Control Risks

RISK

AN ORGANIZATIONAL PERSPECTIVE

Managing Risk | Maximising Opportunity

TABLE OF CONTENTS

Published by Control Risks, Cottons Centre, Cottons Lane, London SE 1 2QG. Control Risks Group Limited ('the Company') endeavours to ensure the accuracy of all information supplied. Advice and opinions given represent the best judgement of the Company, but subject to Section 2 (1) Unfair Contract Terms Act 1977, where applicable, the Company shall in no case be liable for any claims, or special, incidental or consequential damages, whether caused by the Company's negligence (or that of any member of its staff) or in any other way.

INTRODUCTION

There is little doubt that the risk environment faced by multinational companies is becoming exponentially more complex. The headlines have been full of potentially catastrophic geopolitical developments like the rise of a radical Sunni Muslim fundamentalist army in the Middle East, the Ebola epidemic in West Africa, the frayed relationship between Russia and the West, and the conflict in Gaza.

The global regulatory environment is also evolving rapidly, with new anti-corruption enforcement agendas playing out in China, Brazil, India and Canada, and the rise of the empowered whistleblower making it ever harder for companies to control reputational and legal risk. Financial markets seem increasingly unpredictable, divorced from everyday realities. The security environment is deteriorating across geographies, and traditional measures to protect employees appear inadequate in the face of insufficient state capacity, rising public anger over inequality and lack of access to opportunity and government services. Finally, strategic risk questions grow increasingly complex in the face of transformative technological change, market volatility and competitive landscapes in which industry distinctions are blurred and 'disruption' has become a key corporate buzzword.

A few multinationals have placed risk management at the center of their strategic agendas. They have appointed chief risk officers and focused on creating a coordinated approach to risk that encompasses quantitative and qualitative dimensions and applies a thorough, nuanced lens to risk management across the organization. Even so, coordinating and responding to risk remains highly challenging for corporates. And many organizations approach risk management as a painful bureaucratic process rooted in compliance and health and safety – and correspondingly lacking in dynamism and commercial relevance. Anecdotal tales of confusion over scope, communication, responsibility and authority abound.

Here is a sample of off-the-record comments I've heard from clients during the last month:

From a general counsel: "We have tried our best to implement a robust third party due diligence framework, but we still get a ton of pushback from the business about the cost. No, we don't share the reports with the business development team, we just keep them on file in the legal department in case we run into trouble."

From a business development manager in Shanghai: "The anti-corruption crackdown here is truly a game-changer and like nothing we have seen in China before. But head office keeps on pushing us to grow just as fast as before. The compliance people seem to think that all they need to do is hire an FCPA lawyer and they can limit their risks. But business practices from 10 years ago are coming back to

haunt our competitors. I'm really concerned, and I am not sure that the U.S. headquarters really gets it."

From the chief risk officer of a major multinational law firm: "Our people seem to think they can jump on a plane and go wherever they like when they like. We have no idea where most of them are from week to week. The same applies to client acceptance.There are processes in place, but no one pays any attention to them as long as conflicts of interest are cleared." From a chief compliance officer: "My areas of responsibility are growing every month, but my budget isn't. I only get oversight of new deals and ventures at the last minute because the sales people don't want me to have enough information to block their deals."

From a head of strategy: "We just completed a major acquisition and now have on-the-ground presence in a number of new, high-risk markets from Pakistan to Guatemala. We need to roll out a comprehensive approach to risk and have arranged online training on our compliance processes, but the old management team is still in place, and they seem to do things differently from us."

All the problems above could be addressed within a more robust risk management framework, but that is difficult to establish and execute. The traditional preventative approach to risk management is proving inadequate in the face of regulatory complexity, volatility and an environment of constant change. What should replace it is not yet clear. Notably, many companies currently under investigation by the U.S. Department of Justice had expensive risk management and compliance programs. Indeed, sophisticated, quantitative-risk management practices did little to control the financial sector behavior that led to the 2008 financial crisis. The disruption to supply chains from 'black swan' events such as tsunamis – or man-made ones such as Fukushima – is well known, but it is difficult to make provisions for such low-likelihood, high-impact events in practice.

A host of developments suggest that too many companies are reenacting the metaphor of the blind man and the elephant. They need to take the next step: adopt a holistic perspective that embeds risk consciousness into every part of their businesses, not just in the departments charged with formal regulatory or policing roles. In order for the concept of risk to move beyond idealistic aspiration, companies need to look closely at the way they view and understand risk and at the implications for their organizational structures and culture. This paper argues that models of organizational analysis are a critical next step in elucidating and developing meaningful corporate responses to risk.

THE EVOLUTION OF RISK MANAGEMENT

The historic origins of the risk management industry explain why so many companies continue to understand and respond to risk in such a narrow, restricted fashion. Risk management originated in the insurance industry and in areas of corporate internal control, particularly around health and safety issues. The risk management industry evolved significantly following passage of the Sarbanes-Oxley Act of 2002, which prompted U.S. public companies to establish frameworks to manage risk. Many companies use the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework, which specifies creation of a controlling environment and framework. An International Standard for Risk Management, ISO 31000, was created in 2009 to provide a standardized structure for conceptualizing and contending with various risks.

The financial sector in the 1980s began developing sophisticated quantitative tools to understand market, credit, operational and liquidity risk, though these have come into question in the wake of the 2008 financial crisis and amid ongoing evidence of widespread systemic failure in the financial sector. Enforcement of anti-corruption laws, particularly the Foreign Corrupt Practices Act and the U.K. Bribery Act, generated a specific framework to assist companies in managing corruption risk – including policies and procedures, corruption risk assessments, third party due diligence, training, monitoring and review. Finally, strategic planning often involves a risk- or threat-assessment component. Strategic planning uses a host of sub-frameworks, including Political-Economic-Social-Technological (PEST) risk analysis, Strengths-Weaknesses-Opportunities-Threats (SWOT) analysis, and Michael Porter's Five Forces, which are directed at understanding external and competitive environments and an organization's ability to respond.

Today, companies may use a number of overlapping frameworks to understand and respond to risk. The majority of these frameworks remain one-dimensional. No surprise, then, that the organizational response to risk is so fragmented – and that so many companies view risk management as a cost, failing to incorporate it into strategic and commercial considerations. In beefing up risk management functions, corporations have generally hired risk management specialists from the financial services industry, perpetuating a quantitative, market-based focus. This approach is essential but often fails to cover the spectrum of risks companies face.

