

As more and more companies expand internationally, internal auditors are faced with a new mandate — evaluating the risks associated with an unstable global marketplace.

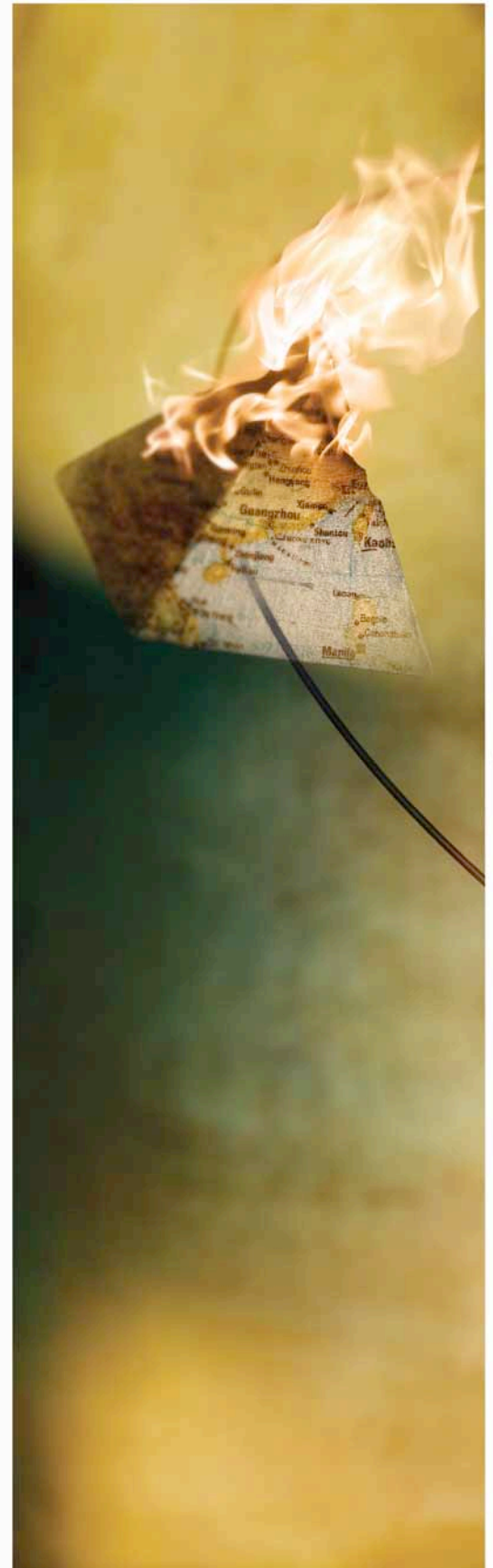
ASSESSING Political RISK

RICHARD CHAMBERS,
CIA, CCSA, CGAP
MANAGING DIRECTOR,
ADVISORY SERVICES
PRICEWATERHOUSECOOPERS LLP

RACHEL JACOBS
MANAGER, GLOBAL STRATEGY GROUP
THE MCGRAW-HILL COMPANIES

ILLUSTRATION BY RICHARD TUSCHMAN

AT A TIME OF INCREASED STAKEHOLDER EXPECTATIONS and competing priorities, annual and enterprisewide risk assessments are now common practices within internal auditing. However, the transition to a more risk-based approach to audit planning is presenting a mix of old and new risk challenges to chief audit executives (CAEs). CAEs continue to face familiar risks in the areas of operations, finance, and compliance, which their internal audit staffs can assess with relative ease and





comfort. At the same time, however, companies are facing a host of new and unexpected challenges as they expand internationally in search of new markets and lower-cost business models.

Three trends, in particular, are increasing the risks faced by companies with global concerns or aspirations:

1. *Financial markets and supply chains are both more interconnected and more volatile.* These conditions should be quite apparent to any organization operating in international markets.
2. *The world is dependent for energy on states with increasing levels of political instability.* Political instability in oil-producing states can quickly produce significant global shock waves.
3. *Increased outsourcing and off-shoring of manufacturing and services heightens*

the fragility of global supply chains.

