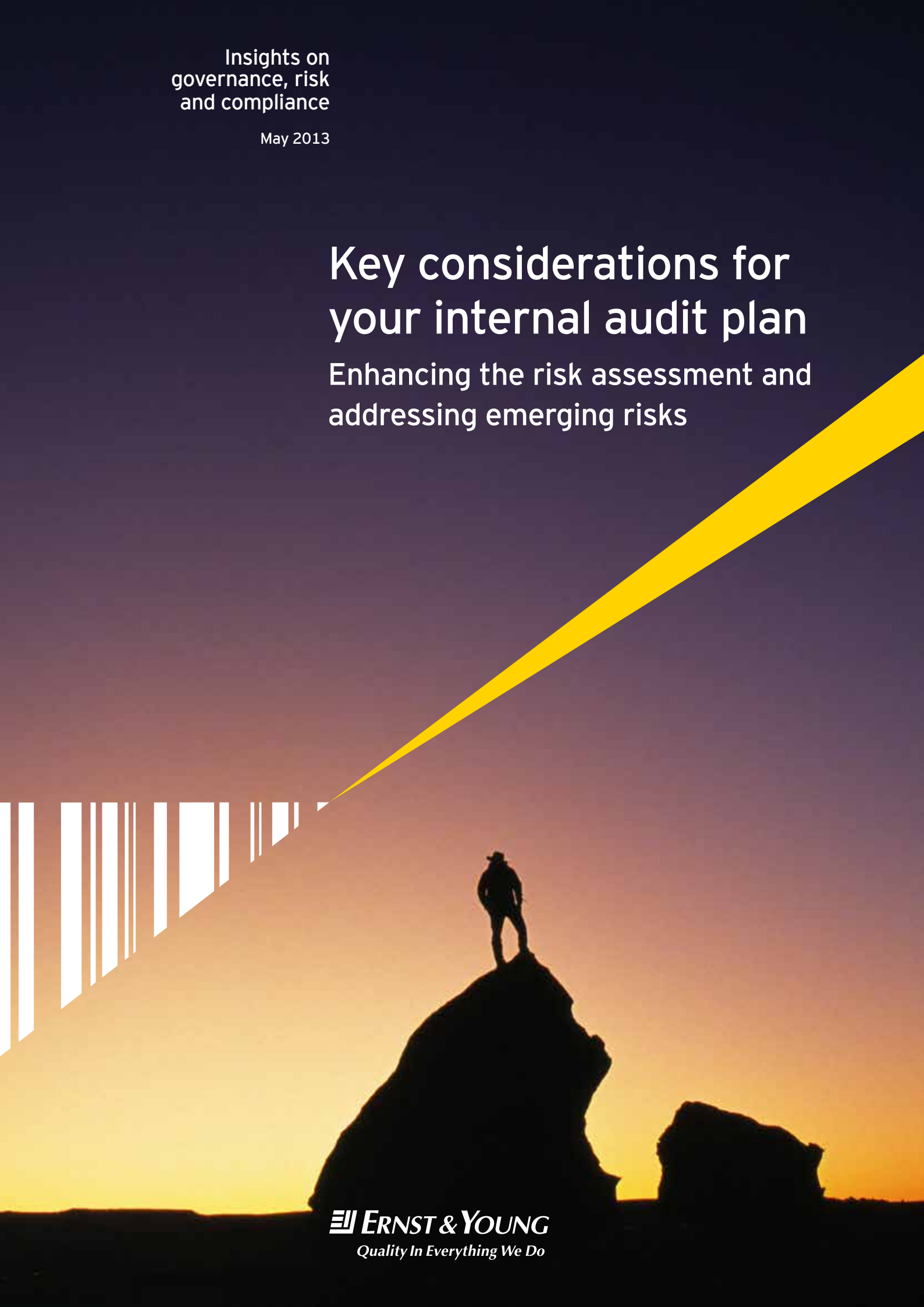
Insights on governance, risk and compliance

May 2013

Key considerations for your internal audit plan

Enhancing the risk assessment and addressing emerging risks



ERNST & YOUNG
Quality In Everything We Do

Contents

The internal audit risk assessment and the ongoing refresh processes are critical to identifying and filtering the activities that internal audit can perform to provide measurable benefit to the organization. While there are often a number of "non-negotiable" activities that internal audit functions must support (SOX and other regulatory compliance, external auditor assistance), the internal audit department has the opportunity to deliver increased risk coverage, cost savings and measurable value to the business by identifying and performing audits across the company's value chain. In our role as the leading provider of internal audit services, we have spent considerable time working with our clients and thought leaders to:

1. Identify emerging risks and areas that most organizations are currently focused on
2. Develop practical audit ideas for these emerging risks
3. Consider the questions that chief audit executives should be asking to further qualify their relevance

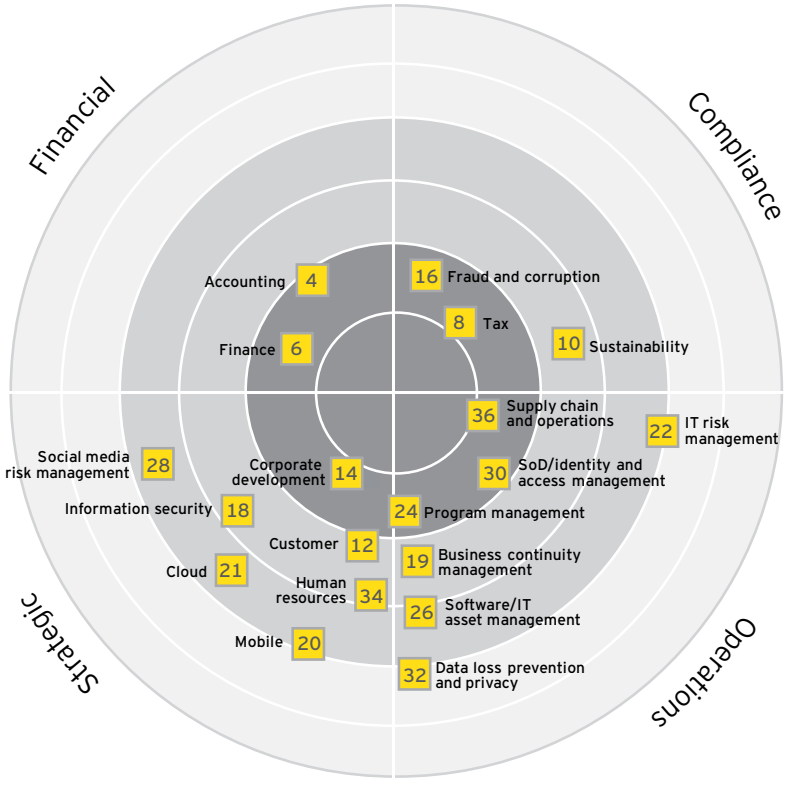
The following pages provide a view of where the processes begin by identifying these emerging risks and focus areas and their corresponding practical, value-based audits. This document is intended to facilitate discussion as your organization develops and updates its internal audit activities for the future.

