

Insights on
governance, risk
and compliance

June 2014

Step up to the challenge

Helping Internal Audit keep pace
with a volatile risk landscape



EY

Building a better
working world



Contents

| | |
|--------------------------------------|----|
| Introduction | 1 |
| The new imperatives | 2 |
| Targeting risks that matter | 5 |
| Social media | 6 |
| Mobile computing | 8 |
| Cloud computing | 10 |
| Cybersecurity | 12 |
| Third-party risk management | 14 |
| Anti-corruption | 16 |
| Business continuity management | 18 |

Introduction

Today, change is coming faster than ever before – and there's more of it. The sheer velocity of change has upended the business environment and rearranged the landscape. Organizations around the world aren't working to get ahead of the curve; they're struggling to keep up – and often not succeeding.

The volatility is claiming big names as well as small. A recent study of the average company life span on the Standard & Poor's 500 index offered startling proof – a company on the index in 1958 could expect to stay there for 61 years; today, a company can expect to stay on the index for just 18 years.¹

With technology and the world economy changing at an accelerating pace, organizations need to adapt swiftly and efficiently. Many businesses face increasing levels of risk due to expanding operations in emerging markets and developing countries. Meanwhile, regulatory requirements are escalating and the intertwined forces of globalization and advances in technology are creating new opportunities, but also new risks.

This volatility and velocity have had a profound impact on the Internal Audit (IA) function. IA must balance priorities and resources to help the organization address the risks it faces today, anticipate emerging risks and stay in the game. The challenge is significant, and so is the payoff – the IA function that successfully adapts to today's rapidly changing world will become a trusted advisor to an organization poised for growth.

To start, the IA function must maintain a laser focus on basic and core activities, but it must also be ready to take on more of an advisory role. And it must be able to “look around the corner” to see tomorrow's risks today.

In the pages that follow, we'll discuss some of the emerging risks that organizations are most likely to face, including those that could impact existing processes – and what your IA function can do to address those risks.

The challenge for Internal Audit is significant, and so is the payoff – the IA function that successfully adapts to today's rapidly changing world will become a trusted advisor to an organization poised for growth.

1. Antonio Regalado, “Technology Is Wiping Out Companies Faster than Ever,” *MIT Technology Review*, 10 September 2013, accessed at <http://www.technologyreview.com/view/519226/technology-is-wiping-out-companies-faster-than-ever/>.

The new imperatives

IA to do list

- ✓ Employ a dynamic risk assessment and flexible audit plan
- ✓ Include management input and directly link to company's strategy and enterprise risk management program
- ✓ Embed data analytics throughout the entire audit cycle
- ✓ Identify redundant or ineffective controls and recommend enhancements and cost savings
- ✓ Perform advisory projects that proactively address control design and process efficiency and effectiveness
- ✓ Facilitate an enterprise-wide assurance map
- ✓ Coordinate the nature, objectives, scope and timing of reporting to the Board and executive management with other risk management, assurance and compliance functions
- ✓ Leverage the work of other assurance and compliance functions

Today, IA must be more vigilant and diligent than ever before.

The reality is that a control environment that is strong today can be compromised tomorrow. For example, increasingly common policies, such as “bring your own device,” bring new risks. To avoid being placed at a competitive disadvantage, organizations must adjust their processes and controls accordingly.

So a flexible and dynamic risk assessment and internal audit plan, once aspirations, are now imperatives. But organizations are increasingly asking for even more. They’re calling for their IA function to take on more of an advisory role in taking a proactive look at the design of controls in areas, such as system development, new product development and strategic transactions.

The risk assessment should be enterprise-wide. It should include management participation and a direct link to the organization's overall strategy and enterprise risk management program. The audit plan results should be refreshed quarterly, as well as when a triggering event (e.g., merger, new product launch, litigation) occurs. Leading organizations are developing a rolling “3+9” plan – a three-month fixed window and a nine-month fluid plan.

The risk assessment also should be comprehensive, looking beyond silos to identify internal and external changes, such as new arrangements with third parties, new regulatory requirements and new technologies, that could affect key existing processes. As part of a comprehensive approach, the organization should also review its processes and controls around social media, mobile computing, cloud computing, cybersecurity, third-party risks, anti-corruption and business continuity management.

A complex reality

Here are examples of how the borders between risks, and between organizational responses, can become blurred:

Social media is no longer an emerging risk; it's here. Your customers use it – and so do your employees. An irate, social media-savvy customer can do rapid, widespread damage to your organization's reputation – and an employee who inadvertently leaks confidential information via social media can cause far more substantial damage to the organization itself.

Meanwhile, companies are demanding that employees be more productive: having a robust **mobile computing** program that allows personal devices to be used safely in a work capacity can raise employee productivity. An employee IT ownership model, typically called bring your own device (BYOD), presents an attractive option. With personal devices now being used to access corporate email, calendars, applications and data, many organizations are struggling with how to fully define the impact to their security posture.



