The Tone at the Top

Assessing the Board's Effectiveness

Thought leaders have long recognized that strong leadership and ethical culture are foundational building blocks of enterprises with top-performing risk management programs. However, it is only in the past few years that the striking number of operating-risk-related events, such as data breaches and Bank Secrecy Act/Anti-Money Laundering (BSA/AML) problems in the United States and money laundering issues in the United Kingdom,[1] have made the consequences of a lack of such leadership conspicuously evident. Consensus is quickly growing that a strong risk culture cannot be developed without a top-of-the-house attitude that continuously demonstrates the board and C-suite care about building and maintaining an effective enterprise risk program, inclusive of both cyber security and third-party risk issues.

The right tone at the top and risk culture are important drivers of improved organizational performance: Companies that incorporate risk management into their strategic planning process and operating model gain clear competitive advantage.[2, 3, 4] Boards have a reason to be concerned and, correspondingly, to evaluate their own effectiveness in driving a more effective risk culture. This article lays out an approach that enables boards to assess their own tone at the top in a way that illustrates the difference between current performance and what boards might envision as a target level.

In May 2012, the US Comptroller of the Currency, Thomas Curry, acknowledged the dramatically increasing impact of operational risk[5] in banking at a speech before the Exchequer Club, saying:

Gary Roboff
Is senior advisor to The Santa Fe Group. He has contributed his professional talents to the financial services industry and, in particular, to financial services payments systems for more than four decades. Roboff has focused on issues such as privacy and information management, business frameworks, changes in the payments and settlement systems, and third-party risk management. He has chaired the board of the Electronic Funds Transfer Association (EFTA) and was a founder of the International Security Trust and Privacy Alliance (ISTPA), serving as vice chair of its board.

> *[Operational risk]…is currently at the top of the list of safety and soundness issues for the institutions we supervise. This is an extraordinary thing. Some of our most seasoned supervisors, people with 30 or more years of experience in some cases, tell me that this is the first time they have seen operational risk eclipse credit risk as a safety and soundness challenge. Rising operational risk concerns them, it concerns me, and it should concern you.*[6]

In the more than four years since Curry's remarks, the consortium of regulators that supervises banks has built an increasingly explicit set of expectations around managing various components of operating risk (e.g., information security, third party) that define the roles boards must play in managing their enterprise risk management structures.[7, 8, 9, 10, 11] And, as part of the regular examination process, board risk-related activities are being reviewed with an eye to ensuring that the board is performing essential tasks. At the same time, the annual Shared Assessments Program's *2015 Vendor Risk Management Benchmark Study*, which measures more than 130 detailed indicators of risk mitigation effectiveness, has shown little apparent progress.[12] In fact, even the most mature vertical sector (banking) is exhibiting, on average, incomplete deployment of third-party risk management controls.

The Relationship Between Tone at the Top and Risk Effectiveness

Discussions within Shared Assessments Program working groups have brought to light what many feel are the two greatest stumbling blocks to improved third-party risk management: corporate cultures that are not sufficiently sensitive to the real-world, day-to-day risk environment, and a lack of resources to do the mitigation job that risk management firm professionals know is important. Both of those characteristics are indicative of corporate risk cultures that lack maturity and may be characteristic of firms governed by boards that are not optimally engaged with information security and third-party risk issues.

A 2016 Ponemon Institute/Shared Assessments Program study of tone at the top and third-party risk found that only 17 percent of companies reported that their boards are significantly involved in overseeing risk management activities, and almost half (48 percent) reported limited or no involvement (**figure 1**).[13]

