctional or ineffective board, which leads to a whole new risk."* Non-executive directors noted that when the risk committee does approve something (e.g., a stress test or a model validation), the understanding is that it is mainly approving the quality of the associated governance processes. Supervisors generally agree, but state that the committee should also *"sanity check"* the output, for example, the magnitude of any capital needs arising from stress tests.

One supervisor suggested that perhaps banks are overly anxious about supervisory requirements: *"There is a misunderstanding [on the part of risk committee members] of what … we expect."* One senior supervisor asserted that the role of the risk committee is *"more limited than we as regulators have come to expect."* The supervisor continued, *"Are the limits consistent with the strategy and the risk appetite? That is all the board can really do. They need to rely on the control functions, on risk management and internal audit. So, how do I monitor the control functions? The risk committee should be doing some benchmarking."*

Risk committee chairs and CROs cite three ways to reduce the pressure on risk committees to approve matters that are more properly management's domain:

- **Regulators can clarify guidance that conflates the responsibilities of management and the board.** Sometimes, regulators fail to clarify which responsibilities belong to management and which belong to the board. One director stated, *"Regulators overuse the word 'approve.'"*

Another said, *"Regulators really believe it's meaningful that we [the non-executive directors] approve the stress-test submission … We don't validate the math … We assure ourselves there is good governance around the process."*

- **Supervisors can refrain from requiring more caution than is called for to apply regulatory guidance.** Day-to-day interactions with supervisory staff may aggravate this issue. A CRO observed that while the supervisory leadership can be empathetic, *"people down in the organization don't speak that language. They want everything to go to the board."*
- **Management – particularly the CRO – can stem the flow of minutiae to the board.** Some CROs acknowledge that in some cases it is within their power to cut down on what goes to the board. Said one, *"Nothing goes to the board without my saying so. A first step [would be] to push back on things that do not absolutely have to go to the board."*

Ensuring the CRO and risk function are effective

In the years since the financial crisis, many organizations have replaced their CROs, in some cases multiple times as they move increasingly senior businesspeople into the role (or in some cases back out of the role: a number of the CROs that moved into the role since the crisis have moved on to other senior executive positions). A major focus initially was on ensuring that the CRO and risk function were sufficiently independent from the businesses. This meant new reporting lines and additional resources to support the enhanced independent role. However, in October 2011, the Financial Stability Board issued a report stating, "While progress is being made at both the supervisory and firm levels toward strengthening the CRO's organization, it was noted that most are not yet considered strong."[17]

Directors, executives, and regulators point to three questions relating to ensuring the CRO and risk function have the appropriate influence over firm risk taking:

- **Does the CRO have strong standing in the executive suite and boardroom?** Everyone agreed with one CEO's view that the CRO has to have *"the right stature in the organization,"* which means the CRO should be *"on the [top management] operating committee."* Some BGLN participants emphasized the visibility of the CRO in the board setting. One executive said, *"The CRO should be in all board meetings."* A chairman agreed, saying, *"That way there's no interpretation."* The CRO should have unfettered access to the risk committee and board chairman. Said one risk chair, *"I would also expect the CRO to come to the risk committee chair to tell me if they were not getting the right response."* Both the CEO and risk committee must support the CRO. Said one CRO, *"The CEO is my partner in all of this. What is different now [from before the financial crisis] is there is clear empowerment of the CRO. The risk committee gives the CRO this validity."*
- **Does the CRO have a good mix of skills?** Many directors have said the CRO must have business acumen: *"[The CRO needs to be] someone who has been in charge of a business. They have to have a feeling for the business and a feeling for risk. You need to have been in a line of business to have*

[17] Financial Stability Board, *Intensity and Effectiveness of SIFI Supervision: Progress report on implementing the recommendations on enhanced supervision,* (Basel: Financial Stability Board, 2011).

credibility and be able to justify answers and make informed decisions." Other directors have emphasized courage and note that too many CROs failed to speak up in the run-up to the financial crisis. Said one CRO, *"It is about courage and conviction. You should never put anyone in [the CRO role] who is not prepared to walk away from their job."* More broadly, CROs need a mix of skills that enable them to properly manage the risks facing the firm in a way that enables gainful risk taking. One supervisor said that the CRO has to be *"a scientist and a poet: you need to be quite nerdy to understand this stuff, but you need to be able to tell a compelling narrative to people who are less qualified in that narrow focus."* CROs also need the power to ensure that the risk and control functions have sufficient resources and do not become the victims of pressure to reduce costs.