Recommended reading

Business Pulse: exploring dual perspectives on the top 10 risks and opportunities in 2013 and beyond Global report

www.ey.com/businesspulse

The risk radar below depicts the risk by functional area of the business, ranked across the risk management spectrum – financial, compliance, operations and strategic. The number associated with each function indicates the page where you can find more information about the emerging risks related to the function, focus areas for internal audit and examples of related audits that deliver value to the business.



Source: Ernst & Young, 2013

Risk assessment leading practices

Why is the need for a world-class internal audit risk assessment more vital than ever?

There are multiple drivers behind the growing importance of executing a robust and comprehensive risk assessment:

1

Internal audit executives continue to be challenged by the Audit Committee and executive management to "look around the corner" and answer the question, "Have we identified all the big risks?"

2

Changes in the marketplace and external environment:

- Increased risk due to expanding operations in emerging markets and developing countries
- Increased regulatory demands
- Increased focus on cost savings across all functions – including internal audit

3

Changes in the role of internal audit within organizations:

- Effective use of internal audit resources no longer means only maintaining a world-class assurance program that keeps the organization out of trouble. The department must also improve the business through value-based audits and recommendations.
- Investors are willing to pay for it – 82% of institutional investors are more willing to pay a premium for effective risk management (source: Ernst & Young survey)

Components of the risk assessment
Data reviewed
Data analytics
Stakeholder engagement
Interview/survey techniques
Collaboration
Audit prioritization
Outputs

When assessing risk to the organization, internal audit functions typically fall between basic and leading on the maturity curve below. As your department moves toward leading by utilizing the techniques listed here, you increase your ability to look around the corner and identify the right risks.

Basic	Degree of confidence	Leading
▸ Internal audit issues ▸ SOX and external audit issues	Low ● ● ● ● ● High	▸ Root causes ▸ Competitor and peer risks ▸ Industry trends ▸ Third-party external risk data ▸ Analyst reports
▸ Analytics run but limited summarization of data ▸ Business and IA leadership struggle to spot trends in data		▸ Risk analytics are based on most critical questions business and IA need to answer ▸ Trending and period-to-period comparisons can identify emerging risks or changes to existing risks ▸ Efforts are aligned with other "big data" initiatives
▸ Focus on Finance/Accounting/IT stakeholders ▸ Heavy emphasis on "home office" stakeholders ▸ Point-in-time engagement primarily during annual risk assessment ▸ Business leaders are not trained on risk management		▸ Includes operational and global stakeholders beyond Finance/Accounting/IT ▸ Risk management is embedded in leadership training ▸ Risk scenario planning workshops ▸ Continuous dialogue with stakeholders (monthly, quarterly meetings) ▸ Risk committee utilized to review risk assessment changes
▸ Inconsistent documentation of interviews ▸ Surveys used for SOX 302 certification purposes or not at all		▸ Subject matter resources participate in select interviews to draw out key risks ▸ Surveys used to confirm risk assessment results with lower-level management not interviewed ▸ Stakeholders self-assess risk based on GRC solution containing dynamic risk database
▸ Internal audit attends interviews with little participation from other risk management functions ▸ Risk assessment viewed as "internal audit's risk assessment"		▸ Risk assessment collaboratively developed by internal audit and other risk management functions ▸ SOX, external audit and other risk management functions participate in interviews ▸ Risk assessment embedded within strategic planning process
▸ Impact and likelihood utilized for prioritization ▸ Audits prioritization based heavily on competencies available in IA department		▸ Relevance to strategic objectives is utilized to prioritize risks ▸ Audits executed based on value to organization and connection to strategic objectives
▸ Relatively static internal audit plan		▸ Dynamic internal audit plan (3+9) ▸ SOX plan ▸ External audit plan and IA reliance strategy ▸ Legal/ethical compliance training plans ▸ Business risk mitigation plans (where appropriate)

What increases confidence in the risk assessment process?

- **Diversity in data,** stakeholders and participants leads to greater risk insight.
- **Technology,** used in the right way, is a game changer.
- **Collaboration** and an **embedded** process lead to a deeper analysis.

Accounting

The pace of change to accounting standards is unprecedented in the US and globally. Multinational organizations need to understand how business decisions affect accounting and reporting today, as well as the impact anticipated changes to standards may have. The business needs to develop practical strategies for managing the impact of accounting changes on the organization. There needs to be particular focus in countries where regulators are increasingly aligning local regulations with IFRS, such as Brazil and the United Kingdom. It is imperative for the internal audit department to be aware of potential changes to accounting regulations, such as:

- **SEC accounting, disclosure and reporting matters** – The SEC staff recently discussed year-end financial statement considerations and their areas of focus: revenue recognition disclosures, valuation of deferred tax assets and observations related to the new fair value disclosures. It is expected that auditors will need to place extra scrutiny in these areas.
- **FASB and IASB** – The two organizations recently commented on their joint convergence projects related to:
  - *Revenue recognition.* The new standard is expected to be finalized in 2013. The remaining issues to be finalized relate to disclosure and transition to the new standard.
  - *Leases.* Significant changes have been made to prior drafts developed by the Boards, and the revised proposal is expected to be released for comment in the first quarter of 2013. The new draft is expected to end off-balance-sheet accounting for leases by lessees.
  - *Financial instruments.* The exposure draft on classification and measurement is expected to be issued in the first quarter of 2013. Many changes have been made for convergence in these areas, but the two Boards remain relatively far apart on the issue of impairment.
- **IFRS update** – The SEC is continuing to investigate whether to incorporate IFRS into the US financial reporting system and, if so, when to do so. The indication is that a decision will not be made anytime soon.