Many organizations are also looking to **cloud computing** to increase the effectiveness of IT initiatives, reduce cost of in-house operations, increase operational flexibility, and generate a competitive advantage. However, like most technology changes, cloud computing presents its share of risks and challenges, which are too often overlooked or not fully understood by businesses that are quick to embrace it. Implementing cloud computing requires a considerable shift from traditional computing methods and business processes.

The addition of new technologies and the impact of these changes to the IT environment further complicates the **cybersecurity** landscape. Organizations have learned, to their literal cost, that cyberspace presents perils as well as opportunities. The digitalization of commerce – in particular, of payment systems – has proven fertile ground for hackers; hardly a month goes by without a headline involving a major retailer and a data breach. Such attacks can inflict considerable damage not only to reputation but also to the bottom line. Other organizations, including government agencies, are also tempting targets.

Leading organizations know it's best to assume that unauthorized users already have access to their systems – that "they're in." They know that revisiting the cybersecurity risk landscape is a must – again, not only regularly but also when a triggering event occurs, such as signing a contract with a new **third-party** vendor.

Many organizations have outsourced some of their activities or processes, from customer call centers to payroll functions. But companies cannot outsource the associated risks; they retain responsibility, and when the third party further subcontracts the work, the risks grow. To manage the risk, companies must make sure that policies at third parties meet their own standards.

This has become especially important because many third-party contracts involve companies based in emerging markets. In some of these countries, **corruption** is a known and significant risk. A regular, ongoing review of third-party activities is a must to make sure your organization is in compliance with US Foreign Corrupt Practices Act (FCPA) regulations, as well as similar legislation in other jurisdictions, such as the UK Bribery Act.

All of these risks can lead to events that significantly disrupt an organization's operations – such as the recent spate of data breaches at major retailers. These breaches have put the retailers' crisis management skills to the test – and highlighted the need for **business continuity management** plans. Leading organizations know it's prudent to prepare for the worst-case scenario – a natural or man-made disaster, or a lesser event that disrupts the organization's activities in whole or in part. A global economy brings global risks.

A strike in France or a hurricane along the US Gulf Coast can impact an organization's operations all over the world. Your business continuity plan needs to reflect not only the scope of the organization's operations, but also the velocity and volatility of the business landscape.

Why EY?

We have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

As the leading provider of internal audit services, we work closely with our clients of all sizes and across all sectors and bring our knowledge and experience to every engagement.

We invest heavily in our people, methodology and technology in support of our commitment to quality. We innovate by utilizing tools and enablers such as embedded data analytics and controls optimization in our work to provide the most efficient and cost effective internal audits.

Our global internal audit methodology features:

- ▶ A proven, consistent global approach, enabled by technology
- ▶ A focus on higher-risk issues with integrated subject matter resources
- ▶ Governance and execution protocols with the rigor to drive change
- ▶ An emphasis on flexible risk assessment and on continuous communication
- ▶ Key performance indicators that drive accountability and performance



Targeting risks that matter

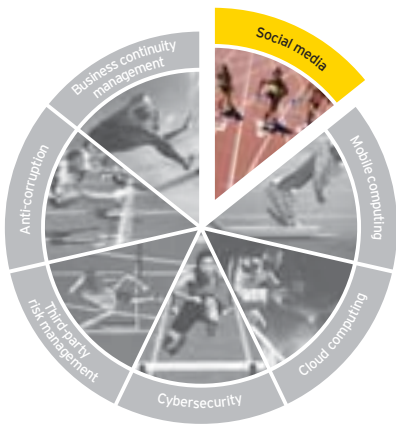
IA needs to adopt a broad, balanced approach. It needs to identify and focus on the risks that matter. Here are seven areas that are not only top of mind for stakeholders, but also deal with key processes that, if not controlled properly, could have a significant negative impact on your organization:

- ▶ Social media
- ▶ Mobile computing
- ▶ Cloud computing
- ▶ Cybersecurity
- ▶ Third-party risk management
- ▶ Anti-corruption
- ▶ Business continuity management

For each topic we present the context, discuss audits that make an impact and present questions for the organization to consider. We also offer suggestions for further reading.

Each of the audits requires a solid understanding of the Institute of Internal Auditors (IIA) standards and the organization's IA approach; an understanding of the organization's strategic objectives and business activities; strong, up-to-date technical IT and regulatory knowledge; strong analytical skills; and the ability to communicate clearly and concisely.





Social media

72% of online adults use social networking sites (and every site could potentially have a negative impact on a business's brand).

Source: Pew Research Center's Internet & American Life Project, August 2013.

Twitter reports
500 million
global tweets per day.

Source: Richard Holt, "Twitter in Numbers," Telegraph, 21 March 2013.

LinkedIn reports more than
259 million
members around the world.

Source: Richard Holt, "Twitter in Numbers," Telegraph, 21 March 2013.

Social media and the websites and internet services that allow users to form networks and share information, views, opinions, photos and other media with each other and the public at large, present unique challenges and opportunities to business enterprises.