Companies are moving into countries that are less familiar with the demands of foreign investors in search of lower-cost locations. At the same time, multinational corporations operating in traditional outsourcing locations continue to be concerned by issues such as the preservation of intellectual property rights.

Risks associated with the pursuit of global markets can be difficult for internal auditors to identify and assess. This is particularly true when it comes to political risk, which can be defined as any political change that alters the expected outcome and value of a given economic action by changing the probability of achieving business objectives.

When companies operate abroad in unfamiliar political environments, they are often exposed to new types of risks and complexities that can threaten business performance as well as mask new opportunities. Such factors can range from regulatory and compliance changes lowering barriers to market entry to practices that violate the U.S. Foreign Corrupt Practices Act (FCPA) (see “The Fight Against Corruption” on this page). Given the scope of such challenges, executives of global companies are searching for the best ways to assess, identify, and understand political events and trends, factor them into their investment decisions, and use the knowledge gained to help improve global business performance.

POLITICAL RISK ANALYSIS

When it comes to making key decisions about global investments, political considerations can be just as important as economic factors in the decision-making process. Part of what makes emerging markets so attractive — pent-up demand in a country opening to foreign trade, investment, and cultural influence — is also what makes such markets unstable.

If a company has existing exposure in foreign markets, or if it is considering making major investments in infrastructure or operations abroad, it needs timely, accurate, and objective assessments of the political environment. Economic analysis fails to tell the whole story, particularly in countries where statistical data is either difficult to collect or is manipulated to serve policy interests. It is simply too risky to base global investment decisions solely on economic data without understanding the political context for a decision.

With political risk analysis, a company can make better and more timely decisions about international operations, protect existing global investments, improve business performance, and exit unstable markets. It can anticipate the business-risk implications of political change as well as identify both opportunities and risks stemming from political shifts and instability. And it can take steps to mitigate risks, protect against unwanted surprises, and improve measurement using risk-adjusted evaluation of international performance.

The Fight Against Corruption

U.S.-based companies have come under greater scrutiny in recent years due to the compliance demands of the Foreign Corrupt Practices Act (FCPA). The sharp upswing in FCPA-related investigations and settlements stems, in large part, from the testing and controls provisions of Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and from stepped-up penalties for corruption-related violations. Other factors behind the surge in FCPA enforcements include elevated whistleblower activity, growing cooperation between international government regulators in the anti-corruption arena, and a dramatic increase in the scrutiny of emerging markets.

In addition to being subject to the FCPA, U.S. companies are now covered by the United Nations Convention Against Corruption (UNCAC), the first international anti-corruption agreement to be applied on a global level. Parties to UNCAC, including the United States, agree to criminalize corrupt conduct, to actively deter corruption, to cooperate internationally on law enforcement, and to take steps to facilitate international efforts to recover assets. The United States, which approved the United Nations measure in late 2006, is actively promoting UNCAC as the cornerstone for regional multilateral anti-corruption activities.

The crackdown on questionable business practices under both the FCPA and UNCAC is forcing many companies to implement complex mitigation measures, to develop more stringent internal guidelines, and to conduct costly investigations of their foreign operations. It's not unusual for some deputy internal audit directors at major multinational corporations to spend up to half their time on FCPA investigations.

The core challenges facing management and internal auditing in assessing FCPA risks deal with identifying officials who might have received questionable payments from the company and the routes through which such payments were made. Political risk analysis can help auditors develop roadmaps to link individuals and government-owned companies with a given entity. Areas of particularly high risk include governmental decision-making in the areas of pricing, reimbursements, formulary listing, bulk purchasing, and licensing as well as charitable contributions and contracts with third-party agents. Political analysts can develop “power maps” to illustrate the linkages between government officials and private industry as well as the subsidiary relationships through which payments could be transmitted.