As organizations are executing the day-to-day activities to meet the reporting requirements, there are specific areas that they need to focus on to mitigate the associated risks:

- **Statutory reporting** – Multinational organizations need to understand the statutory reporting requirements and the processes they need in place to meet them. The business must assess its requirements and evaluate the opportunity to increase consistency in its financial reporting processes.
- **Business transformation** – As organizations continue to look for opportunities to drive cost out of the business through major transformations (e.g., shared service center implementations), the accounting and reporting function must be aware of the significant risk to the business. Organizations must use these transformations as an opportunity to streamline their accounting policies and controls, thereby reducing both cost and risk.
- **ERP system implementation** – The implementation of an ERP system is a significant investment by the organization and often takes several years to be fully integrated. As an organization is planning such a migration, the business should assess the changing accounting and control requirements and incorporate them into their plans.

Recommended reading

Seizing the opportunity in global compliance and reporting: survey trends

www.ey.com/GL/en/Services/Tax/Seizing-the-opportunity-in-Global-Compliance-and-Reporting--Global-Compliance-and-Reporting-Survey

Operationalizing statutory reporting: driving global consistency to create savings and transparency

www.ey.com/Publication/vwLUAssets/Operationalizing_Statutory_Reporting/$FILE/Operationalizing%20Statutory%20Reporting_Driving%20global%20consistency.pdf

The audits that make an impact	Key questions to evaluate during audit
Accounting policy review — The internal audit team focuses on the defined entity-wide accounting policies of the organization. The team reviews the consistency of application across entities through sample testing (e.g., account reconciliations, accruals, manual journal entries). Additional time is spent reviewing accounting policies against leading practices (e.g., number of days to close each month/quarter) and proposed legislation or regulatory changes.	▸ What are the defined accounting policies of the organization? ▸ What is the process to disseminate updates and/or changes to the policy to all personnel? ▸ What is the process for deviating from policy and is there an approval matrix for these deviations based on materiality?
Lease accounting review — The internal audit team inventories and reviews the organization's leases. A review of the policy for leases is conducted, with individual leases being sampled for adherence to policy and applicable guidance. For additional added value to the organization, the internal audit team identifies improvement opportunities in the lease analysis (e.g., use of a standard template) process.	▸ Does the organization have a database or repository of all of its leases? ▸ Is there an approval matrix for leases based on materiality? ▸ What is organization's policy on leases? ▸ What are the controls in place in the lease identification and execution process?
Statutory risk assessment — The internal audit team focuses on the countries in which the organization operates and assesses the statutory risk to the business. A risk assessment is performed of the locations based on the statutory reporting risk of each location, as well as the materiality and inherent risk of the company's operations in each location.	▸ Who owns statutory reporting? ▸ Where have we had issues from a statutory reporting perspective in the past? ▸ For countries in which we operate, which are inherently higher risk? ▸ Are we appropriately aligning our resources for statutory reporting based on risk?

Finance

While finance functions have historically been a focus of internal audit departments, pressures from within the organization to lower costs and improve the efficiency of the function have been augmented by emerging challenges. The push for shared service centers, implementations of global ERP systems, and the standardization of global policies, procedures and operations have increased the pressure on CFOs and their functions. With these initiatives come risks that internal audit needs to identify, assess and help the organization mitigate with appropriate controls and strategies.

In addition to the internal pressures to reduce costs and operate more efficiently, external developments are also demanding more of finance functions. For instance, consider the recent trauma in the global financial markets, the unknown impact of the implementation of the Patient Protection and Affordable Care Act in the United States, and the uncertainty surrounding additional governmental policy and legislation. While all of this is occurring, finance and its leader, the CFO, are expected to serve as a business partner in strategic decision-making by putting the right information in the hands of decision makers at the right time.

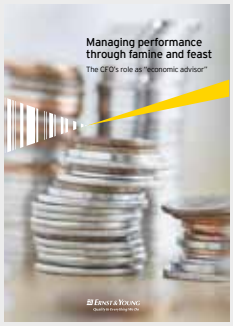
Consider the following finance risks and their impact on the function and organization.

- **Disparate finance systems and processes** – Multinational and global organizations frequently grow through inorganic methods (e.g., acquisitions), often leading to the need to manage different ERP packages and supporting systems. Additionally, the financial processes and their controls are often not consistently designed (or performed), leading to a potential roadblock in the business's operations.
- **Management reporting** – Finance is responsible for assessing the data provided by the business and making decisions that shape the strategy and direction of the organization. Often this data is extracted from the system and manipulated in spreadsheets and other document forms that are not able to be locked down with the same level of internal control as a traditional ERP system. A lack of accurate and easily accessible data leads to delays in the decision-making process and potential missed opportunities.
- **Budgeting and forecasting accuracy** – Oftentimes too much time is invested in the budgeting process and insufficient time is invested in forecasting. As organizations continue to spend increased time on their budgets, specifically the effort to reduce them across the business, the risk that they are focusing on cost reduction efforts at the expense of accuracy of their forecasts becomes real.
- **Value delivery of strategic initiatives and cost reduction programs** – Value delivery of cost reduction efforts are rampant at all large organizations. Unfortunately the desire to reduce costs within the enterprise is often with a short-term view and also frequently non-integrated, failing to achieve sustainable improvement.
- **Manual processes** – Despite the implementation of ERP systems and the standardizing of processes referenced above, processes still rely on resource-intensive, spreadsheet based sub-processes to provide the data the organization requires. This effort is often performed at the detriment of the controls that ensure the validity and accuracy of the data.