As smart phones and tablets become ubiquitous, social media are available almost anytime, anywhere. And thanks to the rapid increase in the number of sites, the year-on-year audience and time spent on social media have skyrocketed.

As their influence has grown, social media have assumed an increasingly powerful role in helping to shape buying behaviors. Social media exponentially amplify the volume, frequency and impact of word-of-mouth marketing.

The speed, spontaneity and pervasive influence of social media have transformed the relationship between companies and their customers, employees, suppliers and regulators.

Companies have taken advantage of social media to strengthen their brand, build customer loyalty and grow market share. But with these opportunities come significant risks, including employees inadvertently leaking sensitive company information, criminal hackers re-engineering confidential information based on information obtained from employee posts, and multiple platforms creating more access for viruses, malware, cross-site scripting and phishing.

Corporations have little choice but to engage with stakeholders via social media, but the risks are real and significant. With its business insights and controls expertise, internal audit can play an indispensable role in assessing, reviewing and measuring compliance with the organization's social media policies.



| Audits that make an impact | Key questions to consider during the audit |
|---|---|
| <p>Social media risk assessment Collaborate with the IT organization to assess the social media activities inside the company and with key service providers that would create the highest level of risk to the organization. Evaluate threats to the organization's information security through the use of social media.</p> | <ul style="list-style-type: none"> ▸ Does the organization understand the risks that relate to social media? ▸ How well are the identified risks managed? ▸ Are mitigation processes adequate and agile? ▸ Who are the key providers of services and what risks reside within their control? ▸ Does the organization have an effective way to monitor social media? |
| <p>Social media governance audit Evaluate the design of policies and procedures in place to manage social media within the organization. Review policies and procedures against leading practices. Evaluate the social media training program.</p> | <ul style="list-style-type: none"> ▸ Is the social media strategy integrated with the company's communications strategy? ▸ Does a governance process exist for social media within the organization? Is it inclusive of the major functional areas? ▸ How well are policies related to social media known among employees? ▸ Is an effective training program in place to make sure that the users are aware of the policies? ▸ Is there a formal structure that identifies key leaders, procedures and policies related to reputational issues? |
| <p>Social media activities audit Review the social media activities of the organization and its users against the policies, procedures and training in place.</p> | <ul style="list-style-type: none"> ▸ Are social media activities aligned to policy? ▸ What corrective actions need to be put in place given activity? ▸ Does the training program provide adequate training for the users? ▸ How does existing activity affect brand and reputation? |
| Key stakeholders/contributors to the audit | |
| <p>CIO and other IT management Legal, HR, communications, investor relations Other assurance/compliance groups involved with reviewing social media Audit committee and C-suite</p> | |

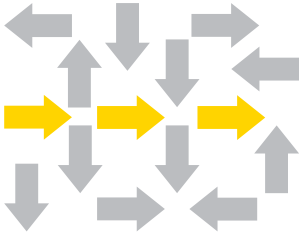


Mobile computing

What is driving mobile computing?

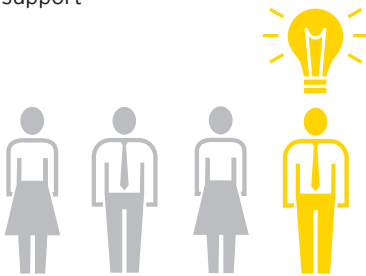
Improving productivity:

Improving employee productivity by extending reach of existing apps, e.g., mobile timesheets



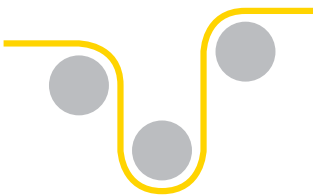
Enabling employees:

Enabling employees via new or more efficient business processes, e.g., mobile field support



Enabling new business:

Targeting new markets or offering clients new products/services, e.g., mobile commerce apps



Estimates suggest that by the next decade, the number of mobile computing devices (e.g., laptops, tablets and smartphones) will be about 10 billion – 1.5 for every man, woman and child on the planet.

Mobile devices allow individuals to access and distribute business information from anywhere and at any time. These devices have already become an integral part of how people accomplish tasks, both at work and in their personal lives. The increasing demand for information from the mobile workforce is driving changes in the way organizations support and protect the flow of information.

Any technological advancement can present the enterprise with new challenges, including:

- ▶ Potential loss or leakage of important business information
- ▶ Security challenges given the range of devices, operating systems and firmware limitations and vulnerabilities
- ▶ Theft of a device due to its small size
- ▶ Compliance with state, federal and international privacy regulations that vary from one jurisdiction to another as employees travel with mobile devices
- ▶ Navigation of the gray line on privacy and monitoring between personal and company use of the device

As mobile devices have become ubiquitous, there has been a huge influx of mobile devices into the enterprise. Whether brought to work by the employee or provided by the company, these devices have been designed to meet the needs of the consumer, not those of the business.