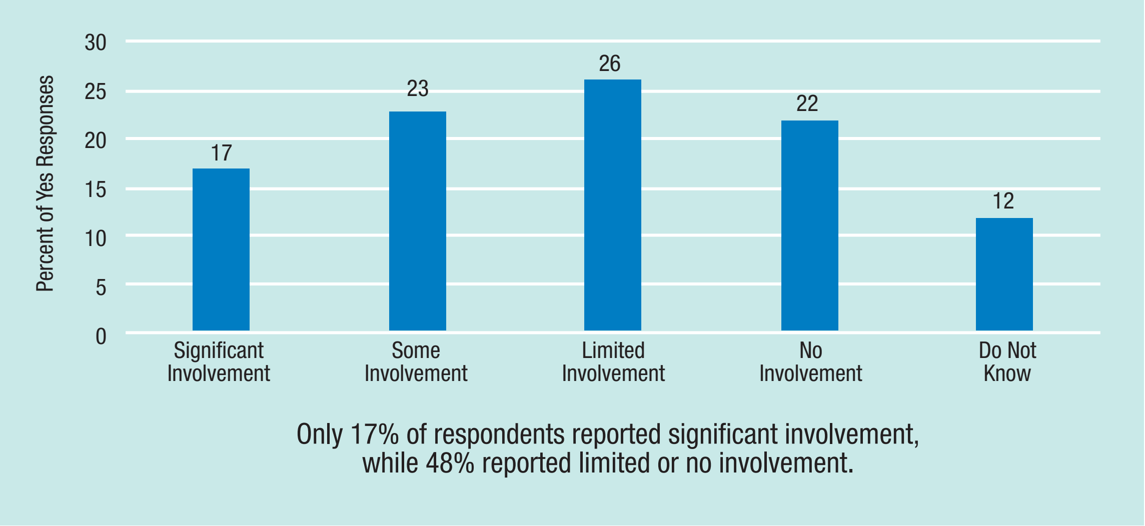
Eleven percent of firms said their organization communicated values throughout the enterprise very effectively, yet 43 percent said communication of values is either not effective or is nonexistent. In that same study, just 33 percent of firms reported that their risk management program and activities are fully determined and established—not a surprising result given the study's reported modest levels of robust board engagement in risk oversight and apparent suboptimal communication of corporate values.

Now, researchers are beginning to study the relationship between board engagement and interaction on risk issues and organizational risk mitigation effectiveness at a greater level of detail. A September 2015 Protiviti study found that companies with a high degree of board engagement are significantly more likely to have other security best practices in place.[14] That relationship was demonstrated in a number of ways including (**figure 2**):

- Having the prerequisites in place to enable the right levels of security
- Demonstrating good risk management processes in the normal course of business
- Demonstrating a higher likelihood of timely recovery after a disruptive event

The *2016 Shared Assessments Program's Vendor Risk Management Benchmark Study*, in the field during July 2016, is attempting to document the relationships, if any, between relative board engagement with internal and vendor-related cyber security risk on the one hand, and the relative maturity of more than 140 detailed third-party risk control areas on the other.[15] Work of this type is essential to illustrating, with more precision, the potential impact of improved board engagement on enterprise risk culture and risk mitigation effectiveness.

Figure 1—How Involved Is the Board of Directors in Risk Management?

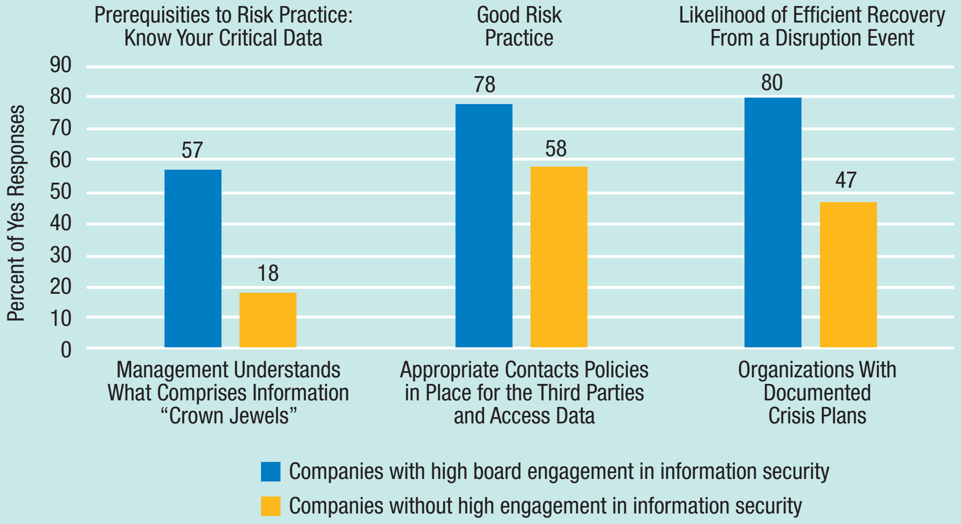


Only 17% of respondents reported significant involvement, while 48% reported limited or no involvement.

