COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2019
Best practices for developing and executing a successful risk assessment

By Stephen Martin, LLM, JD, MBA, and Toby Ralston, CPA, CFF, CFE, MBA

Stephen Martin (smartin@stoneturn.com) is Partner, and **Toby Ralston** (tralston@stoneturn.com) is Managing Director at StoneTurn in Denver, Colorado, USA.

Companies doing business across the globe today are operating in a more stringent regulatory environment. The proliferation of industry, sector, and government agency standards, as well as the increasing use of compliance as a regulatory tool, has put multinational corporations in a position to defend their compliance program and related controls; invest in additional resources meant to prevent and detect misconduct and/or incentivize compliance with laws; sanction inadvertent or deliberate wrongdoing by employees, officers and agents; and ensure effective program oversight by senior management and their boards of directors.

In addition, global organizations face the recently revised Department of Justice (DOJ) guidance[1] on anticorruption and fraud, along with further emphasis on individual prosecutions, liability for third-party relationships, joint ventures, and partnerships, which together send a clear signal to worldwide enterprises that they must carefully review, test, and enhance their compliance programs now or risk harsh legal actions, irreparable damage to their brand, and steep financial penalties for any wrongdoing.

Whether administered internally or with the help of outside experts, conducting an effective risk assessment is an essential step to develop and/or enhance a strong compliance program. An effective risk assessment framework and process helps companies to identify direct and indirect global compliance hot spots that, when used in combination with technology and data analytics, can pinpoint unknown or unwanted trends in order to maintain a world-class compliance program.

When and how to conduct a risk assessment

It's important to understand that risk assessments are a proactive and preventive measure, which should be a regular and systemic part of a company's compliance efforts. In fact, global regulatory and enforcement agencies, including the DOJ, have been very clear that multinational corporations need to be more focused on conducting recurring assessments of risk in order to identify potential vulnerabilities and address any legal or regulatory threats that might crop up on an ongoing basis as an organization grows, adapts, or evolves.

Although there are an innumerable amount of circumstances and unique scenarios within any corporation that could trigger the need for a fresh look at its risk profile, there are certain key catalysts within a multinational organization that should prompt a multidisciplinary evaluation of risk, including:

- **Lack of compliance program:** If the organization does not have a compliance program in place, a thorough, enterprise-wide risk assessment needs to be conducted in order to identify potential areas of weakness and build off of embedded procedures in order to design an effective program from scratch.
- **Evaluate existing compliance program:** Even if a compliance program exists, periodic (e.g., annual, biannual, quarterly) risk assessments need to be orchestrated in order to evolve and enhance the current

program based on new data, management, and regulatory guidance.

- **New strategic initiative:** As multinational organizations grow and expand into new markets, add new services and projects, or enhance strategic initiatives, corporations must assess those associated risks in preparation for the company's expansion to protect against a potential enforcement action or investigation caused by potential regulatory infringements, a lack of proper program oversight, and/or corporate malfeasance.
- **Investigation or enforcement activity:** Once a regulatory or enforcement agency calls for an investigation, it is imperative that a corporation conduct a comprehensive risk assessment to identify known gaps, remediate problems, and prevent future misconduct through enhancement of the compliance program.

As organizations evolve, so too do their risk profiles. Therefore, companies must incorporate, and top management must support, a comprehensive and ongoing risk assessment process—one that is woven into the fabric of the organization to make certain that its strategic, operational, financial, legal, and compliance functions are prepared when a significant challenge arises.

To get started, companies should consider current and potential compliance risks, including systemic, organizational, or industry-specific risks and any other unique risks to their organization. Furthermore, organizations need to take a candid view toward the historical and current adequacy of both existing policies and internal controls meant to mitigate risk. Any proactive risk assessment should include key decision-makers from the corporate level, but it should not be limited to executives. Those employees who are operators of, and responsible for, business operations and mitigating controls should be included in the assessment discussion. Finally, global companies must assess additional and individual regional/country risks, particularly in BRIC countries (Brazil, Russia, India, and China) and other high-risk or emerging markets, to provide a greater corporate line of sight into local management/operations, as well as key compliance risk areas such as corruption, trade compliance, export controls, and antitrust/competition risks. If helpful, organizations can consider risk as organized into the following four main categories.

1. Financial

Compliance regulations in this area are most prolific. As a result, and historically, this risk area has been, and will remain, the most heavily monitored concentration of risk. Finance continues to be a focal point for multinational corporations as they look to assess potential regulatory and legal weaknesses related to financial controls and disclosures. Specifically, this category includes risks associated with markets and credit, capital management, liquidity, treasury, accounting, and financial reporting. Examples of financial red flags that enforcement officials look for include changes in auditors because of accounting or auditing disagreements, geographically scattered business locations with decentralized management and a lack of consistency in defining and applying internal controls, and a failure to enforce a company's code of conduct. In addition to an organization's chief financial officer, chief accounting officer, and head of investor relations/treasury/credit, the organization should consider tapping the expertise of its audit committee in its consideration of financial risk.

2. Legal/Regulatory

As more corporations conduct business globally and across an array of industries, they are more susceptible to potential (and in some cases, unknown) violations associated with changing laws and regulations related to geographic location, sector, and service area. And, like the financial risk category, this area is monitored closely by enforcement agencies and has been something that most global companies watch scrupulously. Therefore, it is important to conduct ongoing assessments of regulatory risks in order to understand how laws and regulations

are changing in all jurisdictions in which a firm operates. Those changes in European law, such as the Markets in Financial Instruments Directive (MIFID II), Senior Managers Regime, and Remote Supervision, need to be identified and fed into a risk taxonomy for those risks to be assessed. Red flags regulators look for in this category include a lack of identifying and planning for future regulatory changes, a lack of identifying and planning for regulatory requirements tied to future product or market expansions or contractions, and a lack of coordination in yearly planning between compliance and IT to build and deploy systems to support a firm's response to regulatory deadlines (e.g., MIFID II). General counsel, a chief legal officer, and external counsel serve to inform and advise organizations in the area of legal/regulatory risk.