By embracing BYOD (bring your own device) and giving employees access to the tools and services they need to do their job, businesses can harness the computing power of smart consumer-focused devices and increase employee efficiency. However, a large portion of BYOD activity still goes unmanaged. Organizations must learn to harness the power of mobile computing and BYOD while minimizing and mitigating their risks.



| Audits that make an impact | Key questions to consider during the audit |
|--|---|
| <p>Mobile device configuration review</p> <p>Identify risks in mobile device settings and vulnerabilities in the current implementation. Include an evaluation of trusted clients, supporting network architecture, policy implementation, management of lost or stolen devices, and vulnerability identification through network accessibility and policy configuration.</p> | <ul style="list-style-type: none"> ▶ How has the organization implemented “bring your own device” (BYOD)? ▶ Are the right policies/mobile strategies in place? ▶ Are mobile devices managed in a consistent manner? ▶ Are configuration settings secure and enforced through policy? ▶ How are lost and stolen devices managed? ▶ What vulnerabilities exist, and how are they managed? |
| <p>Mobile application black box assessment</p> <p>Perform an audit using different front-end testing strategies: scan for vulnerabilities using various tools and manually verify scan results. Attempt to exploit the vulnerabilities identified in mobile web apps.</p> | <ul style="list-style-type: none"> ▶ What vulnerabilities can be successfully exploited? ▶ What is the response when exploited, and do they even know an intrusion has occurred? |
| <p>Mobile application gray box assessment</p> <p>Combine traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical areas of functionality and for symptoms of common poor coding practices. Each of these “hot spots” in the code should be linked to the live instance of the application where manual exploit techniques can verify the existence of a security vulnerability.</p> | <ul style="list-style-type: none"> ▶ How sound is the code associated with the mobile applications used within the organization? ▶ What vulnerabilities can be exploited within the code? |
| Key stakeholders/contributors to the audit | |
| <p>CIO and other IT management</p> <p>Business line management, legal and HR</p> <p>Other assurance/compliance groups involved with reviewing mobile computing (e.g., CISO, compliance)</p> <p>Audit committee and C-suite</p> | |



Cloud computing

Key risk areas include:

- ▶ Business agility
- ▶ Pay-as-you-go versus install-and-own
- ▶ Cost saving
- ▶ Innovation platform for growth
- ▶ Infrastructure utilization
- ▶ Public investment
- ▶ Market research
- ▶ Security
- ▶ Standardization efforts
- ▶ Risk of missing out

Cloud computing is more than a buzz phrase; it has become a force in the marketplace, and it is clearly nearing an inflection point in terms of broad-based business acceptance and use.

The cloud enables organizations to shed their complex internal IT structures, allowing them to focus on strategy rather than operations and respond quickly to changing marketplace conditions.

Cloud computing is evolving rapidly, giving companies a variety of choices. But like most technology changes, the cloud presents its share of risks and challenges that are often overlooked or not fully understood.

- ▶ **Infrastructure and architectural risks:** These risks arise if providers do not achieve performance requirements that organizations and the providers agree to and define in the service level agreements at the outset of the contract.
- ▶ **Standards and interoperability risks:** It is vital that the organization's systems and those of the provider can communicate with one another.
- ▶ **Regulatory and compliance risks:** Organizations using cloud computing services, and particularly software-as-a-service (SaaS), have lower transparency and ownership over security controls and processes that providers implement.
- ▶ **Cloud vendor management and governance:** Contractual risks stem primarily from the types of contracts that clients enter into with cloud service providers (CSPs).
- ▶ **Business continuity risks:** Cloud users are depending on their CSP's business continuity program and disaster recovery capabilities.
- ▶ **Strategy alignment and governance:** Organizations need a governance model including an enterprise-wide cloud risk management approach.



| Audits that make an impact | Key questions to consider during the audit |
|--|--|
| <p>Cloud strategy and governance</p> <p>Evaluate the organization's strategy for utilizing cloud technologies. Determine whether the appropriate policies and controls have been developed to support the deployment of the strategy. Evaluate alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organization.</p> | <ul style="list-style-type: none"> ▸ Is there a strategy around the use of cloud providers? ▸ Are there supporting policies to follow when using a cloud provider? ▸ Are policies integrated with legal, procurement and IT policies? |
| <p>Cloud security and privacy</p> <p>Assess the information security practices and procedures of the cloud provider. This may be a review of SOC 1, 2 and/or 3 report(s), a review of the security SLAs and/or an on-site vendor audit. Determine whether IT management worked to negotiate security requirements into their contract with the provider. Review procedures for periodic security assessments of the cloud provider(s), and determine what internal security measures have been taken to protect company information and data.</p> | <ul style="list-style-type: none"> ▸ Has a business impact assessment been conducted for the services moving to the cloud? ▸ Does your organization have secure authentication protocols for users working in the cloud? ▸ Have the right safeguards been contractually established with the provider? |
| <p>Cloud provider service</p> <p>Assess the ability of the cloud provider to meet or exceed the agreed-upon SLAs in the contract. Areas of consideration should include technology, legal, governance, compliance, security and privacy. In addition, assess what contingency plans exist in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident, and capacity management and scalability.</p> | <ul style="list-style-type: none"> ▸ What SLAs are in place for uptime, issue management and overall service? ▸ Has the cloud provider been meeting or exceeding the SLAs? What issues have there been? ▸ Does the organization have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units? |
| Key stakeholders/contributors to the audit | |
| <p>CIO and other IT management</p> <p>Business line management, legal and procurement</p> <p>Other assurance/compliance groups involved with reviewing cloud computing (e.g., CISO, compliance)</p> <p>Audit committee and C-suite</p> | |



