protiviti®
Face the Future with Confidence

Part Three of a Four-Part Series

The Responsible Technology Firm of the Future: Market Forces

In the first segment of this four-part series, we discussed how the changing landscape of the technology industry requires tech companies to take action to restore and sustain trust in what clearly constitutes a challenging operating environment. In the second segment, we explored some ideas to help pursue this opportunity with a focus on corporate governance and regulatory compliance — a discussion that is especially timely given calls from the chairman of the Federal Communications Commission for greater oversight of major technology companies as executives from two such companies appear before a Senate committee.[1] This third segment continues the discussion with a focus on market forces and an emphasis on three ideas:

- Maximize the company's innovation potential within the confines of social responsibility;
- Pay attention to emerging risks; and
- Better position risk management and compliance within the organization and adopt a compliance framework.

Maximize the Company's Innovation Potential Within the Confines of Social Responsibility

It is inappropriate to discuss the responsible tech company of the future and omit the need for innovation because innovation is at the heart of what stakeholders expect. With the unmistakable mega trends in the business environment, the board of directors has a role in ensuring that the organization it serves is not missing out on opportunities to innovate and, as a result, running the risk of getting swept aside by the forces of disruptive change. In this context, the oft-referenced adage of "disrupt or be disrupted" gives way to the harsher specter of "innovate or die." For innovation to reach its full potential in the digital age, a truly innovative culture must place increased emphasis on diversity, team performance, collaboration, empowerment, continuous learning, ingenuity and change enablement.

[1] "FCC Chair Calls for Greater Oversight of Tech Firms Ahead of Congressional Hearings," Harper Neidig, The Hill, September 4, 2018, available at http://thehill.com/policy/technology/404952-fcc-chair-calls-out-tech-companies-ahead-of-congressional-hearings.

The implication of this point to the concept of the "responsible technology firm of the future" vision is the need for alignment to achieve the balance between the public interest and the responsible tech firm's interest that we refer to in this series. This alignment entails the inherent consideration of the related social impact, stakeholder reaction, brand image and reputational impact in the innovation process. This is how it should work. In this way, companies committed to innovation are more confident in facing the future because they know they are playing the right game, the one that views innovation as a continuous process rather than a dramatic event and as a process that thoughtfully considers the possible unforeseen consequences of the technology offering. With innovation being a strategic imperative, it is an integral part of the confident organization's DNA and is evidenced by setting accountability for results with innovation-related metrics at the organizational, process and individual levels to encourage and reward creativity.

Innovation is almost always thought of as applying to customer-facing processes and a company's product and service offerings. But it should also apply to improving the effectiveness and efficiency of back-office functions, including risk management and compliance. Often, these functions continue even though most companies have not fully leveraged the powerful tools that have emerged in the 21st century — increased computing power, digitization, advanced analytics, mobile and visualization techniques, among others — and the capabilities these tools make possible. Therefore, responsible tech firms should consider the need to innovate and disrupt their risk and compliance functions to keep up with the emerging risk landscape.

With innovation being a strategic imperative, it is an integral part of the confident organization's DNA and is evidenced by setting accountability for results with innovation-related metrics at the organizational, process and individual levels to encourage and reward creativity.

Ask Yourself:

- Do we understand where the organization stands on the digital maturity continuum? Are we a follower? An expert? A leader? And if we're a follower, are we agile enough to keep pace?
- Do we allocate sufficient time to discuss the company's innovation strategy and culture and encourage open discussion on direction and progress? Is this dialogue supported with appropriate innovation-related metrics that tell the full story regarding the results the strategy is delivering, return on investment and the effectiveness of the company's innovation culture and capabilities?
- Do we challenge conventional thinking and disrupt recognized ways of working? Are we agile and adaptive enough to recognize innovation opportunities over time and allocate sufficient resources to pursue them with commitment and purpose? Do we carefully consider the inherent social impact, stakeholder reaction, brand image and reputational impact in the innovation process? Have we considered innovative improvements in our risk and compliance functions to enable our organization to be more adaptive and agile in the face of

an increasingly volatile, complex and uncertain operating environment?

