• • • POINT OF VIEW

protiviti®
Face the Future with Confidence

Part Two of a Four-Part Series

The Responsible Technology Firm of the Future: Corporate Governance and Regulatory Compliance

In the initial 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 this second installment of the series, we begin exploring some ideas to help tech executives and directors pursue this opportunity with a focus on corporate governance and regulatory compliance.

Below we present three suggestions:

- Build and manage a strong corporate governance operation;
- Manage conduct at the top and culture across the organization; and
- Prepare for increased government scrutiny.

Build and Manage a Strong Corporate Governance Operation

In the responsible tech company, governance is all about balancing the focus on innovation and growth with the need to manage risk, compliance and social responsibility issues. Effective governance is about establishing and maintaining a flexible corporate structure that balances the inevitable tension between the entity's value creation objectives and performance goals with the policies, processes and controls it deems appropriate to preserve enterprise value.

Governance best practices focus on achieving this balance in many ways. For example:

- **The board of directors provides the appropriate oversight.** The board needs to take the initiative to ensure that risk and social responsibility are integrated effectively with strategy-setting, performance management and decision-making. The strategy should focus on proactively creating and protecting enterprise value.

- **A formal risk appetite statement is articulated.** This statement outlines senior management's and the board's point of view regarding what they are willing to accept in setting and executing strategy to create enterprise value, the risks they intend to avoid to protect enterprise value, and the strategic financial and operational parameters within which the tech company should operate. Accordingly, risk, compliance and social responsibility issues should be incorporated into the assertions comprising the risk appetite statement.

- **Strong lines of defense are in place and functioning effectively.** Much more than "segregation of incompatible duties" and "checks and balances," the lines-of-defense model emphasizes a fundamental concept of risk management: *from the boardroom to the customer-facing processes, managing risk — including compliance risk and social responsibility — is everyone's responsibility*. There are three lines of defense:

  – Executive management sets the tone with the frontline business unit management and process owners whose activities create risk — they are the first line of defense. As the principal owners of risk, these executives set objectives, establish risk responses, train personnel and reinforce risk response strategies. They implement and maintain effective internal control procedures on a day-to-day basis and are best positioned to integrate risk management capabilities with the activities that create the risks.

  – The second line consists of the independent risk and compliance functions. These functions may include compliance, environmental, financial control, health and safety, inspection, legal approval, quality assurance, risk management, security and privacy, social responsibility, and supply chain. While these functions collaborate with unit managers and process owners to develop and monitor controls and other processes that mitigate identified risks, they also may conduct independent risk evaluations and alert management and the board to emerging risk and compliance issues.

  – The third line is internal audit. It provides assurance that the other lines of defense are functioning effectively.

- **Executive management and the board are the final line of defense.** Amazon founder and CEO Jeff Bezos, in his letter to Amazon shareholders last year, said, "[R]ecognize true misalignment issues early and escalate them immediately."[1] The context of Bezos' statement was on innovation, but it could just as easily apply to risk management, compliance and social responsibility matters that may or may not be related to innovation. The point is that clear reporting lines to executive management and the board are necessary to ensure tech organizations are building cultures that set the standard for corporate responsibility.

[1] "2016 Letter to Shareholders" from Jeff Bezos, The Amazon Blog: Day One, April 17, 2017: https://blog.aboutamazon.com/company-news/2016-letter-to-shareholders.

- **Senior management engages in ongoing dialogue with the board on a timely basis.** The context of discussions regarding critical risk, compliance and social responsibility matters should be the entity's strategic aspirations, differentiating capabilities and the infrastructure necessary to deliver those capabilities, as articulated by the strategy. Discussions of risk, compliance and social responsibility should not be an afterthought to discussions of strategy.

- **Risk, compliance and social responsibility performance is monitored closely.** The old adage of "what gets measured, gets done" applies here. Evaluations of the critical assumptions underlying the strategy as well as the risks inherent in the strategy provide inputs to the determination of key metrics and targets and the need for attention from a risk, compliance and social responsibility standpoint. It is at this point where the management of these issues begins to intersect with performance management.

- **The organization should position itself as an "early mover."** A focus on achieving balance should position the organization to attain "early mover" status whenever it arrives at a crossroads where the company's market position could be harmed significantly if the imminent opportunity or emerging risk is not recognized promptly by the right people and acted upon. Just as the tech company is quick to address innovation and growth opportunities, it should also address risk, compliance and social responsibility issues in a timely manner.