Recommended reading

Managing performance through famine and feast: the CFO's role as "economic advisor"

www.ey.com/GL/en/Services/Advisory/Managing-performance-through-famine-and-feast---CFO-report



Views. Vision. Insights: the evolving role of today's CFO

www.ey.com/GL/en/Issues/Managing-finance/The-DNA-of-the-CFO---perspectives-on-the-evolving-role---The-CFO-s-contribution

The audits that make an impact	Key questions to evaluate during audit
Analysis of the budgeting and forecasting process – Assess the annual budgeting and forecasting processes including the internal controls and potential process, improvement recommendations. Review the primary business segments of the organization, current state processes and root cause issues driving inaccuracies in the forecast.	▸ What is the current process for budgeting and forecasting and is it consistent across business units/locations? ▸ How do we monitor the accuracy of the budgeting and forecasting process? ▸ What are the controls in place to assess accuracy and completeness of the process? ▸ What actions would be required to address the gaps?
Capital allocation review – Review the comprehensive capital allocation process focusing on internal controls and potential process improvement recommendations. Evaluate the capital request and approval process, committee and approval structure and return on investment tracking.	▸ How does the organization manage capital allocation requests and what is the process for prioritizing them? ▸ How does the capital allocation process mirror the goals and strategies of the organization?
Global costing review – Review the policies and internal controls of the process to monitor cost and profitability margin by product line/service. Evaluate the organization's internal control structure and provide potential process improvement recommendations for identified control gaps or deficiencies.	▸ What is the process for determining the profitability (margin) goal by service/product line? ▸ Are controls related to margin analysis designed and operating effectively? ▸ Are there opportunities to increase the efficiency of controls?
Treasury process review – The internal audit team focuses on the business process and controls for cash forecasting, funding, hedging and derivatives, and compliance with applicable debt covenants. Additional focus is given to the vetting and granting of credit to customers (if owned by Treasury).	▸ Who owns treasury and is it a global process? ▸ How do we monitor the accuracy of cash forecasting? ▸ What are the controls in place to assess the treasury process? ▸ What actions would be required to address the issue gaps? What would be the benefits of addressing the identified gaps?
Finance benchmarking assessment – As the organization performs a benchmarking assessment of its finance function, internal audit has a role in the compliance and controls workstream. The team focuses on benchmarking the organization's cost of controls relative to its competitors and industries. Additional feedback is provided on the utilization of technology in the finance processes (automated controls, continuous control monitoring).	▸ What is the company's total spend on the planning, execution and monitoring of controls and compliance? ▸ How does our spend compare with our peers/industry? ▸ Is there an opportunity to leverage additional automation? If so, where and how?

Opportunities for integrated audits between IT and operational audit *Audit was frequently mentioned in survey of leading IA organizations*

Tax

Tax risk goes well beyond the tax technical application of the law. Factors that contribute to increased pressure on organizations to develop and maintain an effective tax risk management strategy include expanding business operations, increasingly complex tax legislation and regulations, significant accounting developments, expanding global internal control and tax authority regimes and greater transparency and increased accountability to stakeholders. Interestingly, since the inception of reporting under Section 404 of the Sarbanes-Oxley Act (SOX 404), tax reasons have accounted for about 30% of adverse opinions filed under SOX 404 each year and continue to be a leading cause of restatements.

The financial crisis has brought about an uptick in globalization, causing a large shift in capital flows toward emerging markets. Policy-makers in emerging markets are rapidly enacting mechanisms to capture their fair share of the global tax pie. In many mature markets, governments have an urgent need to increase revenues. As a result, they are attempting to raise taxes and intensify enforcement for companies operating within their borders.

It is in this context that the following tax topics are receiving attention across the enterprise and should be considered during the risk assessment and potentially in the audit plan:

- **Failure to integrate tax in large global initiatives** — Large initiatives such as moves to a shared service environment, implementation of an ERP or supply chain transformation are all examples of initiatives that are critical for tax to be involved in up front. Where tax is not involved, tax compliance issues, process inefficiencies or a lack of available data for tax purposes all emerge as concerns for the organization.
- **Lack of availability of data** — Tax is one of the largest consumers of data within any organization. A lack of accurate and accessible transactional data for tax purposes is a top root cause of tax compliance issues, not to mention a driver of inefficiencies and excess cost for the organization.
- **Transfer pricing** — While tax owns the transfer pricing policy, it is the business that is typically asked to define and execute the controls that ensure compliance with the policy. Therefore, a key risk related to transfer pricing remains the ability to sustain transfer pricing controls. Operationally, a lack of transparency into transfer pricing profit (due to a lack of data) often leaves the organization waiting until it is too late to make changes to prices or controls. Transfer pricing risk is compounded by tax authorities with very divergent goals.
- **VAT and other indirect taxes** — These transactional taxes continue to create risk due to the fact that heavy reliance is placed on the accuracy of information in the business to comply. While tax can provide direction and guidance related to indirect taxes, it is the transactions being executed by the business that drive compliance, and organizations often do not have the right processes and controls in place. Identifying the right structure (in the business, versus within tax) to manage VAT and indirect tax is a complex issue companies continue to assess.
- **Tax complexity in Brazil and Latin America** — Latin America, and specifically Brazil, continues to present a greater level of tax risk for organizations. This is driven by the complexity of tax rules, a lack of resources familiar with both US and Brazilian tax rules in the region and governmental policy decisions.

Other risks that continue to receive attention include: failure to identify tax planning opportunities and manage tax obligations across all jurisdictions; failure to manage non-income tax obligations like customs duties; failure to track the movement of expatriates and assets across foreign tax locations, resulting in permanent establishment or nexus issues; and/or a lack of resources with tax accounting skills in foreign jurisdictions.

The management of tax risk is complex and requires the participation of different constituents with the requisite skills partnering with the business and tax department to properly assess, remediate and monitor these risks. Internal audit can, and should, play an integral role in the organization's broader tax risk management approach.

