Deloitte.

Winning the away game

Strategies to enhance compliance and business performance in emerging markets

Winning the away game

Strategies to enhance compliance and business performance in emerging markets

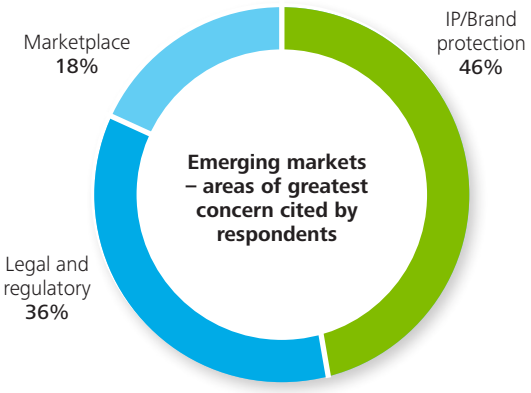
Executive summary

It is well established that emerging markets[1] provide a wide range of opportunities for growth-oriented technology companies. Operating in these high-growth emerging markets, however, has its challenges. In reaching customers, technology companies often rely on third parties, such as distributors, resellers, system integrators and other partners—and for good reason. These partners offer a host of potential benefits, such as established networks, expertise, scalability and flexibility. But working with third parties in countries where the legal environment may be at best unfamiliar, or at worst ineffectual, can expose a company to substantial risks. Additionally, attitudes toward compliance in emerging markets vary considerably, ranging from apathy to blatant disregard for compliance. Companies often do not fully comprehend how these attitudes and legal structures differ from those of their home countries and the compliance risks to which they are being exposed.

To better understand the importance of emerging markets to the IT industry, as well as the challenges of operating within them, Deloitte[2] and the Alliance for Gray Market and Counterfeit Abatement (AGMA®) conducted a survey in 2015 of leading multinational technology companies. The respondents to this survey represented a cross-section of companies of various sizes, each with its own unique vantage point and perspective regarding emerging markets.

The research found that intellectual property (IP)/brand protection risk and legal and regulatory risk are "most concerning," cited by 46% and 36% of respondents respectively. Furthermore, within the IP/brand protection risk domain, 45% of executives ranked "insufficient local regulation to protect their intellectual property" as their top challenge. Meanwhile, within the legal and regulatory realm, 45% worry most about corruption or other non-standard business practices causing them to run afoul of regulations, such as the US Foreign Corrupt Practices Act (FCPA) or the UK Bribery Act, which can lead to substantial fines and reputational damage.

Based on Deloitte's experience serving many of the industry's top technology companies, as well as the first-hand experience of AGMA members, this report seeks to provide insight into frameworks and leading practices for detecting, preventing, and reducing IP/brand protection and legal and regulatory risks in emerging economies.



From BRICs to MINTs, opportunities abound

Despite ongoing investments in the BRIC (Brazil, Russia, India, and China) nations from a market perspective, some believe the MINT countries (Mexico, Indonesia, Nigeria, and Turkey) will be the ones to watch for the next 10 years. The MINTs are united by youthful populations, advantageous geographic placement, and with the exception of Turkey, commodity production.[3] As in the BRICs, much of the future spending in the MINTs will likely be allocated to IT.

The opportunities within the BRICs, MINTs, and other emerging markets were underscored by many of the survey respondents. As expected, approximately 60% of survey participants named China, Russia, India, and Brazil as among the top five developing countries by revenue that they currently sell into. Several more mentioned the MINTs. The United Arab Emirates was also a popular response, while Oman, Poland, Saudi Arabia, Singapore, South Africa, Taiwan, and Vietnam rounded out the list. Respondents further indicated they derive a significant amount of revenue from these markets, with the majority reporting they derive between 10 and 50 percent of their revenue from emerging economies. Of note, over 15% of respondents said their companies look to emerging markets for more than 50% of their revenue.

The reasons for the intense focus on IT within developing economies are many. Technology can play key roles in enhancing the socioeconomic status of the citizens within emerging countries, and these nations often have the advantage of being able to leapfrog adoption of legacy infrastructures. For instance, India, China, South Africa and several other nations adopted wireless telephony much faster than developed markets since they could bypass landlines.