Cybersecurity

EY's 2013 Global Information Security Survey, *Under cyber attack*, uncovered that:

83% of organizations that responded to the survey said their information security function did not fully meet the organization's needs.

65% of respondents cited budget constraints as their number one obstacle to delivering value to the business.

31% of respondents reported that the number of security incidents within their organization had increased by at least 5% over the previous 12 months.

The way in which companies use and rely on their information systems is changing at a pace that we have never seen before, with increased usage of mobile technology, cloud computing and social media.

These trends are gaining traction because they create an unprecedented ease of access to information. At the same time, companies are struggling to find the balance between supporting enabling technologies and improved access to data, with the need to protect that data from an ever-growing number of malicious individuals. Some of these attackers are insiders, some are opportunistic, and some are so advanced they are able to circumvent even the best-funded company's information controls.

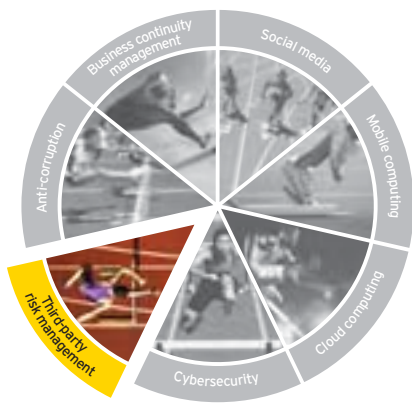
These cybersecurity risks are no longer just the challenge for companies with volumes of customer data (for example, credit card information and protected health information). Increasingly, companies are being targeted for their intellectual property or "crown jewels."

Because of the velocity of change, companies need to focus on identifying these crown jewels and providing differential control of that information. These controls are not just focused on prevention, because companies are finding out that security breaches are a matter of "not if, but when." Companies should focus on "complicating" controls that provide deterrence, assuming that the most persistent attacker will eventually succeed. These controls are balanced by a strong focus on detection and response controls that minimize the time in which attackers are able to maintain access inside a target organization.

Much focus has been placed on achieving compliance with security-focused regulations, but those regulations are meant to set the floor, not the ceiling, for a company's security practices. In addition, each company's security posture is at least as driven by the well-trained people and well-defined processes operating within its environment as by appropriately configured tools and technologies.



| Audits that make an impact | Key questions to consider during the audit |
|---|--|
| <p>Information security program assessment</p> <p>Evaluate the organization's information security program using a framework aligned with widely accepted standards. Provide a clear picture of how the company is prepared to protect the company's key information assets.</p> | <ul style="list-style-type: none"> ▶ How well has the company adapted to the changing threat landscape both in today's world and the unknown future? ▶ Is the company's information security strategy appropriate to protect its critical information assets? ▶ Where are the company's blind spots? ▶ How well does the organization self-assess and mitigate threats? |
| <p>Cyber threat assessment</p> <p>Adopting the mindset, tools and techniques of a malicious attacker, test to determine whether the company's key information assets are at risk. Focus on business and information assets or "trophies," not technology, a notable change from historical "attack and penetration" tests.</p> | <ul style="list-style-type: none"> ▶ What vulnerabilities exist and are exploits of these vulnerabilities detected? ▶ Is external and internal threat intelligence integrated into security practices? ▶ Is the organization able to detect both "noisy" (e.g., brute-force) denial of service attacks and attacks that fly below the radar (e.g., those used by nation-state actors)? ▶ When an intrusion is detected, is the organization's response time appropriate? |
| <p>Identity and access management assessment</p> <p>Review the company's processes for governing who has access to systems and how that access is controlled. Focus on provisioning process, enforcement and certification, role/rule management and reporting and analytics.</p> | <ul style="list-style-type: none"> ▶ Is the company granting access to internal and external users appropriately? ▶ Is access to privileged accounts being controlled? ▶ Is the company positioned to identify and act on inappropriate or unauthorized access? ▶ Are processes enabled for automation to reduce the headcount requirements to implement identity and access management (IAM) processes and controls? |
| <p>Data protection assessment</p> <p>Evaluate the manner in which the company has identified, defined and classified its data, including data protection mechanisms.</p> | <ul style="list-style-type: none"> ▶ Is the company protecting its key information assets across the full data lifecycle (that is, data at rest, in use, in motion)? ▶ Is unstructured data being protected? ▶ Is the company meeting its regulatory requirements to protect data? ▶ Is sensitive data being sent out of the company, and is it appropriately managed? |
| Key stakeholders/contributors to the audit | |
| <p>CIO and other IT management</p> <p>Other assurance/compliance groups involved with reviewing cybersecurity (e.g., CISO, compliance)</p> <p>Audit committee and C-suite</p> | |