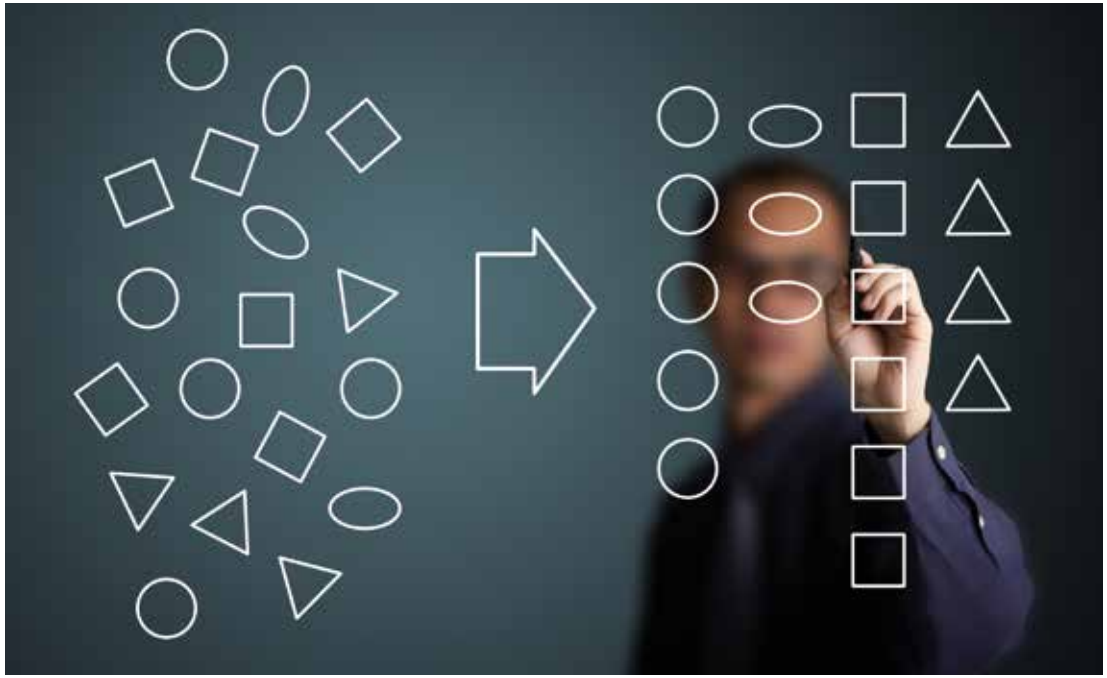
In its 2014 overview of Risk Management and Corporate Governance in 22 countries, the OECD comments:

"Existing risk governance standards for listed companies still focus largely on control and audit functions, and primarily financial risk, rather than on (ex ante) identification and comprehensive management of risk. Corporate governance standards should place sufficient emphasis on ex ante identification of risks. Attention should be paid to both financial and non-financial risks, and risk management should encompass both strategic and operational risks …

"Effective risk management is not about eliminating risk taking, which is a fundamental driving force in business and entrepreneurship. At the same time, the need to strengthen risk management practices has been one of the main lessons from the financial crisis, for both financial and non-financial companies. While this is well recognized, there is limited evidence that listed companies have in fact paid significantly more attention to risk management in recent years."

The OECD concludes by calling on companies to put in place better structures to understand and respond to risk environments. The most successful companies in the future will undoubtedly be those that best understand and respond to the risk environments they face. The best way to do this remains an open question. Placing a central focus on the nature of the organizational response provides a compelling way for companies to address key governance, risk and compliance questions, as well as providing a much-needed path from the theoretical to the practical.

CONDUCTING A RISK ASSESSMENT



Discussions of corporate governance, risk and compliance tend to begin with a debate about corporate risk appetite, followed by the development of a risk taxonomy – a list of risks that can be prioritized, mapped on an impact-likelihood matrix and then transferred, avoided, accepted or reduced, as appropriate.

Often, dozens of risks are whittled down to the top 10 or 20 that an organization deems to be of highest concern and posing the largest potential impact. Mitigation measures are designed accordingly. The risk categories employed vary enormously. One organization, for example, might classify risks as strategic, operational, environmental, financial, competitive and legal. A second organization might use its internal departments as proxies and come up with financial risk, people risk, legal risk, reputational risk, supply chain risk and so forth. Given that models for aggregating risk were largely discredited by the events of the financial crisis, the current approach is to set risk appetite and tolerance with respect to each risk identified.

Developing an understanding of risk appetite and conducting a risk taxonomy are vital steps in developing an organizational capacity to respond to risk. However, these exercises need to be conducted with care and with an eye toward organizational realities. Otherwise they merely perpetuate existing structures and biases. All risks are not created equal, and different risks require fundamentally distinct responses.

Although risks can be divided into multiple categories, it may be helpful to regard them as 1) risks that can be eliminated with the right preventative control environment, 2) external risks that the company cannot mitigate through internal measures and 3) risks that contain an opportunity dimension – and may be welcomed in some cases[1].

Preventable, internal risks are those that a company aims to eliminate and that can be treated with a strong, rules-based compliance culture. These relate to criminal or fraudulent behavior by employees, or failures in standard operational procedures. They might include risks of employee fraud, cyber-security breaches, payment of bribes, conflicts of interest and health and safety regulations. Although the risk of employee fraud, for example, cannot be eliminated entirely, the goal is to get these risks as close to zero as is practically possible. Unsurprisingly, companies in highly regulated industries tend to focus more on internal compliance processes, but the existence of processes does not in itself guarantee an effective response.

[1] Managing Risks, A New Framework, Robert S Kaplan and Anette Mikes, Harvard Business Review June 2012

Strategic and external risks are those that companies may accept in order to pursue a particular strategy; effective risk management lies not in prevention but in scenario planning and rapid response. Because companies routinely underestimate both strategic and external risks – focusing only on the upside opportunities seen in a strategy or market – extra care must be taken to incorporate the possibility of failure. This runs counter to the culture of most organizations. Executives tend to carry a cognitive bias that underestimates risks to strategic plans and forecasts, and overestimates their ability to influence events. And senior management teams are far more inclined to focus on lessons drawn from previous successes, disregarding or underplaying strategic failures.