Ultimately, striking the appropriate balance of innovation and growth on the one hand and risk, compliance and social responsibility on the other is realized through an efficient governance structure supported by an effective enterprise management and monitoring capability.

> *Just as the tech company is quick to address innovation and growth opportunities, it should also address risk, compliance and social responsibility issues in a timely manner.*

Ask Yourself:

– Is senior management informed in a timely manner when critical risks emerge? Is the board engaged in a timely manner on such matters? Does management and the board have the time advantage of more decision-making options before market shifts invalidate critical assumptions underlying the strategy?

– Is there sensitivity to risk, compliance and social responsibility matters across the organization? Is there a strong emphasis on the three lines of defense?

– Do we measure what really matters from a risk, compliance and social responsibility standpoint so that risk-informed decisions can be made?

– Do we place a high enough priority on preserving reputation and brand image and establishing the early warning capability that lays the foundation to move as quickly when critical risks emerge as we do when innovation and growth opportunities arise?

Manage Conduct at the Top and Culture Across the Organization

Culture gives the organization its particular character by infusing the shared values and attitudes that frame how an organization thinks and behaves. It is almost always at the root of all reputation and financial performance outcomes, both good and bad, as it is a potent source of strength or weakness for an organization. Essentially, it is the DNA of the organization.

We define corporate culture as:

> The behaviors that people experience when they work for or interact with the enterprise's management team and other representatives, as manifested through their decision-making, attitudes and day-to-day actions.

The focus here is not on what leaders say, but on what they do and how they conduct themselves. Whatever the belief systems are, they are manifested through the enterprise's actions. Conduct speaks volumes in reflecting what is truly valued.

Some of the greatest technology innovations have resulted from extremely strong and intensely focused cultures. However, these intense cultures may have one or more attributes that also create significant risks or organizational "blind spots" that can unintentionally encourage, enable or condone misconduct or irresponsible business behavior. These attributes may include a warrior or cutthroat mentality, dogmatic doctrines, blind convictions, dominant personalities, extreme bias toward a singular view of the future, and other qualities that can lead the organization to uncharted, stormy waters of conflict with social responsibility and the public interest. By contrast, cultures where misconduct is not tolerated and appropriate conduct is not only table stakes, but also promoted, reinforced and recognized, create an environment where the tech company can harness its full capabilities while also ensuring alignment of innovation strategy and responsible corporate conduct.

Corporate culture is complex, as it often consists of myriad subcultures. For example, every tech organization has an innovation culture representing its "secret sauce" in driving innovation to improve market offerings continuously and create new markets. Other examples of subcultures include a quality-committed culture, safety-conscious culture, and a diverse, inclusive culture. Cultures within a tech company may vary across the organization at different locations, in different functions and departments and, of course, in different countries.

The challenge for the responsible tech company of the future is in creating a strong risk culture, which we define as:

> The set of encouraged and acceptable behaviors, discussions, decisions and attitudes toward taking and managing risk within an institution that reflects the shared values, goals, practices and reinforcement mechanisms that embed risk into the institution's decision-making processes and risk management into its day-to-day operations.[2]

An actionable risk culture helps to achieve the balance discussed earlier between creating enterprise value and protecting enterprise value.

[2] This definition was derived from the one adopted by the Risk Management Association and Protiviti in "Risk Culture: From Theory to Evolving Practice," *The RMA Journal*, RMA and Protiviti, 2013, available at https://www.rmahq.org/WorkArea/DownloadAsset.aspx?id=5452.

In linking culture to conduct, it's important to align the tone in the middle with the tone at the top. Too often, the focus of the board and senior management is limited to the tone at the top. It is one thing to understand the tone at the top, but completely another to ensure that tone is translated into an effective tone in the middle.

Often, we refer to the "tone of the organization," a phrase we coined to describe the collective impact of the tone at the top, tone in the middle and tone at the bottom in shaping an entity's culture and conduct. While tone at the top is important and a vital foundation, the real driver of behavior on the front lines is what employees see and hear every day from the managers to whom they report — irrespective of what executive management communicates regarding the organization's vision, mission and core values. If the behavior of unit and middle managers contradicts the messaging and values conveyed from the top, it won't take long for lower-level employees to notice.