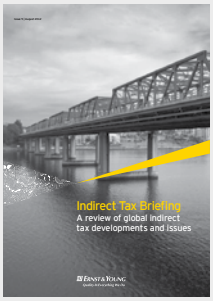
The audits that make an impact	Key questions to evaluate during audit
Transfer pricing audit – This audit is not just an assessment of the company's compliance with policy but a broader look at the processes, controls and data in place to sustain compliance. Assess the accuracy, completeness and availability of data used to understand transfer pricing profit margin, confirm invoices accurately reflect transfer prices, and evaluate the design and operating effectiveness of management's monitoring processes, including reports and periodic meetings to monitor performance. An emerging area of risk to consider would be the harmonization of transfer pricing and custom valuations.	▸ Is the data that is needed to understand transfer price profitability available and accurate? ▸ What controls are in place within the business to monitor transfer pricing compliance? ▸ What can be done to improve the accuracy of transfer prices and reduce frequent changes to transfer prices or year-end surprises? ▸ Is the organization at risk for inconsistent transfer pricing and custom valuations?
Tax data assessment – Evaluate the availability, completeness and accuracy of data needed to comply with tax regulations. This audit is executed by first understanding the source of all data necessary for tax (determined in coordination with tax or third party). The team then evaluates gaps in either the completeness, accuracy and availability of data and articulates the impact of the gap. Management can use the results of this audit to evaluate future actions and the benefits of addressing the gaps.	▸ What data and related data resources are the most critical to efficient and effective tax compliance within the organization? ▸ Where does a lack of data availability, completeness or accuracy create inefficiencies (from a cost or time standpoint) for the organization? What is the impact of those inefficiencies and why do they exist? ▸ How can the gaps be addressed, and what would be the benefits of addressing them?
VAT (indirect taxes) – Perform an end to end process review of the company's VAT tax process. This includes evaluation of how data is compiled, processed and ultimately reported to tax authorities. Confirm that appropriate controls, technology, competencies and processes exist to efficiently comply. This audit may also result in opportunities for substantial cost savings by improving the accuracy and efficiency of the VAT tax process. Other areas of indirect tax such as sales and use tax could also be considered for this audit.	▸ Is data needed for VAT purposes captured accurately and completely? ▸ Are controls in place to ensure VAT is calculated accurately? ▸ Who "owns" VAT processes and do they have the necessary skills to ensure compliance? ▸ Are there opportunities for cost savings related to VAT?
Tax compliance audit – Evaluate the tax provision and other tax-compliance-related processes to confirm controls are designed and operating effectively. To add value to the organization, identify ways in which controls can be further optimized for adequate risk coverage while increasing efficiency.	▸ How efficient is the process to compile data for the tax provision? Is there global visibility into the process? ▸ Are controls related to compliance designed and operating effectively? ▸ Are there opportunities to increase the efficiency of controls?

Opportunities for integrated audits between IT and operational audit *Audit was frequently mentioned in survey of leading IA organizations*

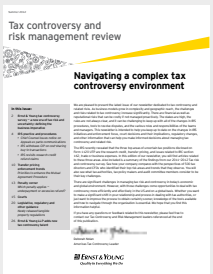
Recommended reading

www.ey.com/US/en/Services/Tax/Tax-Library

Indirect Tax Briefing: a review of global indirect tax developments and issues



Navigating a complex tax controversy environment



Sustainability

Awareness of environmental issues and the increased focus on the scarcity of natural resources has brought sustainability to the forefront for many organizations. In a recent review of the proxy statements of the Russell 3000, more than 900 shareholder proposals were submitted on environmental and social topics, the most across the four major proposal categories (environmental/social, board-focused, compensation and anti-takeover/strategic proposals). This shift was attributed to growing support from "mainstream investors" on environmental/social topics as well as widespread corporate recognition of the business case for sustainability. Additionally, legislation such as the Dodd-Frank Act and disclosure requirements on "conflict minerals" have increased the risk in this area.

As the focus on sustainability grows, key topics continue to emerge:

- **Managing the global supply chain** — There is significant interest in how organizations are identifying and mitigating risks related to sustainability of their supply chain. Stakeholders are focused on sustainability reporting, environmental impacts and human/labor rights and working conditions. Companies are frequently being asked for disclosure of supply chain practices and/or related risks.
- **Linking executive compensation to sustainability metrics** — To drive sustainable change through the organization, the executives must be properly incented and measured. Leading organizations are incorporating nonfinancial performance metrics into their executive compensation programs — a trend that will only increase as sustainability grows in importance.
- **Including environmental/social considerations in employee qualification** — Stakeholders are seeking information on how organizations link their overall business strategies with environmental/social matters.
- **Conflict minerals** — Section 1502 of the Dodd-Frank Act requires certain public companies to provide disclosures about the use of "conflict minerals" from the Democratic Republic of the Congo (DRC) and nine adjoining countries. The minerals requiring reporting are cassiterite, columbite-tantalite, wolframite and gold. These minerals are commonly used in the automotive, consumer products, technology, telecommunications, diversified industrial products, aerospace, power and utilities and chemical sectors.

Even though there are a number of uncertainties related to sustainability, leading companies are leveraging their reporting capabilities as a differentiator to demonstrate their performance and enhance their reputation with stakeholders by focusing on the following:

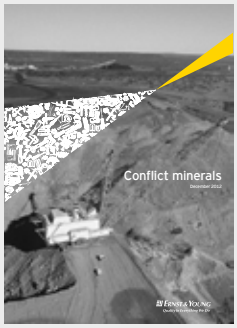
- **Tracking and monitoring of sustainability requirements** — Increasingly, as organizations are being asked for information on their sustainability performance, there is a risk that the company is not accurately and completely identifying the metrics to be tracked. Increased regulatory activities such as the "conflict minerals" disclosure requirements specified in Dodd-Frank have further increased these risks for companies.
- **Data availability** — Being able to measure, monitor and report on the issues that matter to investors, legislators and regulatory agencies is dependent on an organization's ability to easily access the requisite data.
- **Tools to facilitate reporting** — The reporting requirements and needs for organizations continue to grow, but the tools to capture and consolidate the information are still being developed. In a survey of 272 organizations across 24 industry sectors, approximately 25% use packaged software, while the rest rely on spreadsheets, emails and phone calls to track their sustainability metrics.
- **Competitor ratings** — Third parties are now providing investors, regulatory agencies and the public at large with company rankings for efforts in the sustainability and environmental space. Valued sustainability rankings include the Dow Jones Sustainability Index and the Carbon Disclosure Project. The risk exists of negative public perception and decreased brand esteem.