Source: Derived from: Ponemon Institute and Shared Assessments, *Tone at the Top and Third Party Risk,* 2016. Reprinted with Permission.

Figure 2—The Impact of Tone on Risk Hygiene and Business Resiliency

The chart demonstrates the relationship between Tone at the Top and the prerequisites of good risk practice, good risk hygiene and the likelihood of efficient recovery from a disrupting event of any origin.



Source: Derived from Protiviti, Inc., *The Battle Continues—Working to Bridge the Data Security Chasm. Protiviti 2015 IT Security and Privacy Study*, September 2015. Reprinted with permission.

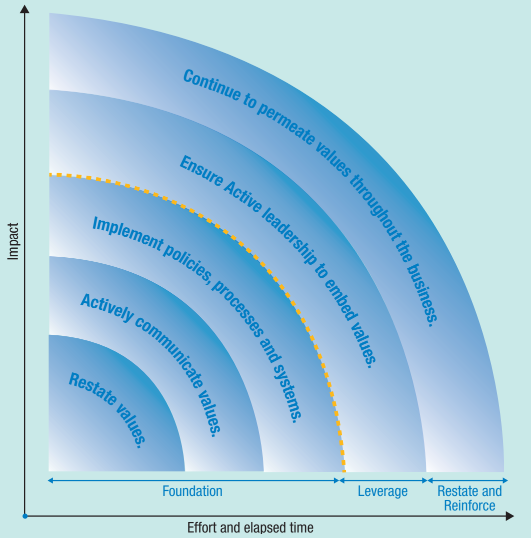
The Human Aspect of Maximizing the Impact of Good Tone at the Top

Corporate risk cultures will not improve if boards of directors simply fulfill the most basic mechanical aspects of their risk responsibilities without effective, ongoing communications that reinforce corporate values and highlight the way in which those values influence risk-related policies, systems and processes.

Building an appropriate risk culture takes time and sustained effort. Boards must engage on risk issues very publicly, both through the chief executive officer (CEO) and directly with key executive risk personnel (e.g., chief risk officers [CROs], chief information security officers [CISOs]). Consistent reinforcement of risk-related values is critical (**figure 3**).

In a July 2016 address to the second annual Culture and Conduct Forum for the Financial Services Industry, the UK Financial Conduct Authority's (FCA) Jonathan Davidson, Director of Supervision—Retail and Authorisations, said he thought there were four

Figure 3— Build Consistently Repeated Leadership Behaviors


Continue to permeate values throughout the business.
Ensure Active leadership to embed values.
Implement policies, processes and systems.
Actively communicate values.
Restate values.
Impact
Foundation
Leverage
Restate and Reinforce
Effort and elapsed time

Source: PWC Co., *Tone from the Top—Transforming Words Into Action*, UK. January 2013, *www.pwc.blogs.com/files/tone-from-the-top.pdf.* Reprinted with permission.

factors influencing risk cultures: "tone from the top,… the formal, tangible practices and cues, which tell people what they need to do to be successful and ensure that the right people are employed and rise to leadership roles,… the narratives that circulate in a firm that explain what the firm is trying to achieve, how it will be achieved and why it is important, … and the capabilities of an organisation."[16] The second and third of those items should be part of an ongoing communications and attribute reinforcement program from the board and executive management.