MANAGEMENT'S ROLE

It is management's role to identify, assess, and manage risk. As more and more companies begin to appreciate the myriad challenges inherent with global expansion, they likely will make political risk, in particular, a key component of their enterprisewide risk assessments and assess it more formally. By taking a comprehensive, enterprisewide approach to political risk, management will enhance its ability to grasp the implications and interdependencies between political risk events and other risk considerations.

Political risk management requires a systematic framework to evaluate the impact and likelihood of individual events and to ensure that political risk information is available when and where it is needed to enhance corporate decision-making. It also requires a formal program to assess and monitor political risk across business lines that includes procedures to gather, interpret, and evaluate political information from multiple sources. Such procedures strengthen management's ability to produce timely, accurate data on a variety of social and political trends and to provide updated political risk assessments to key managers.

To initiate the assessment process, management should conduct a baseline assessment of the political risk events affecting business strategy and objectives related to operational efficiency and effectiveness, compliance, and reliability of reporting. This evaluation should include an assessment of the events emanating from four primary risk event categories:

1. *The macro-political environment*, from the policies and attitudes of political leaders toward business — such as privatization, foreign ownership, and corruption — to regulations, taxation structures, and other factors that can influence both the competitive environment and the ability to do business in a country.
2. *Economic policy*, which influences foreign exchange rates, inflation, and other aspects of economic growth.
3. *Social risks*, such as shifts in demographics or social behaviors as well as societal conflicts or tensions.
4. *Security issues*, such as government preparedness for catastrophic events

caused by either natural or human events — from hurricanes and earthquakes to cross-border conflicts, terrorist attacks, bio-security threats, or environmental disasters.

With the insights gained from these event categories, management can create a comprehensive political risk analysis that encompasses both the risks and opportunities associated with global

Political Risk Assessment — Key Steps

1. **Map the politics.** Create an external political risk profile that provides a cross-country view of portfolio risk and allows the company to manage global investments with a portfolio perspective.
 - Given the natural bias of many internal and external sources of political risk information, rely on a broad spectrum of trusted sources for insight, including in-country networks, on-site management, and neutral third parties.
 - Identify the company's global market presence at an entity, country, and regional level — whether this presence is direct (i.e., ownership interest or control) or indirect (e.g., dependence on a global supply chain or energy pricing influenced by global trends).
 - Evaluate the organization's potential exposure in each jurisdiction, particularly with respect to macro-level risks such as regime change, terrorism, political instability, and weapons proliferation.
2. **Evaluate risks.** Apply the information and insights gained in the political mapping process to identify specific, prioritized, business-relevant risks to operational performance.
 - Examine the relationship between political stability and major, macro-level performance indicators.
 - Develop a structured and iterative approach to assessing the impact of political stability on business performance and capital values.
 - Analyze the impact of identified political and business risks on the company's strategy and regulatory compliance and on critical operations and processes.
3. **Assess controls and plans.** Explore the adequacy of the company's assessment controls and procedures, focusing on the degree to which controls are exercised through corporate oversight or local capabilities.
 - Determine the company's level of preparedness. Examine the quality of existing controls and the adequacy of risk mitigation plans relative to identified business risks.
 - Estimate the impact of political volatility on the company's sales growth and gross margins.
 - Analyze the degree to which the company integrates political risk management into strategic decision-making and operational practices.
4. **Determine acceptability of residual risk.** Integrate political risk management into strategic decision-making and ongoing monitoring activities.
 - Look at the risks that remain after the organization has taken steps to mitigate its risks and evaluate the process the organization uses to determine the acceptability of these risks.
 - Be proactive in communicating information about political risk timely throughout the organization, especially to decision-makers at the corporate and operating-unit levels who are responsible for areas such as strategic planning, operational processes, and crisis preparedness.
 - Consider formalizing political risk assessments by having internal auditing: 1) conduct overall assessments on a regular basis; 2) focus on political risks in a specific country or region, such as a study of potential regulatory changes in Brazil; or 3) audit an issue that continues to challenge international operations, such as potential FCPA violations.

investment decisions. If a company determines that a particular investment is worth the attendant risks, it can take steps to mitigate related risks, such as recruiting local partners or limiting research and development activities in nations where intellectual property is not sufficiently protected.