Strategic risk appetite determines responses to competitors or market developments, to drivers of investment in new business lines or research and development, and to credit risk in the financial sector. Strategic planning is designed to reduce the threat of downside risk and to respond to undesirable events as they occur. These risks are not mitigated via a control model, but they need to be identified so responses to them can be planned.

External risks fundamentally lie outside a company's control. These include geopolitical risks such as expropriation, regime change or instability, along with major macroeconomic shifts. External risks also include natural disasters such as earthquakes. Although companies can rarely influence these events, they can gain significant competitive advantage via extensive scenario-based preparations and the execution of rapid, appropriate responses.

Some risks are more predictable than others. The sanctions against Russia, which took many by surprise, provide a prime example of a shift in the external investment environment that was foreshadowed for years by warning signs. The Arab Spring, on the other hand, was generally not predicted by analysts.

Despite the limitations of scenario planning and political forecasting, companies that focus on external intelligence gathering have opportunities to make lucrative investment decisions that run against the grain of prevailing market opinion. For example, while risk evaluation in sub-Saharan Africa has become more nuanced in recent years, many companies still treat Africa as a monolithic high-risk environment. They fail to take account of critical differences from country to country in investment climate, institutional capacity and political risk. Companies that take time to understand the continent will find that risks tend to be underpriced or overpriced by the market.

In managing preventable risks, cost and proportionality of response are the key issues. In contrast, managing strategic and external risks requires balancing risk and opportunity. For example, sourcing a product from a sole supplier can reduce costs and increase margins while making a company more vulnerable to supply-chain disruption and correspondingly, less resilient. Entering a frontier market may allow a company to exponentially expand its business while massively increasing its political, operational and regulatory risk profile.

By categorizing risks in this way, companies can incorporate consideration of the organizational response. However, risks that might be deemed preventable by one company could be viewed as strategic by another. Even more important, some risks have more than one dimension. Individually limited risks can also have a force-multiplier effect when combined with each other. Currency risks are negligible for a small, domestically focused manufacturing business but may be highly strategic for certain financial sector firms. Physical safety issues might be a primary concern, with a strong strategic and geopolitical dimension, for a junior mining company operating in remote communities in Latin America, but they will be seen as a preventative health and safety risk for the operator of a factory inside the U.S. And a company might face risks of labor force disruption that are highly strategic but that can be mitigated by process enhancements that enable rapid transfer of sourcing and production from one facility to another. These examples show wide variation in the risk landscape experienced by individual companies, illustrating the importance of considering the full organizational implications of the risk management response.

THE ROLE OF RISK CULTURE

Risks have fundamentally different characteristics, which explains why so many companies struggle to respond across the full risk spectrum. The types of risks that are prioritized – and the responses that are favored – reflect an organization's risk culture. Risk management best practice requires developing organizational muscles that can be flexed in different ways, not a one-size-fits-all approach. Still, most company responses are driven by ingrained cultural assumptions about risk.

Companies that have strong internal control systems and a cautious, compliance-based approach to risk often struggle to react quickly to market developments and to be competitive and nimble; their response to the external environment is slow and highly controlled. Meanwhile, companies that focus on strategic and commercial responsiveness often harbor cultures that resist rigid compliance processes; the ability to be fluid in responding to changes in the external environment does not easily flourish in a strong compliance framework. Companies that deal with a complex web of regulations and government interactions are often inclined to leave risk management to the legal department. Companies that face particularly challenging external risk environments may assign risk to the security team. Companies with aggressive investment plans highlight the opportunity dimension of risk. Companies that focus on reputation and customer perception are more inclined to incorporate ethics and governance terminology in their risk management approach.

Numerous research studies have determined that rules and processes do not exist in a vacuum and that organizational culture is a critical explanatory factor of employee behavior[2]. This has led to fashionable talk of 'a culture of compliance'. The norms and assumptions that determine responses to ethical guidelines are more important than procedures that cover every eventuality. If employees do not believe that risk management is an essential component of organizational success, processes will not solve the problem. Indeed, processes that exist but are widely ignored cause more damage than no processes at all because they can generate a false sense of security among senior leaders. The danger is that risk assessments focus too exclusively on process and structure, ignoring more subtle drivers of employee behavior.

Comprehending a company's risk management strengths and weaknesses is greatly enhanced by gaining an understanding of a company's risk culture. This can be viewed as a subset of wider organizational culture – commonly summarized as "the way we do things around here". The importance of culture is often underplayed, as it appears to be a function of human irrationality and is difficult to measure and describe. But ignoring culture is a mistake. When mergers and acquisitions run into trouble, this is often the product of nebulous 'cultural factors' – the difficulties that members of different organizations encounter working together – rather than poor planning, pricing or market strategy. Cultural factors also explain why 70 per cent of organizational change efforts fail.

According to Edgar Schein, a pioneer in the organizational culture field, culture is the most difficult aspect of organizational life to alter. It can outlast leadership transitions, changes in products and services, geographic footprint and other physical, measurable attributes of a company[3]. Schein describes three levels of culture. The first level, an organization's artifacts and rituals, are easily observable. They include facilities, offices, furnishings, the way employees dress and behave and the myths and stories the organization tells about itself and its history. A company that names conference rooms after major global cities is saying something about its culture and aspirations, as is a company whose line managers sit in cubicles, along with their teams.

The second level, espoused beliefs and values, reflect an organization's statements about what it stands for – its primary goals and modus operandi. This includes statements such as 'we put our customers first' and 'we value diversity in our employees'. The values of a company will include perceptions an employee has about its reliability and trustworthiness and will also determine its approach to risk. An organization focused on aggressive expansion into new markets is going to have a different risk culture than a domestic operation in a highly regulated industry.

The second level of culture can conflict with the third level – an organization's underlying assumptions. This level describes traits that are rarely, if ever, discussed; they are taken for granted. Employees

[2] Compliance Culture: A Conceptual Framework, Lisa Interligi, Journal of Management and Organization, May 2010.
[3] Organizational Culture and Leadership: a Dynamic View, Edgar Schein, 1992.

become acclimatized to these 'unspoken rules' over time and may not even be conscious that they exist. Nonetheless, they are critical to understanding organizational culture. For example, employees may avow belief in open communication around risk and integrity issues while communicating a strong, unstated belief that concerns should not be shared with the boss. A heavy focus on internal processes and checks and balances can be undermined by implicit signals that it's OK to game the system. A CEO may speak regularly about transparency and inclusiveness but make opaque, highly political promotion decisions. The existence of this third layer explains why so many organizations engage in apparently contradictory behavior.