Effectiveness in Building Organizational Risk Culture

The Shared Assessments Program has been engaged in an effort to develop an approach that enables boards to:

- Take their own tone-at-the-top temperature
- Judge their relative effectiveness in strengthening internal risk cultures
- Identify steps that might be taken to improve board performance

The first step in this process is examination of the types and qualities of evidence that might typically be available on a firm-to-firm basis. This evidence includes items such as board and board committee meeting minutes and notes, in particular, items that can differentiate a level of board discussion from a process that simply rubber stamps a particular risk policy or risk appetite statement developed by staff with little board input or discussion. Stand-alone strategy statements, report documents and, in particular, risk dashboards intended for board consumption can be useful indicators in the context of incident reports, test and vendor due diligence reports, and other event-specific indicators presented to the board. A communications review examines two-way information flow, both to and from the board.

The review process focuses on areas where boards have important risk oversight responsibility and asks:

- Has the board approved and regularly reviewed a risk appetite statement?
- Has the board established risk structures, authorities and responsibilities across the enterprise?
- Has the board demonstrated a commitment to risk mitigation competence?
- Does the board enforce accountability?
- Does the board regularly review and approve the organization's risk assessment objectives?
- Does the board evaluate management's assessments of risk and changes to the risk environment?
- Does the board review, understand and, when necessary, approve technology and other risk controls?
- Does the board communicate and foster risk communications throughout the organization?
- Does the board provide for independent, comprehensive, and effective audit coverage of the IT and third-party risk management programs and communicate deficiencies to management?

> **"A communications review examines two-way information flow, both to and from the board."**

A prototype examination is being developed with a question-specific, five-point rating scale in which four is the highest (best) score and zero is the lowest (starting point) score. In the following examples, the rating tiers consider whether the item exists, whether the board simply approved the item or helped to hone its final form and whether there was consequential organizational communication of the item from the board to the organization (**figures 4, 5, 6** and **7**). In the proposed scale, evidence of significant board engagement in completing a task or engaging in a required activity is valued more highly than evidence of action-specific organizational communication, because fixing a communications issue is far easier

Figure 4—Risk Rating Scale for Risk Appetite Definition and Updating

Score	Determinant
Four (4)	A formalized statement with evidence of board involvement and wide organizational communication
Three (3)	A formalized statement with evidence of board involvement, but little or no organizational communication
Two (2)	A formalized statement without evidence of board involvement, but with evidence of wide organizational communication
One (1)	A formalized statement approved by the board with little or no discussion
Zero (0)	The absence of a board-approved risk appetite statement

Source: The Santa Fe Group, Shared Assessments Program. Reprinted with permission.

Figure 5—Risk Rating Scale for Information Systems Risk Management Effectiveness

Score	Determinant
Four (4)	A board that regularly receives and discusses information about the effectiveness of organizational internal controls and information management and regularly widely communicates its perspective of the organization's controls effectiveness
Three (3)	A board that regularly receives and discusses information about the effectiveness of organizational internal controls and information management, but does not widely and regularly communicate its perspective of the organization's controls effectiveness
Two (2)	A board that irregularly and infrequently receives and discusses information about the effectiveness of organizational internal controls and information management, but does widely communicate its perspective of the organization's controls effectiveness
One (1)	A board that irregularly and infrequently receives and discusses information about the effectiveness of organizational internal controls and information management and does not widely communicate its perspective of the organization's controls effectiveness
Zero (0)	A board that never receives and discusses information about the effectiveness of organizational internal controls and information management

Source: The Santa Fe Group, Shared Assessments Program. Reprinted with permission.

Figure 6—Risk Rating Scale for Arm's-length Assessment

Score	Determinant
Four (4)	A board that shows evidence of regularly conducting, reviewing and communicating the results of arm's-length evaluations of its third-party risk management processes
Three (3)	A board that regularly conducts and reviews the results of arm's-length evaluations of its third-party risk management program, but does not widely communicate the results of those assessments within the organization
Two (2)	A board that irregularly conducts, reviews and communicates the results of arm's-length evaluations of the organization's third-party risk management program
One (1)	A board that irregularly conducts and reviews the results of arm's-length evaluations of the organization's third-party risk management program, but does not widely communicate the results of those assessments within the organization
Zero (0)	A board that has never conducted an arm's-length evaluation of its risk management process

Source: The Santa Fe Group, Shared Assessments Program. Reprinted with permission.