Recommended reading

www.ey.com/US/en/Services/Specialty-Services/Climate-Change-and-Sustainability-Services

The three S's of environmental marketing: what the revisions to the FTC Green Guides mean for "green" marketing

Conflict minerals



Climate change and sustainability: five highly charged risk areas for internal audit

The audits that make an impact	Key questions to evaluate during audit
Corporate responsibility audit – Evaluate the processes for developing and issuing the corporate responsibility report. Additional focus will be given to the metrics utilized in the report, process for collecting this information, and the verification of the completeness and accuracy of this data. The internal audit team should evaluate the gaps in completeness, accuracy and/or availability of the data required to issue the report.	▸ Who is responsible for developing and issuing the responsibility report? ▸ What are the key performance indicators and metrics supporting the report? ▸ How does the company determine that the information included in the report is complete and accurate? ▸ What controls are in place within the business to monitor the report? ▸ What can be done to improve the accuracy and timeliness of the responsibility reporting process?
Energy management audit – The internal audit team assesses the company's current energy usage at significant locations, as well as their efforts to reduce energy usage. The internal audit team focuses on the company's energy management strategy, how it is implemented, the metrics used to track usage and reductions, and the ramifications of overages and missed projections.	▸ Does the company have defined energy usage/reduction goals? ▸ What is the process for communicating these goals and their importance to employees? ▸ What are the metrics used by the company to monitor energy usage? ▸ How are individuals held responsible to drive reductions in energy usage?
Sustainability metric review – The internal audit team identifies the appropriate sustainability metrics and reviews the organization's approach for monitoring them. Additional focus is given to how the organization manages the identified metrics, monitors their performance and links their performance to executive compensation.	▸ What are the sustainability metrics that are applicable to the organization? ▸ How does the organization monitor the metrics? ▸ How does the organization's performance against the sustainability metrics impact the executive officers?
Conflict minerals review – The internal audit team focuses on the organization's process to comply with the "conflict minerals" disclosure requirement. The team reviews the company's applicability assessment, reasonable country of origin inquiry, due diligence process and conflict minerals report (if deemed necessary). Additionally, the team reviews the required independent audit of the company's conflict minerals report.	▸ Who owns the organization's conflict minerals disclosure? ▸ What is the organization's process for performing the conflict minerals applicability assessment? ▸ What is the process to determine ongoing compliance with the requirements?
Evaluation of consistency and substantiation in disclosures – The internal audit team focuses on reviewing both financial and non-financial publications to evaluate consistency in financial reporting with non-financial reporting – for example, companies that respond to the Carbon Disclosure Project survey and site climate change risks and opportunities as material to the organization but do not disclose them as material in the 10-K. Another example is auditing the data behind any sustainability claims on products and in other communications that would be subject to the FTC Green Guides.	▸ What sustainability claims is the organization making? ▸ Is there consistency in our financial and non-financial publications in this area? ▸ Who reviews the data behind any sustainability claims?

Opportunities for integrated audits between IT and operational audit *Audit was frequently mentioned in survey of leading IA organizations*

Customer

While customers are clearly some of the most valued stakeholders of any organization, conversation related to customer risk is often limited to pricing compliance, sales commissions and rebates/ marketing incentives versus broader operational and strategic concerns. The areas of customer can be compartmentalized as follows: customer strategy, customer experience and insight, and sales and marketing productivity. Below we touch on each of these areas and provide insight into how to broaden the typical customer-related audits and add value to the organization.

Customer strategy

Acquiring, maintaining and expanding relationships with customers are extremely competitive aspects of any business. There are significant risks — from the decision to enter a market (and identify its customers) to the decision to exit a particular product line or service — that organizations must continually evaluate:

- **Market effectiveness and return-on-investment** — In a stagnant economy, there is continued risk related to unproductive use of funds for marketing purposes and an inability to effectively measure return on investment. Internal audit can help manage this risk by assessing ROI and the organization's processes to allocate marketing spend. This is in addition to more traditional marketing and advertising contract audits for potential cost recovery.
- **Pricing strategy and improvement opportunities** — The lack of information to make pricing decisions (primarily total cost data), a disconnected pricing strategy and poor implementation of the pricing strategy through sales channels and contracting create significant risk within the organization.
- **Product innovation and life cycle management** — As organizations focus on improving margin through customer-based product innovation, the risk that product innovation is disconnected from the customer or not fully integrated with the necessary business functions emerges.
- **Digital marketing strategy** — Marketing "went digital" long ago, but in today's rapidly evolving technological world, failure to keep the strategy up to date is a key risk. With social media emerging as a primary way for customers and organizations to connect, the risks related to customer, HR, legal and IT will continue to blur.

Customer experience and insight

With growing pressures on product margins, an increasingly diverse customer base, and rising costs to acquire new customers, more and more companies are differentiating themselves by gathering additional customer insight to improve their customer experience. Companies must be in tune with the real-time experiences and feedback of their customers, and the value of this information must be leveraged and capitalized on.

Based on these focus areas, organizations need to consider the following risks:

- **Failure to properly segment and understand customers** — Organizations may not truly understand the characteristics and needs of their customers, thus resulting in poor pricing and marketing strategies and a drop in profitability.
- **Customer support** — Poor customer support can quickly reduce customer confidence and erode profitability.
- **Lack of proactive metrics to measure performance** — Identifying the right metrics to proactively provide management with an indication of performance is critical and often an area organizations struggle with.