> "My guidance would be if you're going to be doing business in emerging markets you have to devote the infrastructure to successfully manage it—and, having a systematic approach to how you deal with that is very important."
>
> – Brad Minnis, Juniper Networks

Advantages and challenges of engaging third parties in emerging markets

Responses to the survey, macroeconomic data, and trends all suggest emerging markets offer a significant opportunity for growth-oriented technology companies. In some cases, leading companies are pursuing these opportunities by establishing a direct presence in these markets in the form of sales offices and manufacturing operations, or more commonly, by leveraging third parties, such as contract manufacturers, distributors, resellers, managed service providers, and other channel partners. Companies often decide to engage third parties in emerging markets because it represents the path of least resistance. It gives them a way to scale quickly, as well as to save time and money by eliminating the need to invest in warehouse space, technology, transportation, and training.

There is also no substitute for having ready access to a resource network that is up to speed on local customs and business practices. But, engaging third parties in developing markets also exposes companies to heightened risks since these outside vendors have access to the crown jewels: the company's latest and most coveted intellectual property. Despite this level of access, less than half of respondents to a previous Deloitte & Touche LLP survey said their companies always conduct due diligence in emerging markets before engaging a new vendor (43%) or before engaging a new third-party agent (49%).[4]

The reality is that companies risk theft of intellectual property any time they engage a third-party, whether that entity is in an emerging market or not. However, since developing markets are often far away from corporate headquarters, lack of visibility is inherent. Add histories of corruption and insufficient legal structures into the mix, and a perfect storm of risk begins to brew. A recent list of the 10 worst countries in which to do business compiled by CNBC News not surprisingly featured many of the BRIC and MINT countries, which also offer the greatest opportunities for IT growth.[5] Brazil, for example, made the list due to corruption, with government kickbacks being commonly viewed by unethical politicians as the price of admission to the market.[6] India also made the list as it is one of the hardest countries in the world in which to enforce contracts, often taking years for disputes to work their way through the courts.[7]

The risk exposure associated with many of these high-growth markets is alarming, considering the extent to which technology companies transfer IP to partners in developing economies. Indeed, more than half (55%) of the survey respondents say they transfer a "significant" amount of intellectual property to their partners in emerging markets. For those with weak compliance programs, this leaves the door wide open for abuse. Take the practice of contract manufacturing for example, which is prevalent within the technology industry. Contract manufacturing directly puts the proprietary intangible assets of original equipment manufacturers (OEMs) into play and the risk is exacerbated since contract manufacturers often work simultaneously with multiple competing clients in order to operate economies of scale, thus increasing competition. For instance, a contract manufacturer's plant in Mexico can assemble a device to connect TV sets to the Internet for Royal Philips Electronics at very low per-unit costs, because it is simultaneously producing a similar device for Sony on an adjacent production line.[8]

An unscrupulous contract manufacturer can exploit the knowledge it acquires in the course of working for a given OEM for its own benefit, or it can transfer this knowledge to other clients. This leakage may happen even if the contract manufacturer only assembles components made by others, and today it can occur at lightening speed. Via three-dimensional scanning and computer-aided design and manufacturing, companies can copy in a matter of hours components that may have taken years to design, escalating the potential for abuse. CFM International, for example, a joint venture of General Electric and French manufacturer SNECMA, which makes parts for aircraft engines, was forced to take legal action to stem the spread of counterfeit parts within repair and overhaul shops in the United States.[9]

The increasing frequency of cases such as this, along with counterfeiters' heightened ability to "knock off" components in the blink of an eye, are good reasons why IP/brand protection ranked as the number one concern among survey participants. Forty-six percent of respondents said it was their top concern, while 27% ranked it second.

Forty-six percent of respondents ranked "insufficient regulation" as their most important concern relating to IP/brand protection, and 27% cited as their top worry a "lack of commitment by local government/law enforcement to take meaningful action on IP infringements/abuses."