3. Operational

Unlike financial and legal/regulatory risk, operational risk has become increasingly more important to companies and their investors, creditors, and regulators alike with the rise of global social and environmental movements. Regulators are looking at the ways in which organizations employ people, third-party relationships, technology, data, business processes, and controls to enhance business performance. Some red flags for regulators include responsiveness to formal complaints, tone-deafness from top management, a lack of streamlining between disparate IT platforms to combine and analyze linked data for client/customer objectives, a lack of tracking and vetting of third-party relationships, and a lack of planning for damage to physical assets due to climate change or geo-political events. Chief executive officers, chief operating officers, and lead sales representatives can and should contribute to an organization's assessment of operational risk.

4. Reputational

Similar to operational risk, a company's actions and overall standing in the marketplace are becoming more highly scrutinized than traditional measures such as size or financial standing. Within this area, regulators will be looking for deficiencies in corporate governance, strategic risk, crisis management, brand, and reputational risk. An organization's standing with respect to diversity, inclusion, and sustainability can be judged instantaneously and, on occasion, without merit. As a result, reputational risk has become one of the most important (and underappreciated) considerations of an organization's ethics and compliance program. Reputational red flags include the exploitation of marketplace disruption and innovation, an organization's willingness/preparedness in responding to and recovering from crisis events, and gaining insight and assurance relating to corporate sustainability programs. As an example, many international regulatory environments are focusing on conduct risk reporting, which adds a relatively underdeveloped component of risk assessments to an organization's holistic consideration of risk. Chief marketing officers, chief communications officers, and external public relations experts can and should contribute to an organization's assessment of reputational risk.

Tools, such as small-audience pulse surveys, focus groups, and other forms of direct and candid employee feedback surveys, assist companies in their determination of risk profiles, establish a baseline for conduct risk, and unearth conduct risk drivers.

Ideally, a holistic risk assessment will encompass each of the above four categories when a multinational company is developing an entirely new compliance program or doing a periodic review of an existing program. Alternatively, and perhaps more efficiently, companies can simultaneously undertake multiple risk assessments with different areas of focus, meaning more targeted scoping is often appropriate when new risks arise (e.g., when going into a country with a high corruption risk) or specific incidents indicate a need for review (e.g., a whistleblower or other form of complaint). In fact, where needed, a risk assessment can be very narrowly concentrated on only one aspect of the four categories above. For example, risk assessments can be concentrated on bribery concerns in the operational bucket, or sexual harassment in the reputational bucket. Most importantly, risk assessments can be used to pinpoint risk within specific business units, geographies, or even

vendors, agents, and other third parties (e.g., a risk assessment might focus solely on operations in countries with a high corruption risk, or on recently acquired companies). Remember that constricting the scope of a risk assessment is entirely appropriate and can help ensure that new or newly raised risks can and should be remediated through risk-informed and iterative compliance program improvements.

Whatever category of risk is under the microscope, four basic steps should be followed in order to conduct an in-depth and fruitful risk assessment:

1. Gather and review information

In this fact-finding stage, the risk assessment team collects all key information regarding the company's structure and locations, industry sector(s), client base, third-party engagements, policies and procedures, systems and controls, training protocols, audit reports, and compliance reporting. After this information is gathered, the team can appropriately scope the risk assessment, including additional information-gathering meetings, in order to build a comprehensive risk profile.

2. Interview key stakeholders

A list of key stakeholders is then compiled. These individuals are the most knowledgeable about the company's operations, practices, procedures, and its compliance culture. The list should include individuals across the entire organization, including senior management, legal, finance, internal audit, human resources, communications/marketing, and the compliance officer. The team should also consider the best format for evoking actionable information—focus groups, group interviews, and surveys might work best in one situation, but individual interviews could be better suited in other instances, because they may allow employees to be more candid, provide more details and context, and/or describe historical challenges or emerging issues.

3. Review and evaluate identified risks

Next, the team will review the collected information and data and evaluate each significant risk identified against the relevant laws, company policy, mitigating controls, and other applicable standards. For multinational organizations specifically, understanding the impact of international standards and laws on these operations is imperative. If needed, subject matter experts and internal or external legal counsel should be consulted in each local jurisdiction to ensure a comprehensive understanding of best practices, the legal framework, and the regulatory environment. Where possible, a formal risk register should be created wherein each significant organizational risk is mapped against the existing or future mitigating control that the organization relies upon. In an effort to streamline this process, a formal organizational risk evaluation matrix or "heat map" should be developed.

4. Document and report findings and recommendations

Finally, the team documents and reports their findings, offering recommendations for the enhancement of the company's ethics and compliance program. The report should outline each organizational risk profile, the corresponding red flags, and priority risk areas, with the risks ranked according to the likelihood of occurrence and potential severity of impact. The report should also identify any areas that require further assessment and a timetable for updating the risk assessment. Where available, the full report should be presented at periodic and defined meetings of the organization's board of directors. Otherwise, the general counsel and/or chief compliance officer should be notified of the collective findings and appropriate program enhancement actions and plan.

If there is anything to take away, it is this: There exists no one-size-fits-all approach to the assessment of risk, nor is there predetermined guidance as to which testing structure and audit schedule work best for your organization. Risk assessments can be complex and burdensome, thus companies should ensure they have the right team, expertise, data analytics resources, and technology in place to support management through the process, audit current programs, provide actionable tactics for mitigating or remediating future risk, and assist with the implementation of an enhanced ethics and compliance program.