Sales and marketing productivity

For most organizations, a significant amount of capital is spent on sales and marketing to attract, retain and expand relationships with customers. Organizations must develop the appropriate metrics and reporting to monitor the effectiveness of their sales forces and marketing materials. There are a number of focus areas related to sales and marketing productivity that the internal audit department should be aware of:

- **Sales productivity improvement** — This area includes developing and sustaining the right account strategy and opportunity sizing processes. This also includes understanding where and how members of the sales force utilize their time and how it aligns to the overall account and opportunity sizing process.
- **Sales organization structure** — This relates to having the right sales force structure and span of control sizing to deliver on sales goals.
- **Sales performance management** — To obtain the most from the sales organization, it's important to have clear roles defined and a formal career pathing process. Sales metrics and incentive compensation must be aligned to the overall organizational goals to drive the right behavior. This is a critical risk area for members of the sales organization.

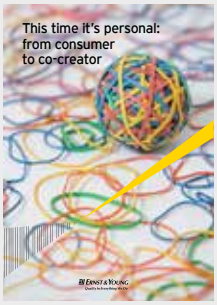
The audits that make an impact	Key questions to evaluate during audit
Marketing effectiveness and ROI review — This audit includes reviewing the process to develop key marketing programs and then assessing management's ability to measure the success. Also included in this audit may be an assessment of key contracts with marketing and advertising vendors. This portion of the audit would be structured as a more traditional contract compliance review.	▸ Are marketing programs developed and approved in compliance with company policies and processes? ▸ Do program incentives drive customer behavior that is aligned to corporate strategy? ▸ Are marketing and advertising providers delivering on contractual terms? ▸ How effectively does the organization measure ROI associated with significant marketing programs?
Product innovation audit — Evaluate the processes and controls related to the organization's ability to innovate. This audit would assess the effectiveness of the stage and gates process defined and, most importantly, how well the innovation process is integrated across business functions.	▸ Does a formal process for product innovation exist? ▸ How well is the process followed when taking a product to market? ▸ How integrated are all business functions in the innovation process? ▸ How does the company measure the success of the product?
Sales performance management — This audit focuses on the incentives utilized to reward sales associates. Assess the alignment of incentive programs with corporate strategy (confirm programs do not reward behavior that is not aligned to strategy). This audit also includes a review of incentive pay, from calculation to payout.	▸ Do incentive programs for the sales force drive the right behaviors? ▸ Is incentive compensation and sales commission calculated accurately and completely? ▸ How are incentive programs developed and approved? ▸ Are internal policies followed?
Pricing compliance and strategy — This audit includes a pricing compliance review, which confirms prices charged to customers on invoices are appropriate per approved pricing. The scope also assesses the process and controls for making pricing changes, approving incentive pricing business cases and other pricing administration activities. A subject matter resource is often used in these audits to take a more strategic look at the pricing strategy, the pricing departmental structure and the metrics used within the department to measure performance.	▸ Is the right information available to make pricing decisions? ▸ How effective are the processes and controls in place to approve pricing decisions? Are customer rebates and incentive programs approved formally with business cases? ▸ Are prices accurately applied to invoices? Are credit memos often issued to reduce prices and are adjustments approved?
Customer experience review — This audit generally focuses on the organization's customer support function. Functional policies and procedures are evaluated to determine how well the organization meets commitments to customers. A more strategic part of this audit includes an assessment of the metrics used to measure customer experience and the accuracy of this reporting.	▸ How effective is the customer support function in meeting customer demands? ▸ Are formal metrics to monitor performance utilized and, if so, how accurate is the reporting associated with the metrics? ▸ Are company policies and procedures followed when supporting the customer?

See also risks and audits related to social media, page 28.

Recommended reading

This time it's personal: from consumer to co-creator

www.ey.com/GL/en Services/ Advisory/This-time-its-personal--from-consumer-to-co-creator



Corporate development

In the ever-changing economic world, the corporate development function is more crucial than ever. Corporate development serves as the lifeblood for an organization by providing strategic advice to the board, actively managing the organization's portfolio, divesting non-core assets and pursuing acquisitions to deliver increased value to the business. In this complex area, there are a significant number of potentially material risks. In the following section, we identify these risks and the audits that may be performed to deliver additional value to the business.

Divestitures

As organizations focus on preserving, optimizing and raising capital, they often use divestitures to strategically manage their portfolios. Deciding when and how to sell an operating unit can be extremely difficult. As companies continue to rationalize their product portfolio based on internal and external factors, internal audit may play a role in enhancing management's credibility and preparedness. By focusing on the right areas, the internal audit team may assist in preserving the deal's value and maximizing the after-tax proceeds for the organization. By remaining an active participant in the process, audit may help to mitigate the risks to the organization in the following areas:

- **Carve-out financial statements** — Being able to appropriately value the carve-out business requires the organization to have the necessary data and financial information. Often this is a significant effort for the organization due to how it is set up (e.g., systems, consolidation process).
- **Tax analysis** — The structuring of the divestiture transaction has a significant impact on the tax implications of the deal. Most transactions involve businesses with operations in multiple countries, further complicating the process and enhancing the risk to both the organization and acquiring company.
- **Buyer diligence** — After deciding to divest of a portion of its portfolio, an organization must have an approach to dealing with the buyer diligence process. Decisions on the amount and type of information to be shared, and at what point in the divestiture life cycle it will be shared, must be made prior to the identification of potential buyers.
- **Operational preparedness** — As a company or business unit is divested from an organization's portfolio, the remaining business must have the appropriate processes and controls in place to ensure that it is prepared to operate post-transaction close.

Mergers and acquisitions

As the business landscape continues to become more and more competitive, organizations are looking for ways beyond organic growth to continue to meet and exceed their goals. In a recent survey of US companies, 76% believe the global economy shows no signs of improvement. Mergers and acquisitions are viewed as one route to help company's meet their targets and continue to deliver value to their shareholders. Organizations must be actively monitoring the M&A market in emerging markets. For instance, Brazil has seen year-over-year M&A activity increase 16%. The acquisition and integration of a business or segment involves significant risk throughout the process and must be tightly monitored by the organization:

- **Validate requirements and understand the issues for the transaction** — As organizations initiate the process to identify possible acquisition targets, there is significant risk if the objectives and goals for the transaction are not clearly defined at a detailed level.
- **Perform due diligence of potential targets** — Organizations must have a defined approach to performing due diligence and financial analysis of the identified targets. They must have previously identified the information that they need and the process they want to go through in order to successfully evaluate the target.
- **Review potential compliance and regulatory issues that may arise from acquisition** — When considering a potential target, the company should be aware of and actively managing the compliance and regulatory issues that may arise as a result of the transaction.
- **Continue ongoing support of the business and its integration strategy** — For the transaction to be truly successful, the organization needs to have a defined plan, process and controls in place to assist with the transitioning of the target. The transaction is not truly complete until the target is operating like other segments of the organization.