By gaining a deeper understanding of organizational culture, it is possible to enhance risk management efforts. Employee surveys, confidential interviews and focus groups are some of the methods Control Risks uses to understand a company's risk culture. It is particularly useful to highlight gaps between employees' experience of risk and an organization's standard responses. Any risk management change effort that does not take into account organizational culture across divisions, locations and levels of seniority will never be 'owned' by the organization. It cannot take root or succeed.

Risk taxonomies are an essential tool in providing an enterprise-level view of risk and in planning an objective, logical organizational response. Still, such exercises will be of limited use if they do not consider the diverse characteristics of individual

ORGANIZATIONAL RISK CULTURE		
	WEAK	STRONG
Strategic Clarity	Little consistency on strategic appetite and overall risk tolerance.	Risk calculations are factored into strategic decisions. Employees are clear about strategy and risk tolerance.
Tone at the Top	"Do as I say, not as I do".	Senior leadership models appropriate behaviors and emphasizes risk, ethics and governance.
Transparency	Little information sharing across divisions, regions and levels of seniority.	Good knowledge sharing, including top-down and bottom-up communication.
Ethics	Focus on ethics is low, and commercial considerations take precedent.	Employees are encouraged to raise concerns, even when this might result in loss of contracts or revenue. Where ethical and commercial considerations are in conflict, ethics predominate.
Structure	Little accountability and ownership of specific risks by departments/individuals.	Risk owners are clearly assigned, have sufficient resources and are incentivized to gather information from all groups that experience the risk or have insight into it.
Hierarchy	Strongly hierarchical and directive. Individuals do not challenge others' attitudes or behavior.	Flat structure in which employees at all levels are encouraged to share ideas and give opinions.
Process	Lack of risk management and compliance processes OR excessively heavy focus on a tick-box process, with little employee engagement.	Proportionate process that supports – but does not override – the need for employee judgment and agency.
Crisis Preparation	Overconfidence: "That wouldn't happen to us."	High preparation through crisis management and business continuity planning.
External Focus	Low use of external sources of information and intelligence.	High use of external information and on-the-ground intelligence, easily accessed by all employees.
Risk Reporting	Signs of ethical breaches, whistleblower reports and other risk events are not investigated and/or not communicated, encouraging apathy.	Concerns and issues are investigated promptly. High-level findings are shared regularly with the board and across the organization.

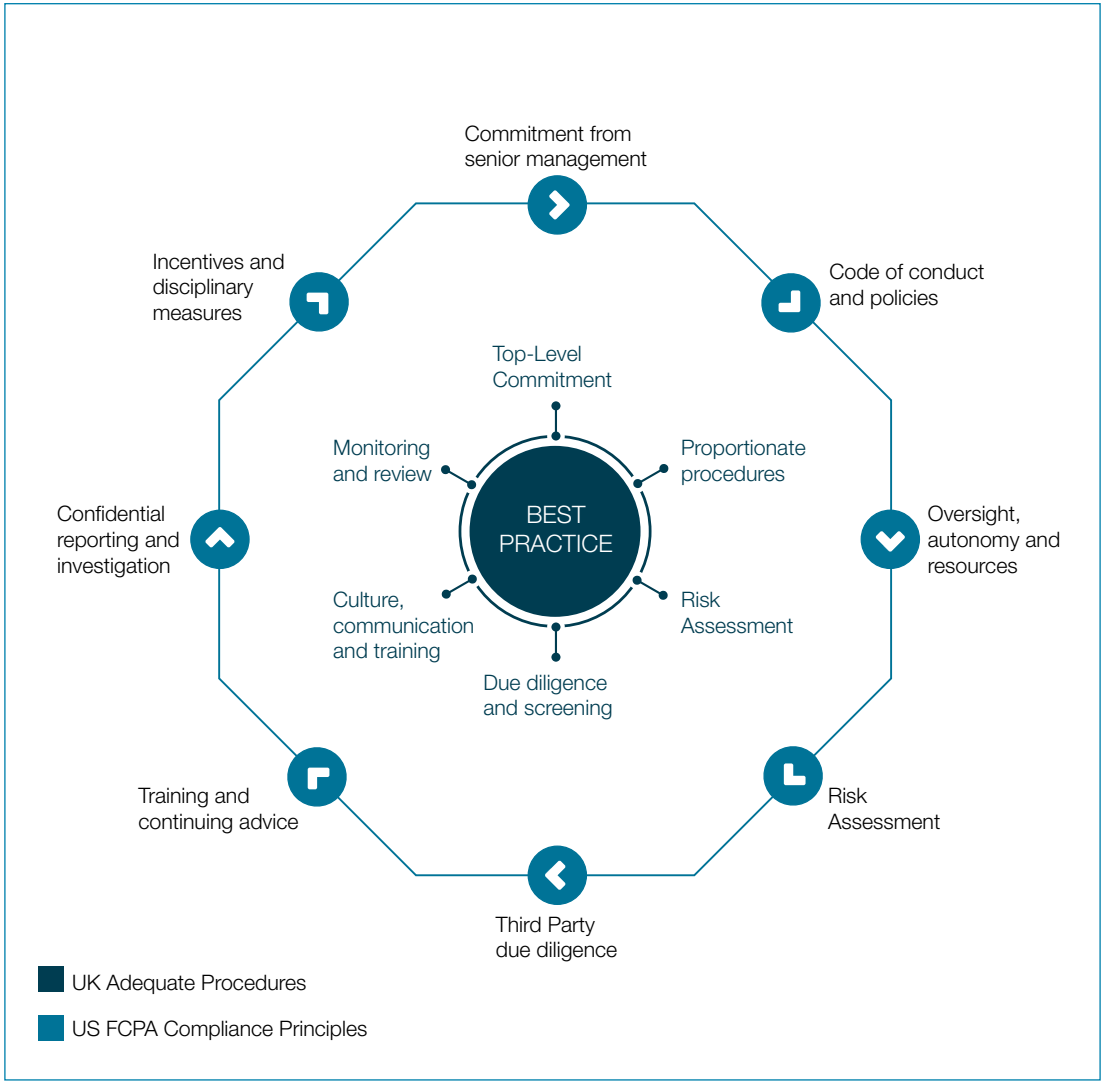
risks and the importance of organizational culture in risk management efforts. It is no accident that state-of-the-art enterprise risk assessments so often end up on a shelf, ignored.