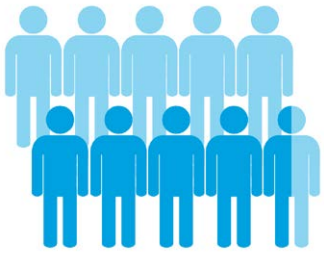
Beyond IP/brand protection, the next biggest area of concern for survey participants is legal and regulatory risk. Thirty-six percent rated this area as "most concerning" to them, and within this realm, they specifically pointed to government corruption as their most disquieting worry. In Deloitte's experience, this worry is typically rooted in the far-reaching implications of, and the penalties associated with, the FCPA and the UK Bribery Act. The FCPA, for instance, prohibits the payment of bribes to foreign officials to assist in obtaining or retaining business. It also requires issuers to maintain accurate books and records and "have a system of internal controls sufficient to, among other things, provide reasonable assurances that transactions are executed and assets are accessed and accounted for in accordance with management's authorization."[10]

The FCPA can apply to prohibited conduct anywhere in the world and extends to publicly traded companies and their officers, directors, employees, stockholders, and agents. Importantly, "agents" can include third parties acting on the company's behalf, such as consultants, distributors, joint-venture partners and others.[11] Sanctions can be significant. A number of multinational companies have been the subject of FCPA violations leveled by the SEC in recent years. These violations have resulted in multi-million dollar fines.

The UK Bribery Act has similar reach and equally acute penalties. Companies registered in the UK must remain cognizant of the extra-territorial scope of the Bribery Act. A company can violate the Act if it fails to prevent associated persons (e.g., employees, subsidiaries, agents or service providers) from bribing another person anywhere in the world to obtain or retain business or a business advantage.[12] Indeed, a foreign subsidiary of a UK company can cause the parent company to become liable under Section 7, or the "failing to prevent bribery" provision, when the subsidiary commits an act of bribery in the context of performing services for the UK parent.[13]

As with the US FCPA, companies must make sure they have strong, up-to-date and effective anti-bribery policies and systems in order to avoid corporate liability for bribery under the UK Bribery Act.[14] Here too, the penalties have teeth: companies can face unlimited fines for violating the Act, while individuals can face up to 10 years in prison as well as unlimited fines.[15]

Challenges in seeing, and subsequently controlling, the actions that "associated persons" are taking on the company's behalf thousands of miles away is one reason why companies rate bribery so high on the list of risks when doing business in emerging markets. The severity of the penalties is another. In Deloitte's experience, this worry is typically rooted in the far-reaching implications of, and the penalties associated with, FCPA and the UK Bribery Act. Nearly two-thirds (64%) say they either don't require partners to provide them with evidence that they have FCPA and/or export compliance policies and procedures in place, or they technically require such evidence but they do not check that the processes are being followed.



45%

of respondents believe that their partners in developing markets are not fully aware of the responsibilities under legislation that their companies must adhere to.

Based on Deloitte field experience, working with third parties in emerging markets raises even more issues than these. Additional challenges include sales to embargoed nations, especially via third parties in the Middle East, as well as an intentional overproduction of goods to be sold through back channels. Our teams have also observed challenges in the area of special pricing, where channel partners have abused discounting structures to increase margins or establish slush funds, rather than to facilitate transactions with downstream customers. Through their work with distributors and resellers, our teams have additionally observed cases where channel partners have bulk-ordered for multiple customers and then presented the transaction as a single order to obtain a larger discount from the vendor. The bulk orders are then decoupled and sold to multiple end users at a higher margin. In this grey market scenario, technology companies lose visibility into the disposition of their products. This increases the likelihood that their products will ultimately end up with brokers or in embargoed nations if deals fall through.

The shared roots of risk

In our view, the risks of intellectual property theft and of legal and regulatory non-compliance in emerging markets share the same roots. The first is lack of, or an under awareness of, contractual obligations and far-reaching laws and regulations. The survey results suggest that third parties are not generally aware of their legal responsibilities in an international context and, even when they are, they are not consistently concentrated on compliance. For instance, 45% of respondents believe that their partners in developing markets are not fully aware of their responsibilities under legislation that their companies must adhere to, and 64% indicated that even if their partners are aware, they do not always show a strong focus on compliance. Based on Deloitte experience, even the most mature organizations in emerging markets have shown an unwillingness to invest in infrastructure to employ control mechanisms in areas such as FCPA and export compliance.

Many emerging market risks related to IP/brand protection and legal and regulatory non-compliance additionally stem from government non-cooperation, in the form of outright corruption in extreme cases, or lack of transparency more commonly. For instance, secrecy/data protection acts in some nations prevent parent companies from seeing pricing information, which can lead to abuse of special pricing deals, lost margin, and inequitable treatment of customers. Visibility into end users and the final disposition of products is often similarly blocked. This can fuel grey market activity as well as heighten the risk of inadvertently delivering products to embargoed countries. While blatant expectations of inappropriate payments to gain market access are waning, many governments do, however, still require a significant portion of sales to state-owned entities to be transacted through authorized purchasing vehicles—a practice designed to guarantee the best pricing for government end users. This can result in excessive discounting, and even worse, lead to the creation of slush funds to be used for inappropriate payments.