Figure 7—Risk Rating Scale for Board-approved Third-party Evaluation Process

Score	Determinant
Four (4)	A formalized, approved process with evidence of board involvement and wide communication
Three (3)	A formalized, approved process with evidence of board involvement, but little or no organizational communication
Two (2)	A formalized, approved process without evidence of board involvement, but with evidence of wide organizational communication
One (1)	A formalized, approved process by the board with little or no discussion and communication
Zero (0)	The absence of a board-approved third-party evaluation process

Source: The Santa Fe Group, Shared Assessments Program. Reprinted with permission.

than changing basic board behavior issues, which may stem from any number of sources. Examples include:

- **Risk appetite definition and updating**—Has the board formalized, approved and communicated a risk appetite statement, including IT security, third-party security, incident recovery, etc., that is directly linked to strategy?
- **Information systems risk management effectiveness**—Has the board received information from internal auditors or outside parties at previously determined intervals about the effectiveness of the enterprise's internal controls and information systems and communicated deficiencies to management?
- **Third-party risk management program—Arm's-length assessment**—Has the board or an audit committee of the board required a periodic arm's-length assessment of the enterprise's third-party risk management programs (the firm's internal auditors may conduct the assessment, or an outside party may be used) and communicated deficiencies to management and the organization more generally?
- **Third-party evaluation process (including IT security)**—Has the board evaluated, approved and communicated a process for reviewing third parties that incorporates IT security, financial adequacy and resiliency as part of a third-party due diligence process?

What Steps Can Boards Take to Improve Their Risk Tone?

Once a board tone self-assessment has been completed, the C-suite and board should establish where gaps are evident and define program steps to close those gaps.

To enable the organization's long-term well-being, organizational leadership should assume prominent roles, both in resolving open issues and in communicating the fundamental importance of improving risk performance. These C-suite and board roles should be established and maintained even if issues are not identified during initial assessments. Ongoing board oversight of risk management programs in general, as well as C-suite leadership surrounding risk management structure, resource gaps, staff training inadequacies, communications effectiveness or other related areas, are essential to achieving program maturity and continuous quality improvement.

Actions may include those in **figure 8**.

Conclusion

While these are among the actions that will most directly influence organizational culture and risk mitigation effectiveness, additional work in this area of inquiry is essential to improve the board's ability to motivate more mature enterprise risk cultures and risk mitigation effectiveness. Development of a self-examination tool for boards to judge their own tone at the top is part of phase-two work now underway within the Shared Assessments Program's Regulatory Compliance Awareness Group.

Author's Note

Additional background on ongoing Shared Assessments Program's tone at the top work is available at: *http://sharedassessments.org/in-tune-tone-at-the-top-white-paper.*

Endnotes

1 For example, in its 2015-16 Anti Money Laundering Report, the UK's Financial Conduct Authority (FCA) said it had found "serious failings in Barclay's AML due diligence" and levied the largest fine for such activities in the regulator's history, UK £72 million, as a result. It said that actions such as the Barclay's fine and other AML enforcement procedures "have prompted many firms of all sizes to recognise the importance of effective AML systems and controls." Davidson, J.; "Getting Culture and Conduct Right—The Role of the Regulator," FCA, 13 July 2016, *www.fca.org.uk/news/getting-culture-and-conduct-right-the-role-of-the-regulator*

2 Bugalla, J.; K. Narvaez; "How Risk Management Can Spawn Competitive Advantage," *CFO*, 28 July 2014, *ww2.cfo.com/risk-management/2014/07/risk-management-can-spawn-competitive-advantage/*