- Are there barriers to innovation and digital transformation that exist within the organization that require attention? For example, do we lack effective processes for (a) identifying and understanding maturing technologies that are expected to have a disruptive impact on the business and (b) capturing external ideas and best practices that can invigorate innovation? Are we unable to apply knowledge of maturing technologies to drive relevant digital innovation initiatives because of inability to reallocate resources or other reasons?

Pay Attention to Emerging Risks

As management focuses on innovation and growth, an eye needs to be kept on newly developing risks that cannot yet be fully assessed but could, in the future, affect the performance or viability of the organization's strategy and business model. For example, take last year's massive, four-hour Amazon S3 service disruption in the Northern Virginia area. Many businesses did not have adequate continuity plans to respond to this type of "tail risk" incident; as a result, they were forced to wait for Amazon to restore service. The good news is that the S3 cloud service has proven reliable over the years and, although the Northern Virginia data center was down, S3 remained functional in the other regions in which it operates. As the largest public cloud offering, many third parties rely on this service; accordingly, any outage is highly impactful across the marketplace. The reality is that system failures do happen from time to time and no system is immune. Therefore, users need to have incident response plans to address the possibility of a failure of this nature.[2]

A risk-savvy tech company recognizes the power of its innovations in triggering transformative forces that can reshape society in fundamental ways, creating new risks and challenging variations of existing risks (cyber risk, for example). Thus, there is the need for balancing focus, as discussed earlier. Just as the hyper-connectivity linking people and things and the digital advances that transform customer experiences create amazing market opportunities, there are important mega trends executives and directors should consider in setting strategy — for example, an aging population, climate change, degradation (quality of air, soil and water), increasing national sentiment, rising geographic mobility, income disparity concerns, and inability of states to cope with these forces. The interconnectivity of these and other trends cannot be ignored such that pursuits of new innovations and growth opportunities are in a vacuum.

Tech executives and their boards should be thinking about the implications to the company's strategy and innovation pursuits of longer-term trends that reach beyond the longest time horizon considered by their strategy-setting and risk assessment processes. For example:

- **Focus on "game-changing" risks –** Risks such as large-scale cyber attacks, constraining regulatory developments, consumer pushback and issues in specific regions where significant investments have been made may be relevant to the company's business model. Consider

[2] "The Day Amazon S3 Storage Stood Still," by Ron Miller, *TechCrunch*, March 1, 2017, available at https://techcrunch.com/2017/03/01/the-day-amazon-s3-storage-stood-still/.

extreme as well as plausible scenarios using these risk considerations.

- **Pay attention to strategic uncertainties –** These uncertainties arise when the critical assumptions underlying the strategy are becoming, or have become, invalid, and management and the board do not know it. Management should consider risks over a sufficiently long-term horizon (say, 10 years) when formulating strategic assumptions for global and regional markets. They should focus broadly on actions competitors may take, how customer preferences could change, the threat of substitute products or the implications of losing a major supplier, channel partner, customer or other vital component of the value chain.
- **Use scenario analysis to evaluate the effect of alternative views of the future –** Use scenario planning and stress-testing routines to challenge assumptions and expectations, address "what if" questions and identify sensitive external environment factors that should be monitored for change over time so management can focus its intelligence-gathering appropriately. By deepening their understanding of the pain of the unexpected, management can identify when contingency plans are required and reinforce the need for flexibility, and even exit plans, in executing the strategy.

The fundamental question is whether the tech company has in place a risk-savvy culture that encourages management to look out far enough, monitor what matters both internally and externally, and devote sufficient time to assess the implications of change on the business. Managers should be encouraged to visualize the big enterprise-wide picture and empowered to take the initiative to collaborate with whoever matters to "connect the dots" when new developments emerge, determine whether the entity's risk profile has been altered in a significant way, and recommend the best approach to address emerging risks.