Even in the best-case scenario where governments do not ask anything untoward of market participants, they often heighten risks for international businesses in other ways. In our experience, weak regulation and lack of enforcement intertwine as the third shared root of IP/brand protection and regulatory risk in emerging markets. Survey participants indeed are concerned about both insufficient regulation and a poor appetite for enforcing whatever regulation exists. Forty-five percent of respondents ranked "insufficient regulation" as their most important concern relating to IP/brand protection, and 27% cited as their top worry a "lack of commitment by local government/ law enforcement to take meaningful action on IP infringements/abuses."

Are companies doing enough?

The survey results highlighted several emerging market risks that keep executives up at night. The results, however, go beyond illuminating the challenges associated with emerging markets to shed light on what technology companies are doing about them. In general, the survey findings suggest businesses may not be doing enough, especially since these risks may not only lead to additional expenses in terms of fines and legal fees but also to lost revenue and under-performance in markets that are key to a company's overall growth strategy.

Consider the following:

- When asked if their companies adjust their compliance activities in developing markets to mitigate risks in those countries, about half of the survey respondents were either unsure or answered "no."

- As with established markets, companies often allocate compliance budgets to developing markets according to the revenue derived from them. The concern here, as well as with the aforementioned finding, is that companies may not be giving developing markets the extra attention they require.

- Less than 30% of respondents say they provide regular compliance-related training to partners throughout the engagement lifecycle. This seems insufficient considering the revenue at stake and that 45% of respondents believe their partners are at least somewhat unaware of their responsibilities under legislation to which the company must adhere (i.e., US, EU, or UK regulation).

Companies also do not appear to be performing sufficient due diligence when establishing relationships with third parties or individuals at third parties. In recent years, the US Department of Justice (DOJ) has fined senior officials at companies for approving third-party agent documentation containing falsified statements, such as the agent's place of business and number of employees. It was noted, during DOJ enforcement action, that company officials failed to undertake any independent review or ask questions regarding the action. In another situation, the DOJ faulted a company for failing to identify red flags when hiring a consultant for work in Honduras. The company had failed to establish requirements for the provision of information regarding conflicts of interest or relationships with government officials.

This is not to imply that technology companies are not taking action. They are. Survey respondents report employing several common techniques to gain visibility into the distribution of products, such as leveraging point-of-sale reports (91%) and performing partner inspections (64%). However, the study findings suggest technology companies may need to do more overall, and they may not be orchestrating their efforts in a structured manner that supports a pervasive culture of compliance.

The need for an integrated approach

Although survey respondents flagged certain risks as "most concerning," all risks are interconnected. We often see risk management programs focused on addressing marketplace and operational risks.

These reactive approaches to third-party management are largely ineffective in mitigating the critical risks associated with engaging partners in developing markets since they often focus on catching past issues rather than preventing new problems, and also are honed in on risks that are "transactional" in nature.

As a result, they may not do enough to help companies reap the benefits they anticipated when they initially entered into these relationships (i.e., growth, innovation, reduced costs, improved customer experience, etc.).

In relation to third-party interactions, Deloitte Consulting LLP's 2014 Global Outsourcing and Insourcing survey underscored the need for an integrated approach to third-party management. It explored companies' satisfaction with their outsourced third-party service providers, many of which are located in developing markets. The survey found that 37% of respondents are facing issues with vendors lacking motivation, and nearly half (48%) are facing issues with vendors delivering poor perceived service quality. What can companies do in emerging markets not only to ensure third-party compliance but also to generate and/or recapture value within their partner networks? In our view, the answer lies in "cultivating a culture of compliance."