- **Does the CRO function have management depth?** The need for increasing seniority and a mix of skills and experience in successful CROs, combined with the high turnover rate among CROs, emphasizes the need for boards and senior management to focus on CRO succession by considering bench strength within the risk organization, but also potential successors from among business line and other executives. The Financial Stability Board emphasized this in a report in 2011.[18]

Notwithstanding the importance of a strong CRO and risk function, many directors believe that, ultimately, *"the CEO is the CRO."* Risk decisions cannot be divorced from the critical strategic and business decisions, so the CEO has to engage actively in risk matters. One chairman observed, *"The CEO needs to say what is acceptable risk and understand the risks."* Some believe that the financial crisis showed that in some institutions, even top-tier management misunderstood their firm's risk profile. The CEO needs to *"explain what he is doing, what are the risks, and what are the costs of the risks,"* said another chairman. Another agreed, saying, *"The CEO must report to the board about risk policy, risk controls, and key specific risks. He must explain where these risks are and their level."*

[18] Financial Stability Board, *Intensity and Effectiveness of SIFI Supervision: Progress report on implementing the recommendations on enhanced supervision,* (Basel: Financial Stability Board, 2011).

Should the risk function have veto powers?

- There is diverging opinion in the industry regarding the importance of veto power for CRO or the risk function at large, or whether the risk function *"always has the last word"* on risk. Some institutions view the veto power of the risk function as sacrosanct and believe that *"ultimately, the CEO should always side with [the] risk [function]."* Others take a somewhat more nuanced position. Said one CRO, *"The CEO may side with the business, but what's important is the open dialogue with the business so that it is clear how the decision is being made. Employees need to know that [the CRO] is OK with it if the CEO sometimes sides with the business so [the risk function is] not seen as the police."*
- In most situations, however, the CEO should be aligned with the risk function's perspective, and at the same time, the CRO and the risk professionals at large should have a good working relationship with the business units so they can collaborate.

Getting the level of detail and information right

A CRO said, *"Knowing where to drill down is the trick; knowing when to be a detail person versus a high-level person."* Most directors insist they should not be caught up in the details. One said, *"It is really about what can really cause a problem for us. What is in place to manage it? What are the key processes, and are they effective?"* CROs tend to agree; one noted, *"[The risk committee] should focus on the trends. Management is here to focus on the detail."*

In this context, the risk organization must continue to work with the risk committee to identify the best way to keep the board informed enough to understand key risks and apply judgment to critical decisions without overwhelming the committee with overly complex information. The risk organization often struggles to strike a balance between being thorough and being concise in reporting to the board: *"If you give the board too much information, they say you are overproviding. If you provide too little information, they want more. But it cannot be too process oriented; they want more content."* Different banks have landed on different ends of the spectrum as a result: one CRO provides the risk committee with reports upwards of 100 pages, with over 100 pages of exhibits, while another keeps reports to approximately 30 pages. A chairman noted, *"A good summary is more difficult to produce than a long report."*

Executives acknowledged that they must be more courageous in stopping trivia going to the risk committee, so it has time to discuss key business risks. Said one, *"A first step [would be] to push back on things [that regulators or compliance professionals propose for the agenda] that do not absolutely have to go to the board."* Similarly, directors need to consider the ramifications of their own requests of management: while it is essential that the risk committee have access to any and all information they require, they should be careful not to create unnecessary work assignments out of intellectual curiosity.

As in prior years, banks are still identifying ways to improve reporting to the board and the board risk committee. BGLN participants identified the following ways to improve risk reporting:

- **Trends.** *"[The risk committee] should focus on the trends,"* said a CRO. One former risk executive said *"the board needs numbers, but they also need to understand the story behind the numbers, and the patterns."* Risk information needs to be *"organized according to the way businesses actually operate."*
- **Transparent assumptions.** *"Assumptions about normal distribution, about linkages and correlations between variables, and expectations about behavior should be more transparent."* A CRO said that executives need their reports to show *"what happens if our assumptions are wrong, and how much will it cost us?"*
- **Decision orientation.** A risk chair explained, *"The committee is most interested in what's behind [the data] and what management proposes we do about it. Looking at our positions, what is easy or difficult to get out of? What's the price of taking our risk down in a certain area?"* A chairman put it as follows: *"You need to keep identifying the five things you ought to be worried about. What are the alternatives, and what are the implications of the choices?"* Another said, *"Management needs to tee up the issues in a way that reduces them to the essential choices, making the business accessible to business judgment."*

Several directors also recommended broad dissemination of risk reports to ensure all board members are sufficiently engaged on the detail and many regard having the risk committee receive the same report as management as a good practice as it avoids loss of meaning and detail in translation and ensures directors and executives are discussing issues with the same set of information at hand.