Managing Corruption Risk: An Example of Complex Risk

The difficulty of responding to multi-dimensional risks is perfectly illustrated by the current state of play on anti-corruption. Although the Foreign Corrupt Practices Act was passed in 1977, the scale and scope of responses to corruption risk have been increasing exponentially of late, with enforcement becoming more aggressive and globally coordinated. Subjected to a bewildering array of overlapping laws and guidance, multinationals are expected to put in place comprehensive systems to ensure that employees do not engage in corrupt behavior. The latter includes the payment of bribes (directly or via third parties), use of anti-competitive insider information, conveyance of excessive gifts and entertainment or pursuit of any illegal or unethical activities designed to drive market advantage.

Discussion abounds as to how companies should respond to and manage corruption risk. Here is the emerging best practice framework promulgated by US and UK regulators. (see right) **>**

This framework provides relatively clear guidance as to how companies should respond to corruption risk, with very little excuse to ignore regulatory direction. Given the framework's focus on policies and procedures, due diligence processes, internal



reporting and accounting, it is unsurprising that companies tend to treat corruption as a 'preventable risk' and make anti-corruption implementation the responsibility of the compliance and legal department. The dominant approach is to treat corruption risk as employee behavior that can be eliminated with the right internal processes, and the regulatory climate means that 'zero tolerance' is the only appropriate public position for companies to take on the issue. It is logical and unsurprising that companies lean heavily on audit reviews and policy implementation to highlight gaps in process. Given the current overall lag in implementation, the companies that have even the basic elements of a program in place can be considered market leaders in tackling corruption.

A compliance-led approach, however, does not tackle the full scale of the corruption challenge, which cuts across every aspect of a multinational company's business. Both the British and American frameworks incorporate an explicit focus on organizational culture, described as 'tone at the top' and 'top-level commitment'. The behavior of senior leaders is rightly understood to be an absolutely critical factor (perhaps the most critical) in embedding a meaningful commitment to anti-corruption.

However, many organizations seem to believe that a statement by the CEO is sufficient and that meeting this challenge is the compliance department's responsibility. There has even been recent discussion of the need for the compliance team to 'sell' itself to the commercial team, an argument that displays the topsy-turvy logic typical of the anti-corruption debate as it stands. The meaningful management of corruption risk relies on senior and middle managers modeling, on a daily basis, appropriate behavior in every aspect of their performance. If the compliance team is used as a bolt-on – set up to police a 'business as usual' approach – employees will quickly find themselves experiencing contradictory messaging and direction about what is important.

The organizational challenges do not stop there. Notwithstanding the validity of treating corruption as a risk that can be mitigated with the right compliance measures, in reality corruption also poses strategic and external risk dimensions that cannot be eliminated, either in theory or in practice. An organization may be committed to a zero tolerance approach to bribery and facilitation payments, but it cannot control the environment in markets where corruption is endemic, often with a strong dimension of extortion. Companies must therefore make strategic decisions as to whether to

enter some markets, accepting a certain level of inherent corruption risk, or stay out of them so they can maintain stated ethical commitments. Treating corruption solely as a preventable risk stymies vital debate around these issues.

The compliance team may hold an accurate understanding of the corruption environment in particular markets, but the implications of this are generally not incorporated into business development and strategic plans. The business growth potential in certain high-risk markets is well known; some level of integrity risk may be considered an acceptable price to pay for first-mover advantage, access to new consumers and the opportunity to take market share from more cautious rivals. If frontline sales teams are being given growth targets of 25 per cent in such markets, it is likely that they will feel a need to 'grease a few wheels'. Aggressive growth and best practice compliance are probably incompatible goals in high-risk markets, and companies need to make clear-eyed decisions as to which is more important.

All too often, the teams that experience the risk are put in highly sensitive situations with little or no local compliance support. Compliance teams sit in head offices, with little visibility of the 'real' risks as they are experienced and an implicit strategy to keep them in the dark. For companies that want to succeed in these markets over the long term, the 'corruption premium' (which could be time or money) needs to be understood and factored into decision-making, targets and individual incentives. Ultimately, the acceptance of more realistic growth plans and planning for operational delays are critical elements of a meaningful response to corruption.

Companies are generally reluctant to embrace the full scope and implications of the corruption risk they face. Executives at global headquarters often have an unrealistic perception of the corruption risks their teams experience on a daily basis, as well as what practices are being employed in remote offices.

For this reason, Control Risks considers that a full and credible corruption risk assessment should include two elements: an objective assessment of the external environment and a thorough investigative approach to weaknesses in process and culture. In particular, it should include confidential interviews across the organization, focused on detecting opportunities to circumvent current checks and balances. A review of financial transactions and audit processes is the best way to locate systemic weakness, but it needs to be guided by intelligence from both inside and outside the organization.

COMMENTS FROM THE FRONTLINE: RICHARD BISTRONG'S PERSPECTIVE

Richard Bistrong spent much of his career as an international sales executive. He currently speaks on foreign bribery and compliance issues from that front-line perspective, writing about them on his blog at www.richardbistrong.com. Richard was vice president of international sales for a large, publicly traded manufacturer of police and military equipment, which entailed residing and working in the U.K. In 2007, as part of a cooperation agreement with the U.S. Department of Justice and a subsequent immunity from prosecution in the U.K., Richard assisted the United States, U.K., and other governments in understanding how FCPA violations, bribery and other misdeeds were occurring in international export sales. Richard's covert cooperation was one of the longest in any white-collar criminal investigation. In 2012, Richard was sentenced as part of his agreement and then served fourteen-and-a-half months at a federal prison camp in the U.S.

Control Risks asked Richard for his perspective on how risk and corruption issues play out in organizations. He offered the following comments:

The current state of compliance often combines idealistic aspirations or poster slogans with tick-the-box rules and procedures that fail to address country-specific risk in the context of global and regional business strategies. A business strategy with aggressive growth targets and lucrative incentive plans speaks to a 'win above all else' mentality, leaving field personnel to ponder: "What does management really want, compliance or sales?"