The fundamental question is whether the tech company has in place a risk-savvy culture that encourages management to look out far enough, monitor what matters both internally and externally, and devote sufficient time to assess the implications of change on the business.

Ask Yourself:

- Are changes in the business environment monitored continuously to identify impacts on the assumptions and risks inherent in the corporate strategy? For example, does the organization monitor key factors that provide insight regarding the continued validity of the key assumptions underlying the business model and the potential for disruptive change? Is management looking out far enough when assessing risk to avoid rooting risk assessments into short-term thinking? Are the board and executive management satisfied that short-termism is not creating unacceptable risks that warrant immediate attention? Are the interrelationships among risks, including compliance and social responsibility issues, and the market actions undertaken by operating units considered?
- Is the board apprised in a timely manner of significant changes in the enterprise's risk profile? Is senior management enabling the collaboration and informal dialogue up, down

and across the enterprise to identify emerging risks on a timely basis? Does the process result in appropriate response plans on a timely basis?

- Do compensation and rewards systems foster a short-termism mentality? Does the board ensure that key executives have "skin in the game" to take risks prudently in the pursuit of value-creating opportunities? Are senior management and the board satisfied that business plans and requests for investment funding are presented with a balanced view of the rewards and risks?
- Are we agile and adaptive enough to recognize innovation opportunities and emerging risks over time and capitalize on, endure or overcome them with timely adjustments to our strategy and infrastructure?
- Is the corporate culture open to risk-oriented, dissenting perspectives or are such perspectives viewed as barriers to the enterprise's core mission? Do senior leaders pay attention to the warning signs posted by risk management and compliance functions, particularly with respect to signs of disruptive change? Are efforts undertaken to minimize groupthink during the risk/reward decision-making process, including ensuring a diversity of viewpoints are engaged in the process?

Better Position Risk Management and Compliance Within the Organization and Adopt a Compliance Framework

Strong internal controls strengthen and increase confidence, thus building trust with customers, investors, governmental agencies and society at large. Trust is the currency of the global economy. That reality suggests that risk management and compliance need to be strengthened in many tech companies. Generally, risk management and compliance functions are responsible for overseeing or coordinating an organization's risk management and compliance efforts. They ensure that the company and its employees understand and are complying with the entity's risk management framework and are aware of and have undertaken steps to implement processes to comply with applicable laws and regulations and internal policies.

In practice, there are at least four basic models[3] to position these functions within the organization:

1. A committee structure approach in which the function lead either chairs or reports to a management risk committee as well as reports to a C-level executive who manages the interactions with the board;
2. Dual reporting to the executive team and the board or a committee of the board;
3. Direct report to the CEO or another senior executive with dual reporting to the board or a committee of the board; and
4. Primary board report, either to the full board or a committee of the board.

[3] Note that the references to the board in the model descriptions can mean the full board or a designated board committee. Most boards choose to designate a separate committee to oversee risk matters. That may mean a separate risk committee of the board or an existing committee that assumes risk oversight responsibility.