Directors, risk officers, and supervisors may wish to consider the following questions:

- ? What is the core role of the risk committee? In what areas should the risk committee have an approval role?
- ? How can risk committees manage their time effectively to ensure they remain focused on strategic risk discussions?
- ? How does the bank ensure that the CRO has both sufficient independence, yet also sufficient standing with the board and the management team, as well as the right mix of skills to prosecute their role effectively? What actions does the CEO take to actively support the CRO?
- ? How can banks improve their risk reporting to ensure boards understand enough to apply judgment without getting overwhelmed by detail?

Conclusion: the journey continues

BGLN participants agreed that their institutions have made real improvements in risk management and governance and recognized the value they derive from the significant investment involved. Developing more detailed risk appetite statements and improving risk infrastructure were important first steps, supported by enhanced risk leadership in the board and management. The quality of risk dialogue between the board and management, and between banks and supervisors, has improved significantly, as has the depth and quality of risk information shared among these constituents.

Yet, few institutions would be so bold as to state they have completed their risk journey, even those that had adopted good practices and systems prior to the crisis. Notwithstanding the progress that has been made across the industry, some key steps remain ahead for most banks. These include better operationalizing risk appetite frameworks and more effectively instilling and monitoring a supportive risk culture, enhancing risk IT systems, and investing more in identifying and reacting to emerging risks.

Directors, CROs, and supervisors agree that banks are on an ongoing journey to improve their risk governance. They may debate how much progress has been made, but they know the journey continues. As a Japanese proverb says, "When you have completed 95% of your journey, you are only halfway there."

About this document

The Bank Governance Leadership Network (BGLN) provides a unique forum in which key non-executive directors of major global banks can develop and share perspectives on the defining issues of the new banking environment, in conjunction with key internal and external constituencies. The network is convened by Tapestry Networks with the sponsorship and support of Ernst & Young.

ViewPoints aims to capture the essence of the BGLN discussion and associated research; it is produced by Tapestry Networks. Anyone who receives *ViewPoints* is encouraged to share it with those in their own network. The more board members, senior management, advisers, and stakeholders who become engaged in this dialogue, the more value will be created for all.

Appendix: Interviewees

Since early 2009, Tapestry Networks and Ernst & Young have been leading an initiative, the Bank Governance Leadership Network (BGLN), which brings together directors and executives (notably chief risk officers) from leading global banks, and key regulators and supervisors, to discuss the ongoing challenges confronting their institutions. Approximately 200 individuals currently participate in the network, along with over 80 Ernst & Young professionals. This issue of *ViewPoints* draws on dialogues with over 120 BGLN participants and includes discussions from seven BGLN meetings and the third Bank Directors Summit, all of which took place in 2011. A list of individuals who attended BGLN meetings in 2011 and who engaged in one-on-one dialogues on the key issues follows:

Directors and executives

Bank of America

- Susan Bies, Audit Committee Member, Enterprise Risk Committee Member
- Donald Powell, Audit Committee Member, Compensation and Benefits Committee Member, Executive Committee Member

Bank of China

- Jackson Tai, Audit Committee Member, Connected Transaction Control Committee Member, Strategic Development Committee Member

Barclays PLC

- David Booth, Risk Committee Chair, Corporate Governance and Nominations Committee Member
- Sir Richard Broadbent, Former Senior Independent Director, Deputy Chairman, Corporate Governance and Nominations Committee Member, HR and Remuneration Committee Chair
- Alison Carnwath, Audit Committee Member, HR and Remuneration Committee Member
- Lawrence Dickinson, Company Secretary
- Simon Fraser, Audit Committee Member, HR and Remuneration Committee Member
- Dambisa Moyo, Risk Committee Member

BNY Mellon

- Nicholas Donofrio, Risk Committee Chair, Executive Committee Member, Corporate Social Responsibility Committee Member
- Catherine Rein, Audit Committee Chair, Corporate Governance and Nominating Committee Member, Executive Committee Member
- Brian Rogan, Vice Chairman, Chief Risk Officer