When anti-bribery compliance is not incorporated in business strategy, and compliance remains one dimensional, corruption risk becomes a containment policy. This is like catching a falling knife after a violation is discovered. Worse, it puts those in the field in harm's way as they come to think of anti-corruption and financial upside (both for individuals and for the company) as a zero-sum game because both cannot be delivered to management.

The strategic dimension of corruption risk is too often ignored, if acknowledged at all, in the 'compliance debate'. As boards, C-Suites and shareholders demand greater returns – and with many areas that have the greatest short-term potential for business growth visibly corrupt and unstable – is anyone trying to reconcile such aggressive strategies in the context of corruption risk? After bold forecasts have been achieved, does anyone ask: "How did we get here?" Or is it all high-fives in the C-Suite and boardrooms?

Since all risks are not created equal, compliance cannot offer a 'one size fits all' model to the teams that face corruption and risk on the front lines of international business. Management needs to address specific country and regional risk when developing business strategies and the incentive packages that flow from those strategies. An individual working in the Andean region of South America should not have the same bonus plan index and growth target as someone who has business responsibility for Scandinavia. Forcing a global business model onto regions that feature significant differences in corruption risk poses great peril to those on the front lines, as well as to those responsible for giving them appropriate, real-world compliance tools.

Currently, the way most organizations structure and treat corruption risk makes meaningful debate around these critical issues impossible, particularly for publicly listed companies. How often do you hear CEOs and CFOs talking about having walked away from markets while they announce profit reductions during investor calls? The combination of earnings pressure, which resets every quarter, and the attraction of new, lucrative, highly corrupt markets morphs the 'clear-eyed decisions' warranted with respect to business strategy.

Now we have the dissemination of language around corporate ethics, culture and anti-bribery compliance, along with the rollout of high sales targets in high-risk markets, with no acknowledgement of inherent contradictions. When incentives, as a function of those financial targets, are then indexed to personal financial performance, compliance and financial success become a zero-sum game. In such situations, compliance becomes 'bonus prevention' and field personnel often take compliance into their own hands exposing themselves and their employers to inevitable corruption risk.

When multinationals start to take a holistic and organizational approach to compliance, they begin to recognize that they need to walk strategy and business plans back in order to move compliance forward. The 'rogue employee' script kept in the top drawer might be useful (even appropriate) when

violations surface, but it never results in an introspective examination of the contradictory messages inherent in corporate strategies and pay plans that were sent to the field.

I often ask how frequently C-Suite and compliance leaders bring personnel in from the field to inquire about the risks they face and to look into the specific challenges presented by each region and territory. (I like to tell compliance teams that "the more upsetting those conversations are, the better they are going" because then they can address what they know.) The application of such realism might be best applied not by the C-Suite, but by risk, audit and governance committees on boards of directors, which might be best-suited to ask: "How are we achieving such aggressive targets in regions that have such a poor reputation for procurement integrity?" Boards should be asking what their companies are doing to help the international teams that face corruption risk head-on.

From my perspective, there is a complete lack of discussion, debate or basic dialog about the behavioral components affecting those on the front lines of international business, potentially causing employees to rationalize bribery. I often revisit my own 'perfect storm' of rationalization, which speaks to the instability of international markets, lucrative incentive compensation, a lack of witnesses and finally, the illusion that bribery is a victimless crime. All of these affected my thinking during my career. While this in no way justifies bribery – there can be no justification for criminal conduct – it at least addresses the rationalizations and temptations that exist among those closest to risk. That realization can be a first step in admitting, "Yes, we have a problem."

CLARIFYING THE ORGANIZATIONAL RESPONSE TO RISK

RESPONSIBLE	Who will actually be mitigating/monitoring/controlling this risk? Who is assigned to work on understanding this risk?
ACCOUNTABLE	Who will be at fault if this goes wrong? Who has the authority to make decisions about managing this risk?
CONSULTED	Who has roles that would give them insight into this risk? Who experiences this risk on a daily basis?
INFORMED	Who needs to know the agreed response to this risk in order to do the job? Who has to be updated on progress in managing this risk?

Once a company has mapped its risk universe, it needs to tackle the organizational response. A responsibility assignment (RACI) matrix (see above) can be used to establish which teams and people are responsible, accountable, consulted and informed about each risk. Ultimate responsibility may continue to lie in the standard risk ownership departments, but employees who experience actual risk need to be assigned a role in this matrix. Cross-functional accountability is also important, particularly for such nebulous areas as political risk.

Organizational analysis can be used to address any gaps in implementing an organization's desired risk management approach. Organizational analysis has five levels: intrapersonal, interpersonal, group as a whole, intergroup and inter-organization. Each can provide a useful lens to examine the effectiveness of the risk-mitigation strategy and implementation. Each level of analysis is independently useful and can provide valid insights into organizational processes[4].

Intrapersonal Risk Management

The intrapersonal level involves understanding how employees are motivated and rewarded and how these incentives are communicated and understood. Suppose employees who work on the front line in high-risk markets receive mandatory annual training on how to manage corruption risk. Is it acceptable for them to walk away from business opportunities that might compromise the integrity of the company? Behavioral metrics are often factored into performance reviews but are rarely given the same weight as commercial indicators of success. In other words, are sales teams merely informed about bribery risk in a pro forma fashion – or when they need to be held accountable?

Key considerations in intrapersonal management of risk include the following:

- The degree to which employees are capable, motivated and qualified to perform their assigned risk management tasks;
- The degree to which employee roles in risk management are built into their defined roles and tasks or are additional or contradictory;
- The degree to which individual incentives focus exclusively on performance or include a meaningful behavioral component. In addition, a focus should be on the metrics of incentive indexes. In other words, is the bonus linked to corporate, divisional or individual performance?
- The degree to which an employee has a sense of individual responsibility in managing a risk;
- The degree to which an employee's wider incentives support or contradict the stated risk management goals;
- The degree to which individual employees understand the company's strategy, mission and risk appetite;
- The degree to which employees are encouraged to be transparent about the risks they face and to communicate concerns to higher levels in the hierarchy.

Interpersonal Risk Management

The interpersonal level involves understanding the relationships and communication among individuals in the organization. Critical areas to examine include the flow of information, the level of conflict and trust and the relationships across the organizational hierarchy. In the risk management context, it is critical to look at the relationships among those who establish the organization's risk strategy and risk appetite, those who experience actual risk and those who are responsible for addressing it.