Keys to cultivating a culture of compliance

A robust, mature internal compliance framework is typically required in order to cultivate a culture of compliance. This framework enables the company to take an integrated, proactive approach to the selection and management of third parties as opposed to a reactive one. It seeks to do this through internal controls, frequent communication, and ongoing training so that partners are aware of compliance and performance expectations, and that red flags, if raised at all, are noticed before violations are incurred and performance degrades. The objective is not simply to avoid penalties but more broadly to create value through risk management. A culture of compliance can produce a wide range of savings and improvement opportunities in the areas of operations, strategy, reputation and finance:

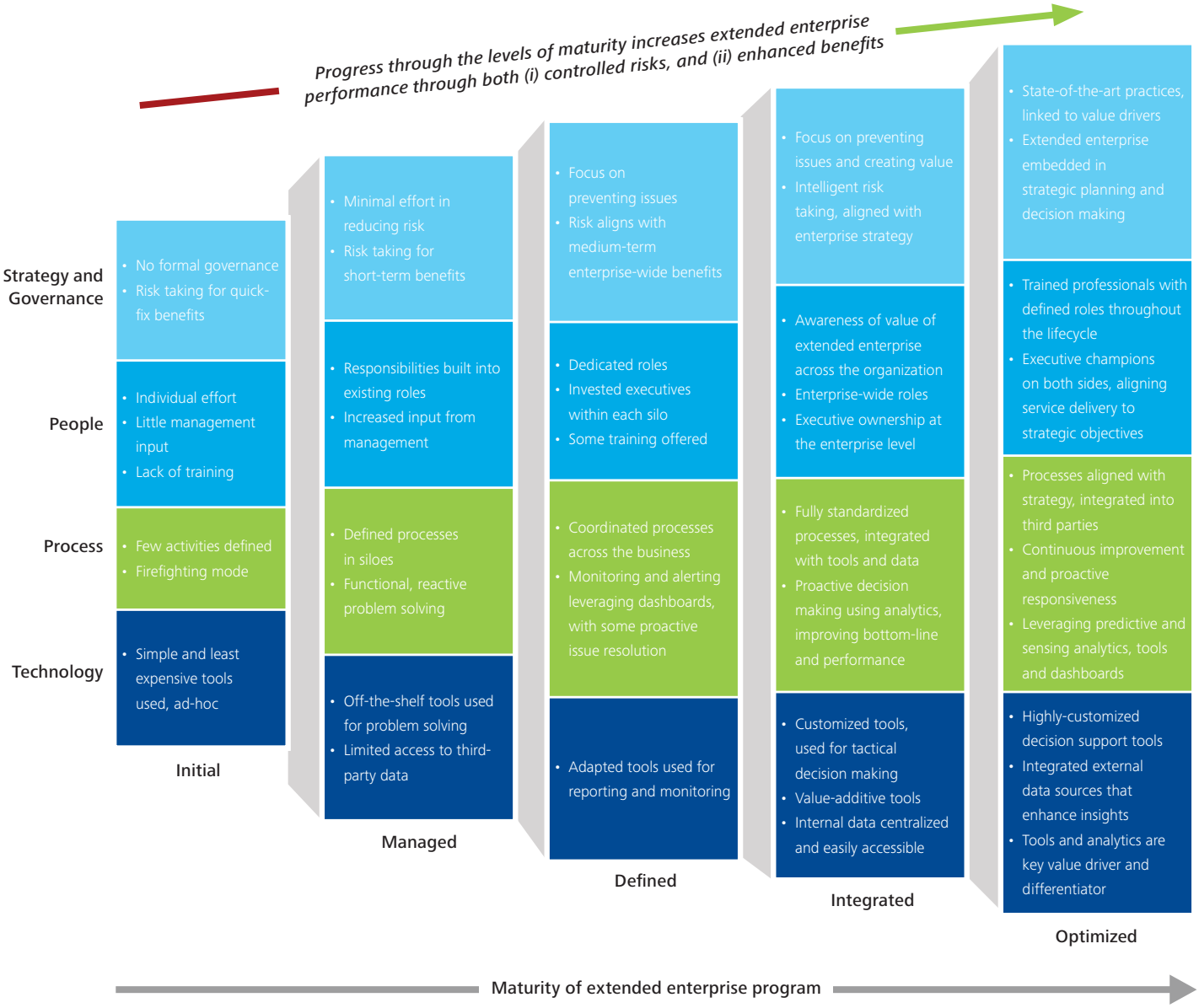
- **Operations:** As employees spend less time tending to ongoing crises, they can focus on adding value to the business.
- **Strategy:** Greater insight into emerging market territories makes decision-making easier, more effective and more impactful.
- **Reputation:** Brand image, customer confidence and relationships are enhanced via compliance and transparency.
- **Finance:** Cash savings can be generated from reduced legal fees and regulatory fines, as well as from decreased grey market activity, since incentives can be more appropriately applied.