Third-party risk management

Key risk areas include:

- ▶ Brand damage
- ▶ Reputation
- ▶ Service and product risks
- ▶ Operational and supply chain risks
- ▶ Legal liability/contract enforcement
- ▶ Regulatory compliance
- ▶ Information security and privacy risks
- ▶ Improper use of trade secrets
- ▶ Third-party use of subcontractors

In a post-financial-crisis world, transparency has become a top-of-mind issue for organizations doing business in both developed and developing countries. As a result, risk management continues to be an important topic for many organizations.

Negative publicity and fines for regulatory compliance infractions, security breaches and data thefts involving suppliers have required companies to continually improve their program and related controls.

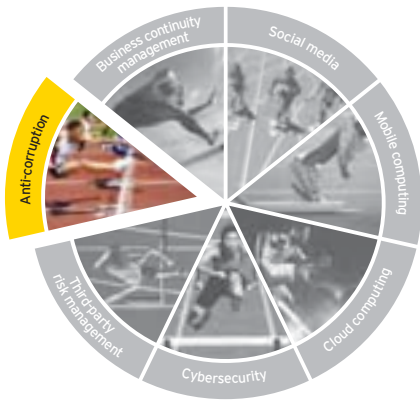
While the processes can be outsourced, the risks involved generally cannot. For example, a US Foreign Corrupt Practices Act (FCPA) violation by a third party could result in fines for the company, and the company would remain responsible for breaches of client confidentiality or privacy that occur at an outsourced site.

As companies look to their suppliers to do more for them, they are becoming more reliant on the third parties with whom they do business. This goes well beyond financial viability of the supplier. In today's connected environment, a supplier's actions may have unintended consequences for the companies that buy from them. External suppliers and business partners must be held to the same corporate standards as the company's own employees.

Companies often take an ad hoc, supplier-by-supplier approach to third-party risk. They struggle to understand their overall exposure related to third parties and have difficulty determining whether that exposure is within the bounds of their risk appetite. Companies without a third-party risk management program in place can find themselves facing not only financial but also reputational, compliance and brand risk.



| Audits that make an impact | Key questions to consider during the audit |
|--|--|
| <p>Overall third-party management program</p> <p>Assess the overall program in place to manage third-party risk across the organization. Cover risk assessment criteria and process, program ownership, roles and responsibilities of various managers/departments, communication protocols, approval authorities, waiver protocols, policies and procedures including dissemination and training, and an ongoing monitoring program.</p> | <ul style="list-style-type: none"> ▶ How consistent is the global supplier risk management process? ▶ How embedded is the process in the organization? ▶ Are ownership, roles and responsibilities clearly understood? ▶ Are risk management processes in place for both direct and indirect suppliers? |
| <p>Contract management process</p> <p>Audit process ownership and control and oversight responsibilities; the overall process for signing new contracts and renewing existing contracts; and the compliance process, including legal, regulatory and company policy. Make sure to include ongoing review of active contracts.</p> | <ul style="list-style-type: none"> ▶ Does the organization have a well communicated process for maintaining and managing contracts? ▶ Have metrics and criteria been established for periodic reviews? ▶ Is the delegation of authority (signing authority) understood, enforced and monitored? |
| <p>Supplier management program</p> <p>Include supplier site reviews, where applicable, relating to security policy; privacy and data management (e.g., leakage and protection); personnel security; access control; physical and environmental security; systems development and maintenance; contract assessment and/or compliance with contracts, standards or service-level agreements; financial assessment; process, risk, and control mapping and assessment; compliance with laws and regulations; and contingency/business continuity planning.</p> | <ul style="list-style-type: none"> ▶ Does the organization have a comprehensive process that is communicated both internally and to suppliers? ▶ Have criteria and metrics been developed that identify potential issues early? ▶ Does the organization have a process requiring periodic submissions of key information by suppliers for review and follow-up? |
| Key stakeholders/contributors to the audit | |
| <p>CIO and other IT management</p> <p>Legal, HR, communications, investor relations</p> <p>Other assurance/compliance groups involved with reviewing third-party risk management</p> <p>Audit committee and C-suite</p> | |



Anti-corruption

EY's 13th Global Fraud Survey, 2014, discovered that:

1 in 5 businesses still don't have an anti-bribery/anti-corruption (ABAC) policy.

45% of organizations have not introduced a whistleblowing hotline.

In **40%** of the countries we surveyed, more than half the respondents said corruption was widespread.

Less than **1/3** of businesses are conducting anti-corruption due diligence as part of their mergers and acquisitions process.