[4] Wells, L. (1995). The group as a whole: A systematic socioanalytic perspective on interpersonal and group relations. In J. Gillette & M. McCollom, (Eds.), Groups In Context: A New Perspective on Group Dynamics. University Press of America.

Although 'tone at the top' is an overused term, its applicability in the interpersonal context is clear: If a company's espoused beliefs and values emphasize ethical behavior and encourage whistleblowing and other responses to concerns about risk, the basic underlying assumptions must also support these values. All too often, the behavior of senior leaders demonstrates a belief that the company's stated values do not apply to them. Nothing undermines a robust risk culture more quickly than a 'do as I say, not as I do' approach.

Key considerations in interpersonal management of risk include the following:

- The nature of authority in the organization and the degree to which employees are encouraged to communicate risk concerns upward in the hierarchy;
- The nature of top-down communication and whether only information that has a positive slant can be communicated;
- The dominance of particular behavioral norms that encourage 'groupthink' while discouraging diverse perspectives and debate on risk issues;
- The degree to which employees are encouraged to compete for particular rewards vs. cooperating and sharing information;
- The degree to which employees respect internal processes and are rewarded for following them;
- Ultimately, whether employees trust their leaders to 'do the right thing'.

Group Risk Management

Most companies assign ultimate responsibility for risk to a particular group – either to the board and senior executive team or to a designated risk committee. Indeed, the corporate response to large, holistic problems is typically to set up a cross-functional committee and hope this addresses the issue. As experience shows, these groups can be complex and difficult to manage, with physical distance, cultural differences and varying management styles posing barriers to effectiveness. Leadership teams need to work hard at ensuring their departmental interests are represented and at considering the corporation's broader interests. In practice, this is harder than it sounds, particularly because team members are often competing for resources, visibility and power[5]. Business developers believe that without them, the company would collapse. Manufacturers believe that without them, there would be nothing to sell.

The behavior of the risk committee is particularly important because tensions, contradictions and lapses in transparency will trickle down to the rest of the organization. The work of the risk management team is to consider the many, often-competing factors that converge only at the top of the organization and then to work out those dynamics and priorities. A subtle pressure to conform and speak from a big-picture perspective can overwhelm the need to argue aggressively for a given department's interests, which can be regarded as parochial, narrow-minded and inappropriate. Representatives need to be comfortable making a case for the risks and concerns that affect their divisions, or they will become sidelined.

It is the job of the CEO or risk committee leader to focus the discussion and set priorities accordingly. This is an area in which external consultants can bring an objective perspective and challenge embedded norms and blind spots. Ultimately, however, risk management decisions need to be embraced by the company and implanted in its culture.

Key considerations for group discussions of risk include the following:

- Which risk owners speak most often in meetings and have access to the biggest budget and resources;
- Which risks are addressed at the senior level, and do these reflect the concerns and experiences of subordinate employees;
- Whether multidimensional risks are assigned to particular divisions, and what roles accord to other teams affected by a given risk;
- Whether there is a shared understanding of corporate risk appetite, or does debate and conflict stem from fundamentally different concepts as to what level of risk is acceptable;
- Whether there is a diversity of perspective on risk or a narrow concept of what risk means to the organization, and is this reflected in the composition and behavior of the team;
- Whether particular interests or divisions are routinely dismissed, ignored or blamed for wider organizational problems.

[5] Senior Executive Teams: Not What You Think, David N. Berg, Consulting Psychology Journal, Vol 52.

Intergroup Risk Management

Intergroup dynamics are perhaps most important of all in a risk management framework. In order for a holistic risk management approach to be effective, the risk ownership functions need to work closely with the core business in both gathering and sharing insights. However, this will be ineffective if the fundamental concept of risk management remains a policing function – a check and balance on the company's core growth activities. Processes need to be established that make responsibility, accountability, consultation and information requirements clear to the various stakeholders. There is little substitute for communication and debate about specific risks to embed an understanding of how to mitigate the risk across teams.

The degree to which different divisions can maintain responsibility over specific risks while gaining key input from other teams and stakeholders will greatly depend on the nature of group boundaries within the organization. Boundaries act as the 'container' that holds the task the group is addressing while they govern interaction with members outside the group[6]. Boundaries can be temporal, geographic, hierarchical or functional; they can both facilitate and undermine effective risk management and responsiveness. For example, if meetings never start or end on time and lack a clear agenda (they have weak time boundaries), this will signal something important to attendees about the meetings' purpose and effectiveness. If group discussions are open and constructive, but meaningful comment ceases whenever senior executives are present, this may indicate that the group has a strong sense of hierarchical boundaries.

Organizations whose group roles and processes are rigid (groups are "overbounded") will struggle to understand and respond to all dimensions of risk. Organizations that de-emphasize processes and roles (groups are "underbounded") may determine that 'everybody' owns a particular risk and thereby fail to set up accountability. Clayton Alderfer's work on intergroup relations established the following group characteristics[7] (see below):

Clearly, the need for effective risk management relies on boundaries between organizational functions and roles being sufficiently fluid to drive debate and discussion, yet sufficiently clear that people understand the roles and tasks they are being asked to fulfill. Companies may be tempted to eliminate group boundaries entirely and embed risk owners into commercial front-line teams, but this is surprisingly hazardous. Investment banks frequently took this approach prior to the financial crisis and later found that risk managers tended to become 'infected' by the group's culture, losing sight of the oversight role.

PROPERTY	OVERBOUNDED	OPTIMALLY BOUNDED	UNDERBOUNDED
Goals	Single, unitary	Multiple, with established priorities	Little consistency on strategic appetite and overall risk tolerance.
Authority	Hierarchical, monolithic	Negotiated hierarchy with relevant group representation	Several competing authorities without mode of resolution
Roles	Detailed, precise, restrictive	Defined, with opportunities for adjustment	Imprecise, incomplete, conflicting
Leadership transition	Top-down	Accomplished taking account of diverse perspectives	Bottom-up
Communication	Withholding information; positive slant	People meet as needed, speak and listen, provide balanced perspectives	Parties do not meet often, simultaneous talking, information with negative slant
Economic condition	Secure	Dynamic with opportunities and hazards	Insecure

[6] The BART System of Organizational Analysis: Boundaries, Authority, Role and Task, Z. Green and R. Molenkamp
[7] The Five Laws of Embedded Intergroup Relations Theory, Clinton Alderfer, in The Practice of Organizational Diagnosis: Theory and Methods

Key considerations for interactions among groups include the following:

- Whether the purpose of risk management is understood and aligned with the wider purpose and core goals of the organization – is it regarded as a core element of organizational success or an irritating distraction from everyday business;
- How and when information is shared – risk owners need enough time to evaluate a particular risk, as well as comprehensive information about the initiative or transaction;
- Whether risk owners have the resources and budgets they need to fulfill the tasks they are assigned, or are they expected to achieve the impossible;
- Whether risk owners have the ability and motivation to meet regularly, communicate, discuss and share ideas with each other and with the divisions and functions of interest.