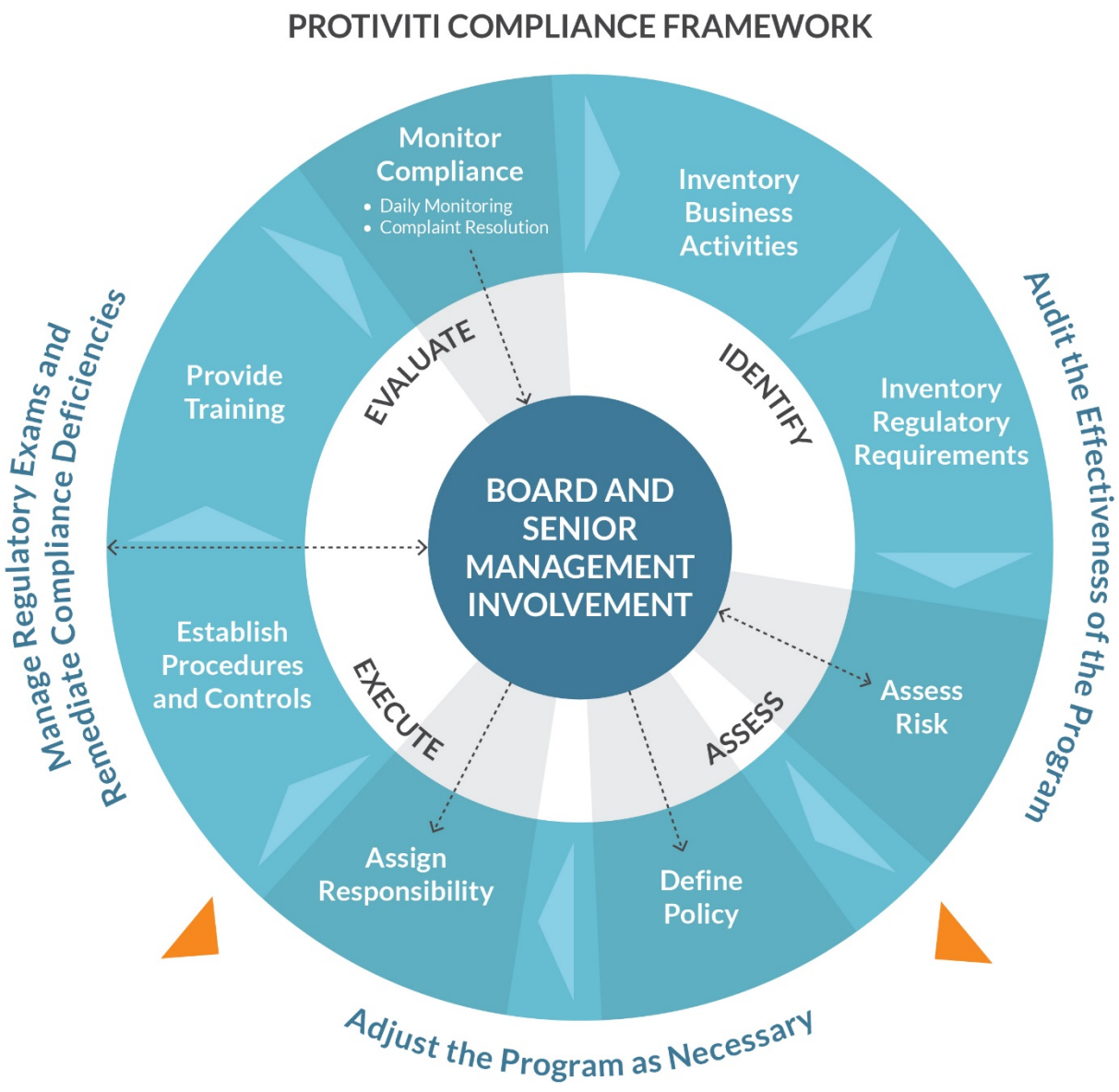
While there are pros and cons with respect to each of these models, it is important to note that the further down the organization these functions are, the greater the risk the unvarnished truth will not be escalated to the CEO and board — particularly when there are serious differences in views regarding the firm's risks and profit generation model. Accordingly, the CEO and board should evaluate the stature and positioning of the functions within the organization and evaluate whether an upgrade is needed. More formalized and direct reporting to the board results in directors having the option of meeting with the function heads in an executive session.

In understanding the scope of each function's activities, it is important to note that other functions within the entity may deal with certain risk and compliance matters. For example, there may be specific risk and compliance domains already in place such as: environment, health and safety; contracting; product quality; employment and labor; security and privacy; financial reporting; Sarbanes-Oxley Section 404; and anti-corruption. These domains need to be identified and the assurance they provide to senior management and the board understood to avoid needless redundancies.