"Despite cultural differences and challenges in obtaining compliance, emerging markets represent the biggest business opportunity for many high-tech companies in the current market economy. As such, they cannot be ignored. This puts the onus on participating businesses to educate their partners in emerging markets about applicable regulations and to elevate awareness regarding compliance expectations."

– Sally Nguyen, AGMA President

How does your approach stack up?

The maturity model below outlines progressive levels of advancement across the main attributes of a robust internal compliance framework (i.e., governance, people, process and technology).



The path forward

Regardless of where your organization stands now, there are several leading practices that can help companies mitigate IP/brand protection and legal and regulatory risks as well as increase the likelihood of improving the returns on emerging market operations.

Put boots on the ground

64% of survey respondents said they employ dedicated compliance personnel in developing markets. Having dedicated compliance personnel in each country is likely impractical and cost prohibitive, but there are approaches to maintain a local presence.

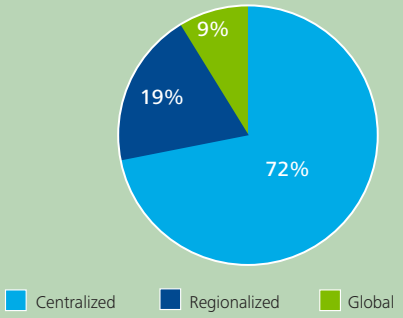
For example, certain compliance activities can be taken on by local staff in country. Dedicated compliance personnel can perform regular visits to (i) perform other compliance activities that are centrally managed, (ii) check in with local staff to ensure that local compliance activities are being performed, and (iii) touch base with key partners to communicate and educate.

It is important to avoid the common pitfall of locating compliance personnel operating exclusively in regional service centers, or only in areas where it is inexpensive to house teams. Having some presence is paramount, even in places that are geographically dispersed or where the costs may be higher.

Establish a strong central organization

A strong central organization is essential for ensuring that rules are applied consistently and for preventing local teams from going rogue. Centrally managed activities might include development and execution of a risk assessment framework, creation of policies and procedures, and overall management of compliance activities. We often find strong reasons to tweak compliance policies and procedures to fit local needs, but this ought to be managed centrally and not left up to the territories to "set their own rules."

How survey respondents have structured their compliance organizations



Increase the number of touch points with partners

Companies need to help their partners understand the nature of the business and why certain systems are in place, rather than merely demanding that people "work with them."

This may mean spending time, money and even doing some fieldwork to better understand the local culture, and how people perceive their responsibilities related to performance, regulatory compliance and information security. The survey revealed that respondents are often unaware of regulations with which they need to comply. This implies that more frequent communication is needed—possibly in the form of holding meetings with regional legal teams and key partners to review relevant regulations and identify process changes, as necessary; conveying the notion that channel partners are expected to push knowledge of regulations downstream; and making legal information and compliance expectations easily accessible to third parties via a partner portal.

Retain focus on corruption and fraud in parallel with a wider compliance program

A strong internal controls environment is often perceived to be the best defense against corruption and fraud. This environment should support the execution of three basic tactics as part of a broader compliance program:

- Develop internal controls and monitor compliance with them
- Perform due diligence prior to engaging third parties in emerging markets in addition to conducting periodic reviews of existing vendors
- Look for red flags such as deviations in order patterns, incomplete documentation, avoidant communication, illogical product configurations, large deals that emerge suddenly or with little or no lead time, or unwillingness to provide visibility into end customers

To maximize its effectiveness, the broader program should include a formal anti-fraud policy that is communicated regularly to employees, partners and suppliers around the world.

"In our experience, companies often take expectations of compliance for granted, i.e., 'the rules are the rules'; so their channel partners in emerging markets, or elsewhere, will automatically follow them. But, rules and regulations are meaningless if third parties don't understand or respect them due to cultural differences. That's why a systematic approach to communication, monitoring and due diligence—or creating a culture of compliance—is so important."