Figure 8—Board Actions to Improve Risk Tone Performance

Risk Remediation Area	Action(s)
Communications	• Acknowledging suspect culture and leadership issues and identifying specific ways to resolve them • Linking specific risk-related metrics to existing operational and executive reporting and upgrading that reporting where gaps exist • Providing guidance that enables the board to play its proper role in ensuring that established risk appetite levels are not exceeded
Communications and education	• Promoting robust risk-related information sharing within and beyond the organization (for example, by encouraging senior staff to play high-visibility industry roles in key risk organizations) that recognizes the rapidly evolving risk management landscape and its importance to ongoing organizational success[17] • Establishing and maintaining an ongoing dialog with the CISO (or equivalent position) on all aspects of risk management and encouraging continuous risk program updates to the board and audit committees (and/or separate risk committees) on a defined frequency
Education	• Training board members to better understand the importance of good risk hygiene and its relationship to ongoing organizational health, while reinforcing the board's specific risk-related responsibilities • Identifying situations where remedial IT and third-party risk management education is required for individual board members and providing that education
Strategic risk perspectives	• Reinforcing the relationship between risk and business strategy awareness, setting specific expectations for ongoing board engagement with risk mitigation issues that are integrated from a business strategy perspective • Ensuring periodic reviews of the organization's risk appetite statements that encompass the components of IT and third-party risk in the statements

Source: The Santa Fe Group, Shared Assessments Program. Reprinted with permission.

[3] Zolkos, R.; "Strategic Risk Management Provides a Competitive Edge: When Strategy and ERM Meet," *Strategic Finance*, January 2008, *https://erm.ncsu.edu/az/erm/i/chan/m-articles/documents/n StrategyandERMMeetSummary.pdf*

[4] Funston, R.; B. Ruprecht; "Risk in the Strategic Planning Process," *Business Finance*, 1 May 2007, *http://businessfinancemag.com/business-performance-management/risk-strategic-planning-process*

[5] Bank for International Settlements, *The New Basel Capital Accord,* Basel Committee on Banking Supervision Consultative Document, April 2003, p. 120, *bis.org/bcbs/cp3part1.pdf*

[6] Remarks by Thomas J. Curry before the Exchequer Club, 16 May 2012, *www.occ.gov/news-issuances/speeches/2012/pub-speech-2012-77.pdf*

[7] Office of the Comptroller of the Currency, *OCC BULLETIN 2013-29. Subject: Third-Party Relationships*, Department of Treasury, USA, 30 October 2013, *www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*

[8] Office of the Comptroller of the Currency, *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations and Insured Federal Branches; Integration of Regulations*, Department of Treasury, USA, 12 CFR Parts 30 and 170. Docket ID OCC-2014-001: RIN 1557-AD78, 2 September 2014

[9] McNally, J. S.; *The 2013 COSO Framework and SOX Compliance: One Approach to an Effective Transition*, Committee of Sponsoring Organizations of the Treadway Commission (COSO) with the IMA, June 2013

[10] Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook, Appendix J: Strengthening the Resilience of Outsourced Technology Services*, February 2015, *https://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf*

[11] Federal Financial Institutions Examination Council, *"Vendor and Third-party Management,"* FFIEC Information Technology Examination Handbook InfoBase, 2016, *http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/operational-risk/vendor-and-third-party-management.aspx*

[12] Shared Assessments Program and Protiviti, *2015 Vendor Risk Management Benchmark Study: The Shared Assessments Program and Protiviti Examine the Maturity of Vendor Risk Management*, June 2015, *www.protiviti.com/en-US/Documents/Surveys/2015-VendorRiskManagement-Benchmark-Study.pdf*

[13] Shared Assessments Program and The Ponemon Institute, *Tone at the Top and Third Party Risk*, June 2016, *http://sharedassessments.org/ponemon-study/*

[14] Protiviti, *The Battle Continues—Working to Bridge the Data Security Chasm*, 2015, *www.protiviti.com/en-US/Documents/Surveys/2015-IT-Security-Privacy-Survey-Protiviti.pdf*

[15] Additional questions were added to the 2016 survey.

[16] *Op cit,* FCA

[17] Such as industry-specific Information Sharing and Analysis Centers (ISACs)