CIBC

- Gary Colter, Corporate Governance Committee Chair, Management Resources and Compensation Committee Member
- Nicholas Le Pan, Risk Management Committee Chair, Corporate Governance Committee Member
- Ronald Tysoe, Audit Committee Chair, Corporate Governance Committee Member
- Tom Woods, Senior Executive Vice President, Chief Risk Officer

Citigroup

- Michael O'Neill, Director, Chairman of Citi Holdings Oversight Committee and Member of Risk Management and Finance Committee
- Anthony Santomero, Risk Management and Finance Committee Chair, Audit Committee Member
- Diana Taylor, Nominations, Governance, and Public Affairs Committee Chair, Personnel and Compensation Committee Member

Credit Suisse

- Tobias Guldimann, Chief Risk Officer, Executive Board Member
- Jean Lanier, Audit Committee Member, Compensation Committee Member
- Anton van Rossum, Risk Committee Member
- John Tiner, Audit Committee Chair, Chairman's and Governance Committee Member, Risk Committee Member

Deutsche Bank

- Karl-Gerhard Eick, Audit Committee Chair, Supervisory Board Member

HSBC

- John Coombe, Non-Executive Independent Director, Audit Committee Chair, Risk Committee Member, Remuneration Committee Member
- Douglas Flint, Group Chairman
- Marc Moses, Group Chief Risk Officer

ICBC

- Sir Callum McCarthy, Strategy Committee Member, Risk Committee Member, Nominations Committee Member

ING

- Koos Timmermans, Vice Chairman, Executive Board Member, Former Chief Risk Officer

JPMorgan Chase

- Sally Dewar, Managing Director, International Regulatory Risk
- Jamie Dimon, Chief Executive Officer and Chairman
- Laban Jackson, Jr., Audit Committee Chair
- Barry Zubrow, Chief Risk Officer

Lloyds Banking Group

- Lord Alexander Leitch, Non-Executive Director, Deputy Chairman, Audit Committee Member, HR and Remuneration Committee Member, Nominations and Governance Committee Member
- David Roberts, Risk Committee Chair

Macquarie Group

- Stephen Allen, Head of Risk Management Group
- Michael Hawker, Audit Committee Member, Risk Committee Member
- Peter Warne, Risk Committee Chair, Audit Committee Member, Corporate Governance Committee Member, Remuneration Committee Member

Morgan Stanley

- Roy Bostock, Nominating and Governance Committee Member, Risk Committee Member
- Martin Cohen, Managing Director and Corporate Secretary
- Sir Howard Davies, Risk Committee Chair, Audit Committee Member
- Keishi Hotsuki, Chief Risk Officer
- C. Robert Kidder, Lead Director, Compensation Management Development and Succession Committee Member, Nominating and Governance Committee Member

- Donald Nicolaisen, Audit Committee Chair, Compensation Management Development and Succession Committee Member

Rabobank

- Pieter Emmen, Director, Group Risk Management
- Marinus Minderhoud, Audit, Compliance and Risk Committee Chair, Supervisory Board Member

RBC

- Morten Friis, Chief Risk Officer

RBS

- Nathan Bostock, Head of Restructuring and Risk
- Sir Sandy Crombie, Senior Independent Director, Group Sustainability Committee Chair
- Sir Philip Hampton, Chairman

Société Générale

- Benoît Ottenwaelter, Chief Risk Officer
- Nathalie Rachou, Audit, Internal Control and Risk Committee Member

Société Générale/Unicredit

- Anthony Wyand, Vice President of the Board, Audit, Internal Control, and Risk Committee Chair, Nomination and Corporate Governance Committee Member, Compensation Committee Member, Société Générale; Internal Control and Risks Committee Chair, Permanent Strategic Committee Member, UniCredit

TD Bank

- Mark Chauvin, Chief Risk Officer
- Brian Levitt, Chairman of the Board, Corporate Governance Committee Chair, Human Resources Committee Member
- Harold MacKay, Risk Committee Chair, Audit Committee Member
- Wilbur Prezzano, Human Resources Committee Chair, Risk Committee Member

UBS

- Axel P. Lehmann, Risk Committee Member
- Maureen Miskovic, Former Group Chief Risk Officer, Group Executive Board Member
- David Sidwell, Senior Independent Director, Risk Committee Chair, Strategy Committee Member