Management also can use scenario planning to put changing political risk scenarios into perspective. At its core, scenario planning seeks to determine the driving forces behind trends in global affairs — drivers that can include market factors, social trends, and technology development as well as patterns of coercion or state regulation. Analysts synthesize these factors into a forward-looking picture of the political environment and assess how these events could impact business decisions. With such scenarios, managers can improve corporate decision-making by identifying

a range of possible outcomes and how they might impact a company's overall risk portfolio.

INTERNAL AUDITING'S ROLE

With management responsible for the identification, ongoing assessment, and management of political risk events, internal auditing can play a role by evaluating the overall effectiveness of these processes. Lack of consideration of political risks by management should be a red flag to internal auditing and the audit committee that senior executives could be overlooking a key area of potential risk, thus increasing organizational vulnerability.

Whether or not management is addressing political risk on a formal basis, this risk needs to be a key consideration in internal auditing's risk-assessment process. If management's enterprisewide risk assessment does

include political risk events, internal auditing should weigh the findings of management's risk assessment and its impact on the internal audit plan. Conversely, if the enterprisewide risk assessment conducted by management does not formally address political risk events, internal auditing should consider expanding the scope of its audit and risk-assessment activities to incorporate this type of risk.

Internal auditors should gather objective information about political risk events, factor this information into their risk-based audit planning activities, and communicate the audit findings to the audit committee and management. Until political risk analysis is firmly embedded within the organization's management activities, and internal auditing can assess the overall effectiveness of these activities, auditors should be sure to include a clear focus

10 Steps to Foreign Corrupt Practices Act Compliance

There are several steps organizations can take to ensure compliance with the FCPA.

Step 1 — Ensure that corporate standards address FCPA compliance issues and establish minimum thresholds for compliance. Update corporate documents, policies and communications relating to anti-bribery and anti-corruption activities, internal controls, payments to government officials, and other pertinent subjects.

Step 2 — Evaluate corporate policies to ensure that they appropriately address compliance with provisions of the FCPA. Develop a set of "global" standards and expectations for controls around high-risk business activities that establish a basic expectation for having process and controls related to books and records requirements.

Step 3 — Provide management training on FCPA compliance. Promote compliance by educating local management on the key tenets of FCPA, the inter-communications of regulatory agencies, expectations of international and local country "pharma codes," risks of whistleblowers, and increases in local regulatory agency investigations.

Step 4 — Assess FCPA compliance and document processes and controls in select/higher risk subsidiaries (leverage Transparency International's Corruption Perceptions Index, revenue data, and anecdotal information to select regional representation). Conduct risk assessment findings by affiliate, produce detailed process maps for each high-risk business activity, and create recommendations for corrective action or remediation.

Step 5 — Develop a "global" FCPA compliance implementation program. Develop a formal, standard set of processes and model policies and procedures to be implemented locally. Create an implementation tool kit with recommended monitoring controls and internal reporting protocols to meet FCPA compliance requirements.

Step 6 — Conduct subsidiary pilot programs focused on testing the execution of the FCPA compliance implementation program locally. Test and refine your Step 5 deliverables.

Step 7 — To support global rollout of the FCPA compliance implementation program, conduct global training on the FCPA, company policies, the FCPA compliance implementation program, and the implementation tool kit. Conduct webcasts and selective live meetings designed to train local management on FCPA, company expectations for FCPA implementation, and tools to promote implementation.

Step 8 — Implement the FCPA compliance program globally. Develop target dates for subsidiary implementation of the program.