Efficiency and incremental value-add are vital to risk and compliance functions. In the past, as regulatory requirements and oversight expanded, the costs and demand for resources mounted. For example, previously, as industry-relevant certifications and regulatory audits expanded, so did demands on tech companies. These demands present more of a commercial risk than a regulatory risk, particularly for large tech companies (especially cloud companies). These requirements — SOC1 and 2, HIPAA, GDPR, Sarbanes-Oxley, ISO, and other compliance activities faced by end users of technology solutions — have literally "piled up" over the years with the prospects of more of the same looming large on the horizon. Security, privacy, integrity and continuity are all critical areas of concern, especially for cloud companies. Integrating myriad requirements imposed on technology companies — whether from regulations, industry standards, certification requirements or customers — into an overall compliance strategy and resultant program, can both yield efficiencies and increase effectiveness of controls.

Elements of Ineffective Positioning of Risk and Compliance Functions

- Internal controls are often ignored or an afterthought given emphasis on innovation and technical development (not unusual in many early-stage and rapid-growth companies)
- Not viewed as a peer with line-of-business leaders
- No direct reporting line to the board
- Perception that managing risk falls to the function rather than being an organizational imperative
- Activities mired in minutiae
- Constant turf wars within entrenched silos
- Risk not valued as an equal discipline to opportunity pursuit
- Function seen as a blocker to getting things done
- Lack of clarity as to the function's role and how it interfaces with senior line and functional management



A compliance framework, as illustrated above, can be useful in the design, evaluation and ongoing improvement of an integrated compliance program. It provides the structure to capture and consistently manage compliance requirements emanating from multiple sources, the flexibility to apply a risk-based approach to procedures and controls ensuring compliance with requirements, and the clarity regarding roles and responsibilities for compliance across the company, including among senior management and the board. A principles-based compliance framework offers an actionable "road map to success" in that it enables management to evaluate the current-state compliance program in the context of management's risk appetite, identify gaps that must be addressed, and establish a remediation plan that engages relevant stakeholders on a timely basis.

Strong internal controls strengthen and increase confidence, thus building trust with customers, investors, governmental agencies and society at large. Trust is the currency of the global economy. That reality suggests that risk management and compliance need to be strengthened in many tech companies.

Ask Yourself:

- Are the executives responsible for risk management and compliance viewed as peers with line-of-business leaders in terms of experience, authority and CEO access? Are there any elements of ineffective positioning present in the organization?
- Are the right individuals leading risk and compliance? Are the CEO and board satisfied (a) with the scope of their responsibilities and (b) that they can be effective contributors to the C-level and boardroom dialogue?
- Are there multiple teams involved in risk and compliance roles, and are the lines of responsibility between these various roles clearly delineated and understood to ensure the collective efforts are not redundant and that significant risks are addressed?
- Do the board and senior management leverage the risk and compliance functions in obtaining relevant and insightful risk reports? Do the functions have a direct reporting line to the board?
- Does the organization have a compliance strategy and program that focus sufficient attention on the effectiveness and efficiency of compliance policies, processes, organization, reporting and systems in addressing its compliance with applicable laws, regulations, requirements and internal policies?

The final installment of this series will focus on the opportunity to improve the focus on corporate social responsibility.

Contacts

Matthew Moore
Managing Director
Global Leader, Risk & Compliance practice
+1.704.972.9615
matthew.moore@protiviti.com

Gordon Tucker
Managing Director
Global Leader, Technology, Media & Telecommunications practice
+1.415.402.3670
gordon.tucker@protiviti.com

Shelley Metz-Galloway
Managing Director
Risk and Compliance practice
+1.571.382.7279
shelley.metz.galloway@protiviti.com