UniCredit

- Karl Guha, Chief Risk Officer, Executive Management Committee Member

U.S. Bancorp

- Richard Davis, Chairman, President, Chief Executive Officer
- Richard Hidy, Executive Vice President and Chief Risk Officer
- Olivia Kirtley, Audit Committee Chair, Executive Committee Member, Governance Committee Member

Wells Fargo

- Michael Loughlin, Executive Vice President and Chief Credit and Risk Officer

Westpac

- Greg Targett, Chief Risk Officer

Regulators, supervisors, and policymakers

Australian Prudential Regulation Authority

- Heidi Richards, General Manager, Diversified Institutions Division
- Ian Laughlin, Member

Bank for International Settlements

- Jaime Caruana, General Manager

Basel Committee on Banking Supervision

- William Coen, Deputy Secretary General
- Neil Esho, Senior Member of Secretariat
- Stefan Walter, Secretary General

China Banking Regulatory Commission

- Liu Mingkang, Former Chairman

Federal Financial Supervisory Authority (BaFin)

- Claudia Grund, Senior Adviser, Banking Supervision
- Ludger Hanenberg, Senior Director, Banking Supervision
- Frauke Menke, Executive Director, Banking Supervision

Federal Reserve Bank of New York

- Michael Alix, Senior Vice President, Financial Institutions Supervision Group
- Sarah Dahlgren, Executive Vice President, Financial Institutions Supervision Group, Federal Reserve Bank of New York
- James Hennessy, Senior Vice President, Chief of Staff, Financial Institution Supervision
- Steven Manzari, Senior Vice President, Market and Liquidity Risk Department

Financial Services Agency

- Katsuhiko Komai, Chief, International Affairs Section, Inspection Bureau
- Akiko Nakamura, Inspection Bureau
- Kiyotaka Sasaki, Director, Inspection Coordination Division

Financial Services Authority

- Clive Adamson, Director of Supervision, Business Conduct Unit
- Andrew Bailey, Deputy Head of the Prudential Business Unit, Director of UK Banks and Building Societies
- Thomas Huertas, Former Head of International Division
- Rosalie Langley-Judd, Manager, Governance Policy, Prudential Policy Division
- Lyndon Nelson, Director, Risk Management Division
- Ian Tower, Head of Wholesale Banks & Investment Firms Department

Financial Stability Board

- Eva Hupkes, Adviser, Regulatory Policy and Cooperation
- Costas Stephanou, Member of Secretariat

Office of the Comptroller of the Currency

- Michael Brosnan, Senior Deputy Comptroller, Large Bank Division

Office of the Superintendent of Financial Institutions

- Jacqui Campbell, Manager, Corporate Governance Division
- Barbara Demone, Manager, Financial Conglomerates Group
- Gaetano Geretto, Senior Director
- Maria Moutafis, Director, Corporate Governance
- F. Edward Price, Deputy Superintendent, Office of the Superintendent of Financial Institutions (OSFI)

Swiss Financial Market Supervisory Authority FINMA

- Mark Branson, Head of the Banks Division

UK Independent Commission on Banking

- Bill Winters, Member

Ernst & Young

- Andy Baldwin, Sub-area Managing Partner, EMEIA Financial Services

- Chris Bowles, Partner, UK Financial Services Risk Management Lead
- Tom Campanile, Partner, Enterprise Risk Management, Financial Services
- Stephen Christie, Strategy and Business Incubation Lead
- Carmine DiSibio, Vice Chair and Managing Partner, Financial Services
- Stephen Gregory, Partner, Advisory Services, EMEIA Financial Services
- Stephen Howe, Jr., Americans Managing Partner, Member Global Executive Board
- Patricia Jackson, Head of Prudential Advisory Practice, EMEIA Financial Services
- John Liver, Partner, Financial Services Advisory
- Marcel van Loo, Banking & Capital Markets Leader, EMEIA Financial Services
- Christopher Maher, Principal, Financial Services
- Lawrence Prybylski, Global Practice Leader, Financial Services Risk Management
- Tim Rooke, Partner, Risk Advisory Services, EMEIA Financial Services
- William Schlich, Global Banking & Capital Markets Leader, Financial Services
- Donald Vangel, Adviser, Regulatory Affairs, Office of the Chairman

Tapestry Networks

The team involved in producing this report includes:

- Dennis Andrade, Principal
- Christopher McDonnell, Principal
- Mark Watson, Partner
- Thomas Woodard, Partner