Step 9 — Perform post-implementation validation reviews at select subsidiaries, focusing on those that did not receive implementation assistance, to assess management's implementation of the FCPA compliance program.

Step 10 — Develop reports on the results of post-implementation reviews for each subsidiary. Include recommendations for improvement. Transfer internal audit programs for ongoing FCPA compliance monitoring.

on political risk events as part of their overall annual risk assessment.

In assessing political risk management, auditors should determine whether:

- Current risk-management processes consider relative or potential exposure on a country-by-country basis and provide a portfolio view of risk across all of the company's global operations.
- The organization has a structured approach to translating risk events that stem from political change into business risks and analyzing their potential business impact.
- The quality of the risk-management controls and risk-mitigation plans is sufficient to address the political risk events facing the company.
- How the organization makes decisions about residual risks once it has taken steps to mitigate political risk events.

For new or existing investments or operations, and for sales or supply chains in international markets, internal auditing should monitor rapid economic growth, instability or deterioration, increasing levels of foreign investment, and major changes in governmental leadership. Auditors should also pay close attention to potential changes in regulations or trade agreements affecting the organization, such as social unrest and major security issues that are not being addressed adequately.

A country's relative stability and openness also need to be factored into evaluations of political risk management. "Stability" is the capacity of political leaders to withstand destabilizing political events and avoid creating their own. "Openness" is the degree to which a country is open to global influences, including those brought into the country through free and independent media and sale of commercial products. Countries can be stable because they are open, like the United States, or stable because they are closed, like North Korea. To transition from one end of the spectrum to the other, a country must often go through a difficult period of political instability. Good analysts will look for such inflection points when assessing global risk exposures.

In assessments of political risk management, internal auditors also should keep in mind three caveats with respect to the monitoring process:

1. Political risk assessments are inherently more subjective than economic analysis

and are thus more vulnerable to bias.

When seeking information about political risk, internal auditors should look to analysts who account for such bias in the pursuit of an objective viewpoint on a given situation.

2. A systematic approach to gathering and processing information is more important than the choice of quantitative versus qualitative analytical methods.
3. Organizations have a tendency to make international business decisions based on incomplete or misleading information about

UNDERSTANDING POLITICAL RISK

To a growing extent, audit committees and executive management — internal auditing's key stakeholders — are acknowledging that political risk is a major and growing concern for companies pursuing global markets. At the same time, because political risk events are so difficult to measure and quantify, they are rarely assessed and incorporated into audit plans by internal auditors or addressed by any other corporate functions.

Within most companies, internal auditing is responsible for identifying



the political landscape from local sources, a factor pointing to the need for objective, third-party analysis. When local sources provide input for decisions affecting global operations, they rarely do so with the intent to mislead. However, their input can be skewed by a wide range of factors — from the influence of local news reports and the acclimation of local managers or expatriates to risky environments to the desire to promote personal interests, such as the expansion of operations under one's own control.

At one time, corporate internal audit functions sought comfort in the fact that the political climates in which their companies operated were relatively stable and predictable. However, with continued growth of the global economy, more and more companies are expanding operations into geographic regions in which their internal auditors have little or no knowledge or experience. The ability of internal auditing to assess and address expansion-related risks in the future will be a key success factor in providing comprehensive audit coverage.

and prioritizing areas of significant risk and for developing an audit plan to address these risks effectively. To fulfill this mandate, CAEs and their internal audit staffs need a solid grasp of how political factors affect corporate governance and regulatory compliance in addition to operating performance and bottom-line earnings.

Political events and the risks and opportunities they can create for organizations pursuing global markets are real and warrant the attention of internal auditors and the enterprise leaders they serve. At a time when risk-based auditing has become a major driving force within business circles, the internal audit risk assessment and audit planning activities of multinational organizations need to address changes in the political environment. By monitoring organizational exposures to political risk events, internal audit groups will help their organizations create a systematic, companywide approach to risk management.

To comment on this article, e-mail the authors at richard.chambers@theiia.org.