– Jana Arbanas, Deloitte Advisory Partner, Deloitte & Touche LLP

Invest in the right people

Compliance professionals who are responsible for risk management in emerging markets require specialized skills. When asked what attributes should be required for compliance professionals in developing markets:

82% of survey respondents identified knowledge of the local business and legal landscape

73% underscored the need for local language skills and familiarity with the local business culture

27% indicated a need for audit experience

Additional responses from survey respondents included the ability to sell the business benefits of compliance, integrity and analytical skills.

Leverage technology and tools

While companies are at varying stages of maturity in terms of their technology environments, they will generally want to progress toward tools that enable real-time monitoring and predictive analysis for certain high-risk activities.

They will also want to make it easier for third parties to understand performance expectations as well as to provide feedback on how well certain processes are working.

Partner portals, mobile apps, and analytics solutions can be helpful in sharing insights with partners and in establishing a mutually beneficial feedback loop.

Call to action

The business case for operating within emerging markets is well documented, yet some technology companies have yet to reap the full range of benefits they anticipated when they made the decision to go there. Others may be sitting on the sidelines because they are unsure if selling into emerging markets is worth the risk. With the economic growth in developing markets outpacing opportunities within the developed world, technology companies may soon be compelled to act in order to improve the operations they already have abroad and/or to pursue growth beyond their established territories.

In either case, developing a culture of compliance by implementing a broad risk-management program will almost certainly be central to the success of their efforts. The benefits of such a program are automatically associated with preventing damages that "cost the company" in terms of fines, legal fees, brand erosion, and lost opportunities. However, this perception is incomplete.

A culture of compliance is equally essential for achieving benefits related to profitability and performance, many of which companies expected to gain when they made their decision to enter emerging markets in the first place. These benefits may include revenue growth, supply chain efficiency, improved customer experience, enhanced brand image, increased working capital, and recovery of underreported sell-side revenue, among others. It is the combination of damage prevention and revenue optimization that makes the case for cultivating a culture of compliance so compelling, and it is why many technology companies need to do more to develop one.

About the survey

Deloitte, in conjunction with AGMA, has completed its second survey to provide insights into the challenges associated with operating in emerging markets and leading practices for detecting, preventing, and reducing IP/brand protection and legal and regulatory risks therein. It is based on online interviews with business decision-makers at leading multinational technology companies.

Contacts

Jana Arbanas
Principal
Deloitte Advisory
Deloitte & Touche LLP
+1 415 783 4523
jarbanas@deloitte.com

Munir Qassim Moon
Manager
Deloitte Advisory
Deloitte & Touche LLP
+ 1 415 783 6204
munmoon@deloitte.com

Sunil Gopal
Senior Manager
Deloitte Advisory
Deloitte & Touche LLP
+1 408 704 4023
sungopal@deloitte.com

Endnotes

1 For purposes of this paper, the term "emerging markets" generally refers to countries outside the US, Canada, Western Europe, Australia, New Zealand and Japan.

2 As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

3 Wright, Chris. "After the BRICs are the MINTs, but Can You Make Any Money from Them?" Forbes, January 6, 2014, http://www.forbes.com/sites/chriswright/2014/01/06/after-the-brics-the-mints-catchy-acronym-but-can-you-make-any-money-from-it/

4 "Look Before You Leap: Navigating Risks in Emerging Markets," Deloitte Financial Advisory Services LLP, 2012, pg. 2.

5 "The World's 10 Worst Countries for Business," CNBC, http://www.cnbc.com/id/45128939/page/1, accessed May 30, 2015.

6 Ibid.

7 Ibid.

8 Arruñada, Benito and Vázquez, Xosé. "When Your Contract Manufacturer Becomes Your Competitor," Harvard Business Review, September 2006, https://hbr.org/2006/09/when-your-contract-manufacturer-becomes-your-competitor.

9 Ibid.

10 "Spotlight on U.S. Foreign Corrupt Practices Act," U.S. Securities and Exchange Commission, https://www.sec.gov/spotlight/fcpa.shtml, accessed June 1, 2015.

11 Ibid.

12 "The Bribery Act," Transparency International UK, http://www.transparency.org.uk/our-work/business-integrity/bribery-act, accessed May 26, 2015.

13 Ibid.

14 Ibid.

15 "Bribery: What is it and what's the penalty?" BBC News, http://www.bbc.com/news/business-13977221, May 28, 2014.