Senior management should consider culture-related measures and develop a practical approach to measuring, monitoring and reinforcing that makes sense. The CEO, senior management team, unit leaders, and chief ethics and compliance officers and other second-line functions should regularly communicate and reinforce the essential aspects of the corporate culture in appropriate forums and with consistent messaging. They should consider the cultural implications of significant internal and external events and major adjustments to the strategy, and plan accordingly. Onboarding of new hires should emphasize the importance of the enterprise's culture. Also, the board should be engaged to ensure directors are on the same page with management in understanding, measuring and reinforcing the corporate culture.

With today's optics, the tech organization should have zero or low tolerance for misconduct. Conduct relates to all aspects of how a company operates and interacts with customers, markets, investors and stakeholders. Misconduct through any of these channels can have significant and permanent consequences for the firm (e.g., loss of trust, reputational damage). That is why conduct at the top may be a more important point of focus for a tech organization than tone at the top because it can drive undesirable conduct across the organization.

> *The real driver of behavior on the front lines is what employees see and hear every day from the managers to whom they report — irrespective of what executive management communicates regarding the organization's vision, mission and core values.*

Ask Yourself:

- Can the board and CEO agree on the state of the current culture and whether it is aligned with the enterprise's strategy, mission, vision and core values? Is the mood in the middle aligned with the tone at the top? Are there any gaps between the current and desired culture?

- Does the entity measure its culture and monitor and improve it over time as needed? Does the board have transparency into how well the culture is functioning? For example, how does culture impact employee performance, productivity, recruiting and retention?

- Are there subcultures in conflict with each other? If so, do they present exposure to organizational dysfunction (e.g., excessive risk-taking, off-strategy decisions, or unethical and irresponsible business behavior that is not in either the company's interest or the public interest)?

- Is the culture in the boardroom and C-suite fit for purpose in today's environment? Are diversity and inclusion considered by the nominating committee when evaluating candidates for the board, and when considering executive management candidates?

Prepare for Increased Government Scrutiny

For all of the reasons cited in the opening conversation regarding the changing landscape, it is not an unreasonable scenario to expect the tech industry to encounter increased regulation, challenges from the anti-competitiveness contingent and questions regarding societal benefit. For example, additional regulatory changes and scrutiny could affect how tech products or services are produced or delivered.

To illustrate: Conversations today are taking place among legislators and regulators around combating disinformation, protecting user privacy and promoting competition in the tech space. These conversations are driving policy developments that could introduce new web platform requirements, create fresh legal liability exposures for the tech industry, initiate General Data Protection Regulation (GDPR)-like privacy rules in the United States, affect consumer education, and enhance intelligence-gathering activities, among other things. Whether any of these proposals find their way into enacted law or new regulations is an entirely different discussion. The point is that policymakers are actively engaged.[3]

> *The tech industry's encroachment on other industries, some of which are highly regulated, is blurring the lines in a way that is most certain to drive increased regulation.*

Privacy and identity management and information security risks continue to be a moving target and addressing them may require additional resources as privacy and consumer protection demands increase. The developments on the consumer privacy protection front (e.g., the European Union's GDPR legislation, regulations passed in the United States in California,[4] New York[5] and other states,[6] and other international regulations either in the works or already in place, such as China's Cybersecurity Law) represent the proverbial "elephant in the room" that no one can ignore. The tech industry's encroachment on other industries, some of which are highly regulated, is

[3] "Scoop: 20 ways Democrats could crack down on Big Tech," David McCabe, Axios, July 30, 2018, available at www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html.

[4] "California Enacts Sweeping GDPR-Like Privacy Law," Morgan Lewis, JD Supra, July 10, 2018, available at www.jdsupra.com/legalnews/california-enacts-sweeping-gdpr-like-13533/.

[5] "New York Cybersecurity Regulations: An Important Step, but Still a Long Way From the GDPR," Tony Kontzer, RSA Conference, March 29, 2018, available at www.rsaconference.com/blogs/new-york-cybersecurity-regulations-an-important-step-but-still-a-long-way-from-the-gdpr.

[6] "US States Pass Data Protection Laws on the Heels of the GDPR," Jeewon Kim Serrato, Chris Cwalina, et al., Norton Rose Fulbright Data Protection Report, July 9, 2018, available at www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

blurring the lines in a way that is most certain to drive increased regulation. Financial services (fintech) is one example, but there are surely others (e.g., energy and utilities, healthcare and retail). All of these and other developments on the regulatory front create exposure to increased regulatory oversight, consumer protection-related fines and penalties, and the attendant erosion of brand image and reputation.