Inter-organizational Risk Management

Finally, inter-organizational approaches can be an effective way to share best practice on a range of risk issues. Industry interest groups have been effective in certain areas at driving knowledge-sharing and collective action. This is often seen as the most effective approach to long-term, endemic issues such as demands for facilitation payments. The new compliance landscape – in which regulators tend to pursue companies in the same industry, or those using the same service provider – renders these relationships even more important. All companies in an industry are accountable, but responsibility for this particular agenda often (rightly) sits with the largest and most influential player in the sector.

Companies can manage risks in the wider environment by cooperating with each other and by sharing ideas and best practices. This happens informally in many industries and among risk owners in companies. Such cooperation is a key aspect of knowledge generation, but it must not undermine strategic goals.

On a broader scale, companies will be better placed to manage external risks if they engage with the wider environment and are regularly gathering intelligence and information about developments in the sector, country or region of interest. This requires extending the idea of inter-organizational risk management beyond industry competitors to include think tanks, NGOs, diplomats and political and economic analysts. This is an additional way to ensure that an objective and timely view of the risk landscape can correct organizational prejudices and assumptions.

Key considerations include the following:

- Whether the company regularly engages with industry groups to understand best practice and keep track of developments;
- Whether the company considers political and economic risks that may affect its business, prioritizing and adjusting strategy in response;
- Whether the company interacts in a meaningful way with external stakeholders, including investors, the media, local communities and governments;
- Whether the company gathers information from key customers, suppliers, distributors and partners, feeding it into the risk management process;
- Whether the company conducts regular scenario planning and has crisis management and business continuity built into its approach to new initiatives.

CONCLUSION

Corporate risk management approaches are still at an early stage of evolution. Current approaches to risk management seem inadequate in the face of tectonic shifts in the geopolitical, technological, regulatory and macroeconomic landscape, with information flows too rapid to control. Given all this, companies need to develop the organizational capacity to understand and manage risks – to flex risk management muscles in different ways that address their specific challenges.

The structures that are put in place will vary greatly according to industry, market and an organization's overall risk appetite. Beyond the broad comments herein, it is difficult to generalize as to what will work best for an individual company. Still, a greater emphasis on the organizational dimension of risk management – and how human beings interact with and respond to the risks they face – will always yield benefits. It is time to move on from checks and balances to embrace innovative approaches that can help all employees engage in addressing how risk plays out in their professional lives.

ABOUT THE AUTHOR

ALISON TAYLOR
SENIOR MANAGING DIRECTOR

Alison is based in New York and manages a team of specialist regional investigators located in Los Angeles, New York, Mexico City, Bogotá and São Paulo.

Her areas of expertise include evaluation of client risk exposure and designing enterprise-wide anti-corruption and compliance programs, due diligence, business intelligence, complex political intelligence, country risk analysis and management consulting. Alison's recent experience includes:

- Developing a comprehensive anti-corruption training program for the global corporate headquarters of a large multinational bank.
- Providing comprehensive, predictive strategic consulting, commercial and corruption risk assessments for large companies in all sectors.
- Leading project teams in conducting comprehensive due diligence programs for multiple Fortune 500 extractives clients.
- Conducting sensitive litigation support and business intelligence projects in a variety of high-risk emerging markets across Africa, the Middle East and Latin America.

Alison joined Control Risks in 2003 in London as the director for the Middle East and Africa Corporate Investigations and Compliance team. She was made an Associate Director in the practice in January 2006 and a Director in July 2008 following the rapid growth and expansion of the business. She recently spent eight months working for Transparency International, helping develop an anti-corruption advisory business for corporations.

Prior to joining Control Risks, Alison worked as a journalist, editor and research manager for companies including Law Business Research and the Press Association. Between 1997 and 2003 Alison had a variety of roles. These included working as a corporate strategy consultant for PricewaterhouseCoopers in Chicago, San Francisco and London, specializing in e-commerce strategy, consumer products and retail; and as a country analyst for HIS Global Insight, providing risk assessments, predictive analysis, and economic development forecasts for Sub-Saharan Africa.

She regularly writes and presents on issues relating to corruption, strategy, and risk management in emerging markets.

Alison graduated from Balliol College, Oxford University with a Bachelor of Arts degree in Modern History, and also holds a Master of Arts degree in International Relations from the University of Chicago, specializing in economic development policy in emerging markets. Alison is a Certified Anti-Money Laundering Specialist (CAMS) and has a working knowledge of French and Hindi.

Control Risks' offices

abudhabi@controlrisks.com
alkhobar@controlrisks.com
amsterdam@controlrisks.com
baghdad@controlrisks.com
basra@controlrisks.com
beijing@controlrisks.com
berlin@controlrisks.com
bogota@controlrisks.com
chicago@controlrisks.com
copenhagen@controlrisks.com
delhi@controlrisks.com
dubai@controlrisks.com
erbil@controlrisks.com
hongkong@controlrisks.com
houston@controlrisks.com
islamabad@controlrisks.com
jakarta@controlrisks.com
johannesburg@controlrisks.com
lagos@controlrisks.com
london@controlrisks.com
losangeles@controlrisks.com
mexicocity@controlrisks.com
moscow@controlrisks.com
mumbai@controlrisks.com
nairobi@controlrisks.com
newyork@controlrisks.com
panamacity@controlrisks.com
paris@controlrisks.com
portharcourt@controlrisks.com
saopaulo@controlrisks.com
seoul@controlrisks.com
shanghai@controlrisks.com
singapore@controlrisks.com
sydney@controlrisks.com
tokyo@controlrisks.com
washington@controlrisks.com

www.controlrisks.com