Fraud awareness, prevention and mitigation are everyday issues that need to be a permanent fixture on the organization's agenda. Companies must be vigilant in making sure they comply with regulatory and legal issues.

The FCPA prohibits US companies and their subsidiaries, officers, directors or employees from bribing foreign officials (directly or indirectly) for the purpose of obtaining or retaining business. The FCPA has become an enforcement priority for regulators and a major compliance issue for US companies with global operations. The US Securities and Exchange Commission (SEC) and the US Department of Justice (DOJ) have stepped up their efforts to investigate and prosecute business corruption, significantly raising the reputational and financial risks to companies.

The legislation is not limited to the US. In 2010, the UK Bribery Act was passed and has attracted additional focus from an international perspective on fraud and corruption. This expansive statute covers commercial bribery and does not have an exception for facilitation payments (going beyond the provisions of the FCPA).

Additionally, much like FCPA, the government and regulators are not required to demonstrate actual knowledge of the act by executives – what is known and what you should have known are equally important.

A number of threats related to fraud and corruption risks exist, such as:

Improper payments – Both the FCPA and the UK Bribery Act require organizations to monitor their relationships with suppliers and customers, including a focus on any payments. There is a definitive focus on the BRIC (Brazil, Russia, India and China) countries, as continuing education and monitoring is needed there, as well as other emerging markets (such as Africa).

Loss of key suppliers due to an improper relationship or a relationship built on bribes – As organizations monitor their relationships with suppliers, they must be prepared to handle the fallout from relationships built on unethical and illegal acts. As part of this planning and monitoring, they must be able to replace key suppliers.

Loss of key customers and associated expected sales revenue – Similar to key suppliers, organizations must be prepared to walk away from customers that have relationships built on unethical or illegal behavior, including side deals or kickbacks.

Third parties making improper payments or associating with unethical behavior – As organizations enter new countries and utilize subcontractors, joint ventures or other third-party relationships, they must be sure that their code of conduct and policies are followed to remain compliant with all applicable laws and regulations.

Additionally, organizations must focus on the reputational risk due to being associated with unethical or illegal behavior. Negative public perception can be as damaging as legislative or judicial fines or punishments.



| Audits that make an impact | Key questions to consider during the audit |
|---|--|
| <p>Supplier management review</p> <p>Evaluate the process that management has put in place to qualify and accept suppliers, specifically focused on BRIC countries and other emerging markets (such as Africa). Focus on the controls for making sure that company policies and procedures are in place and being consistently followed. Focus on the company's strategy to track and handle supplier management in the high-risk locations. This will include a review of supplier acceptance and the periodic supplier continuance review process.</p> | <ul style="list-style-type: none"> ▶ What high-risk markets does the organization operate in? ▶ What is the process for accepting new suppliers? ▶ Who is involved in the process and what are the controls in place? ▶ What is the process for validating continuing relationships with suppliers? |
| <p>FCPA program assessment</p> <p>Review the company's approach to FCPA compliance. Undertake a detailed review of the policy, procedures and internal controls in place to remain compliant. Review the company's training and education programs for employees and third parties as well as the company's approach to remaining up to date on all applicable laws and regulations.</p> | <ul style="list-style-type: none"> ▶ Who owns and is responsible for FCPA compliance? ▶ What is the organization's process for risk-assessing the countries in which it operates? ▶ What is the process for making sure that the FCPA compliance program remains up to date with any new legal or regulatory requirements? |
| <p>Whistleblower audit</p> <p>Focus on the company's compliance program, with an emphasis on the policies, procedures and internal controls of the program. Review the whistleblower hotline, management's response to new accusations and the process to follow potential issues identified through to completion. Also focus on the controls in place to make sure that whistleblowers' anonymity, as defined by the law is protected.</p> | <ul style="list-style-type: none"> ▶ Who owns and is responsible for the company's compliance program? ▶ What is the process for a whistleblower to provide feedback to the company? ▶ What controls are in place to make sure that the program promotes confidentiality of those who contact the whistleblower hotline? ▶ What is the process for following up on tips provided through the hotline and other channels? |
| Key stakeholders/contributors to the audit | |
| <p>Legal, business lines, HR, compliance</p> <p>Other assurance/compliance groups involved with reviewing for anti-corruption (e.g., internal control functions, information security)</p> <p>Audit committee and C-suite</p> | |



Business continuity management

Effective BCM is rising in importance on the corporate agenda. It includes:

- ▶ Business continuity
- ▶ Program governance
- ▶ Clear policies that are communicated to and understood by employees
- ▶ Disaster recovery plan
- ▶ Crisis management plan

As organizations grow in size and complexity within the world of the extended enterprise, the impact of non-availability of any resources has become magnified.