Tech companies need to take steps to address this fluid environment. Some suggestions follow:

1. **Get a grip on regulatory developments** — A strong compliance management system (CMS) can add considerable value in identifying, inventorying, and monitoring complex regulatory requirements across regional, country and state jurisdictions, customer bases, and products and services. The compliance function should own the responsibility and ensure that the right people are aware of the requirements affecting the company's operations and market offerings. Addressing multiple control requirements separately each time a new regulation is enacted can be costly and inefficient when there are similar requirements involved.

   To mitigate the duplication of effort caused by these redundancies, the CMS can incorporate a common control framework that can be mapped to the various regulatory requirements and frameworks to which the tech company is subject. This framework combines overlapping control objectives to streamline the compliance process so that management and the compliance function can focus on a smaller set of controls in meeting the requirements of all regulatory frameworks. Heavily regulated companies spend a lot of time designing and implementing new business processes to meet compliance requirements. That can be especially frustrating for businesses that face multiple compliance requirements. That is why a common framework can support efforts to achieve compliance efficiencies. This area is one that may likely require investment due to the considerable subject-matter expertise needed to address the mandates of multiple jurisdictions.

2. **Implement a process to monitor policy shifts on the geopolitical stage and manage their effects** — The process of staying in touch with the sources of power begins with monitoring legislative, regulatory and global market developments through appropriate means (e.g., hiring insiders and consultants, tracking developments through published sources, monitoring geopolitical hotspots, and keeping close tabs on special interest groups). The process also entails engagement of and informing legislators, regulators and policymakers through point-of-view statements, face-to-face meetings, lobbyists, correspondence, social media, advocacy groups, industry associations and other means. It continues with responses to new legislation and regulations through updating policies, modifying existing processes and systems, and implementing new processes and systems. Thus, the process facilitates monitoring, engagement/outreach, and response.

3. **Evaluate strategic assumptions** — Every organization's strategy has underlying assumptions, explicit or implicit, about the future. These assumptions represent management's "white swans" or expectations about the regulatory environment and global markets. In times of uncertainty, it makes sense to assess the underlying strategic

assumptions in light of likely regulatory actions in relevant markets.

4. **Consider the implications of scenarios germane to the markets in which the organization operates and begin preparing for the possible** — Define appropriate plausible and extreme scenarios, taking into account the impact of various policy initiatives on the company's markets, channels, customers, labor pool, supply chains, cost structure, discretionary spend and business model. Use the scenarios to understand the potential impact on the business and formulate strategic alternatives to capitalize on market opportunities and address potentially disruptive change. Update the analysis as the regulatory agenda unfolds and policies are clarified.

5. **Update M&A plans and strategy** — The global mergers and acquisitions (M&A) market remains active as tech companies continue to pursue transactions that complement organic growth and advance their respective strategies. Companies should consider the shifting regulatory dynamics as they develop and reassess their M&A appetite given the overall corporate growth strategy, the economic climate, changing consumer behavior and other market developments.

6. **Pay attention to sovereignty risk** — Geopolitical dynamics can create country risk. The primary objective of managing country risk is to protect company investments from risks of impairment and to sustain return on investment (ROI). Investment impairments may arise from confiscatory actions by a sovereign entity, such as nationalization of the business or expropriation of assets. ROI reductions may arise from discriminatory actions by a sovereign entity directed at the company, a targeted industry, or companies from certain countries; such actions might include additional taxation, price or production controls, and exchange controls, among other things. Both investment impairments and ROI reductions may arise from destructive or disruptive events or circumstances (e.g., violence, terrorism, war or infrastructure deficiencies). Such risks must be addressed by understanding the driving forces of change in countries in which the company does business and taking proactive steps to manage identified exposures.

Ask Yourself:

– Is the board and senior management satisfied the organization is in tune with the business environment and staying relevant in the marketplace? To that point, does management have a process in place to monitor legislative, regulatory and geopolitical developments and keep current with developments germane to the business and industry?

– Is there a process for reaching out to policymakers, legislators and regulators with the objective of informing them of the company's storyline and sharing marketplace realities when circumstances warrant?

– Does management respond in a timely manner to new laws and regulations and geopolitical developments with appropriate revisions to the strategy and its supporting policies, processes and systems? How do the board and senior management know?

The next two installments of the series will emphasize how to improve the focus on market forces and 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

protiviti®