High-profile events caused by natural disasters and technology infrastructure failures have increased awareness of the need to develop, maintain and sustain business continuity programs. Although these large-scale events – such as the March 2012 Japanese earthquake and tsunami – dramatically challenge the existence of some companies, there are smaller, less impactful but more frequent disruptions that cause many executives to question their organization's ability to react and recover. The big disasters, as well as these smaller disruptions, have prompted leading executives to hope for the best but prepare for the worst by investing in effective business continuity management (BCM).

Effective BCM is rising in importance on the corporate agenda. Volatile global economies have greatly reduced margins for error. Companies that previously would have survived a significant disaster or disruption may now find the same event pushing their corporate existence to the brink. Executives are realizing that effective BCM may be the only buffer between a small disruption and bankruptcy.

BCM should be viewed as an enterprise-wide risk effort and the reality is that it is often IT that is asked to lead critical planning activities and serve as lead facilitator. IT systems and disaster recovery procedures are a cornerstone of the broader BCM plan. But a crisis management plan, another key component of BCM, has become even more important now that social media can reach a company's stakeholders and customers in a blink of the eye. Companies need to know what is being said, by whom and know that they are well prepared to react appropriately and quickly.



| Audits that make an impact | Key questions to consider during the audit |
|---|--|
| <p>Business continuity program integration and governance</p> <p>Evaluate the organization's overall business continuity plan, including program governance, policies, risk assessments, business impact analysis, vendor/third-party assessment, strategy/plan, testing, maintenance, change management and training/awareness.</p> | <ul style="list-style-type: none"> ▶ Does the organization have a holistic business continuity plan in place? ▶ How does the plan compare to leading practices? ▶ Is the plan documented and communicated appropriately? ▶ Is the plan tested? |
| <p>Disaster recovery</p> <p>Assess IT's ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.</p> | <ul style="list-style-type: none"> ▶ Are disaster recovery plans aligned with broader business continuity plans? ▶ Do testing efforts provide confidence that systems that can be effectively recovered? ▶ Are all critical systems included? Are they defined? |
| <p>Crisis management</p> <p>Review the organization's crisis management plans, including overall strategy/plan, asset protection, employee safety, communication methods, public relations, testing, maintenance, change management and training/awareness.</p> | <ul style="list-style-type: none"> ▶ Are crisis management plans aligned with broader business continuity plans? ▶ Are plans comprehensive and do they involve the right corporate functions? ▶ Are plans well communicated and tested? |
| Key stakeholders/contributors to the audit | |
| <p>Legal, business line management, IT, HR, compliance, security, corporate communications</p> <p>Other assurance/compliance groups involved with reviewing BCM (e.g., internal control functions, information security, compliance)</p> <p>Audit committee and C-suite</p> | |



Keep pace – take action

As its mandate expands, IA needs to conduct multiple balancing acts simultaneously. Is your IA function prepared to help management answer questions like these?

- ▶ Can that security breach at XYZ Company happen to us?
- ▶ Do our suppliers embrace our ethical culture and comply with laws and regulations?
- ▶ How quickly can we respond to natural disasters or other disruptions to the business?
- ▶ Do our employees understand the risks of using social media?

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights.



Accelerating high growth companies' climb to the top: *strong risk management practices and Internal Audit capabilities as drivers for growth.*
www.ey.com/IAriskmanagement



Expecting more from risk management: *drive business results through harnessing uncertainty.*
www.ey.com/REPM



Building trust in the cloud: *creating confidence in your cloud ecosystem.*
www.ey.com/cloudtrust



Matching Internal Audit talent to organizational needs: *key findings from the Global Internal Audit Survey 2013.*
www.ey.com/IASurvey2013



Overcoming compliance fatigue: *EY's 13th Global Fraud Survey.*
www.ey.com/fraudsurvey



Under cyber attack: *EY's Global Information Security Survey 2013.*
www.ey.com/giss2013



Anti-corruption internal audits: *a crucial element of anti-corruption compliance.*
www.ey.com/anticorruptionIA



Using data analytics to enhance compliance with corporate social media policy.
www.ey.com/SManalytics



Bring your own device: *security and risk considerations for your mobile device program.*
www.ey.com/byod


About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited.
All Rights Reserved.

EYG no. AU2515
ED None

 In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, go to: ey.com/advisory.

The leaders of our Risk practice are:

| Global Risk Leader | | |
|-------------------------------|------------------|--|
| Paul van Kessel | +31 88 40 71271 | paul.van.kessel@nl.ey.com |
| Global and Americas IA Leader | | |
| Michael O’Leary | +1 312 879 4605 | michael.oleary@ey.com |
| Area Risk Leaders | | |
| Americas | | |
| Amy Brachio | +1 612 371 8537 | amy.brachio@ey.com |
| EMEIA | | |
| Jonathan Blackmore | +44 20 795 11616 | jblackmore@uk.ey.com |
| Asia-Pacific | | |
| Iain Burnet | +61 8 9429 2486 | iain.burnet@au.ey.com |
| Japan | | |
| Yoshihiro Azuma | +81 3 3503 1100 | azuma-yshhr@shinnihon.or.jp |