Would-be buyers should also perform anti-corruption due diligence as a first step in considering deals abroad. This due diligence should be performed prior to traditional financial due diligence of a potential target. This is especially important given the potential for successor liability of an acquired organization, and is an area where internal audit can be of significant value to the organization.

The audits that make an impact	Key questions to evaluate during audit
Merger and acquisition process integration review – This audit is focused on evaluating the organization's process to integrate operations, technologies, services and product lines after the transaction has closed. The internal audit team focuses on the policies and procedures in place to make the transaction as seamless as possible. Additionally, the internal audit team will review the defined key performance indicators (KPI) for the integration, as well as the process to monitor the KPIs.	▸ What are the defined control points in the integration process? ▸ Who is involved in the acquisition integration process and what are their roles? ▸ What are the KPIs to determine whether the integration is successful? ▸ How is the acquired organization transitioned to the company's policies and procedures in a timely manner? ▸ Are there any new reporting requirements or disclosures as a result of the acquisition? ▸ What is the process for assessing the culture of the target organization and identifying the steps necessary to assimilate the people into our business?
Business development/due diligence assessment – The internal audit team will focus on the process and controls in place to manage the business development life cycle from the identification of target organizations to the qualification and offer process. Additional consideration is given to the strategic decision-making process for the allocation of capital.	▸ What is the process and what are the controls for identifying and qualifying acquisition targets? ▸ Who is responsible for monitoring the controls and how effectively are they operating? ▸ Where do vulnerabilities or gaps exist? ▸ What is being done to remediate these gaps?
Divestiture/carve-out review – The internal audit team reviews the process and controls in the divestiture/carve-out life cycle, from review of existing business units/segments to the qualification of potential buyers and the offer process. The team focuses on the process and controls in place during the identification, analysis and potential sale/closing of the operations/business unit. A focus is placed on the carve-out life cycle, including strategic analysis, opportunity analysis, transaction development, negotiation advice and execution, and measuring and monitoring of transaction efficiency and effectiveness.	▸ Is the carve-out life cycle formally defined and adhered to? ▸ What are the defined control points in the divestiture process? ▸ Who is involved in the process and what is their level of involvement? ▸ What are the key performance indicators to determine success?

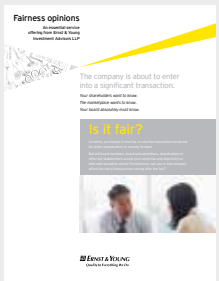
Opportunities for integrated audits between IT and operational audit *Audit was frequently mentioned in survey of leading IA organizations*

Recommended reading

www.ey.com/US/en/Services/Transactions/Corporate-Development

Divesting for value

Fairness opinions: the company is about to enter into a significant transaction



Fraud and corruption

Companies must recognize that 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 ensuring their compliance with regulatory and legal issues. The Foreign Corrupt Practices Act (FCPA), enacted in 1977, 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. In 2010, the SEC and DOJ alleged FCPA violations against 47 companies and levied more than US$1.7b in penalties. To demonstrate that this was not a passing fad, the SEC and DOJ alleged violations of 16 companies and levied fines of US$509m in 2011.

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** — As referenced in both of the aforementioned acts, organizations must 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 (e.g., 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 while still operating their business.
- **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. By remaining diligent and proactive, the internal audit function may play a key role in the organization's compliance in this area.

Recommended reading

www.ey.com/US/en/Services/Assurance/Fraud-Investigation---Dispute-Services/Assurance-Services_FIDS_Library

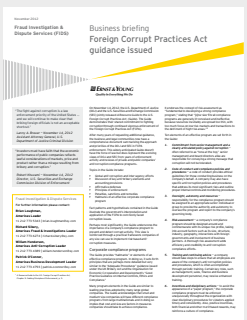
Navigating today's complex business risks: Europe, Middle East, India and Africa Fraud Survey 2013

Building a robust anti-corruption program: seven steps to help you evaluate and address corruption risks

The audits that make an impact	Key questions to evaluate during audit
Supplier management review – Evaluate the process management has put in place to qualify and accept suppliers, specifically focused on BRIC (Brazil, Russia, India and China) countries and other emerging markets (e.g., Africa). The internal audit team will focus on the controls for ensuring that company policies and procedures are in place and being consistently followed. Additional focus will be 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.	▸ 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?
● **FCPA program assessment** – The internal audit team would review the company's approach to FCPA compliance. A detailed review of the policy, procedures and internal controls in place to remain compliant will be a focus of the team. The internal audit team will review the company's training and education programs for employees and third parties. Also, the team will focus on the business' approach to remaining up to date on all applicable laws and regulations.	▸ 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 ensuring the FCPA compliance program remains up to date with any new legal or regulatory requirements?
● **Whistleblower audit** – The internal audit team would focus on the company's compliance program with an emphasis on the policies, procedures and internal controls of the program. The internal audit team will review the whistleblower hotline, management's response to new accusations and the process to follow potential issues identified through to completion. Additional focus will be given to the controls in place to ensure anonymity of whistleblowers as defined by the law.	▸ 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 ensure 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 mediums?

● *Audit was frequently mentioned in survey of leading IA organizations*

Business briefing: foreign corrupt practices act guidance issued


Fraud Investigation & Dispute Services (FIDS)

Business briefing
Foreign Corrupt Practices Act guidance issued

Ernst & Young

Information security

Recommended reading

Fighting to close the gap: Ernst & Young's 2012 global information security survey

www.ey.com/giss2012

Traditional security models focus on keeping external attackers out. The reality is that there are as many threats inside an organization as outside. Mobile technology, cloud computing, social media, employee sabotage — these are only a few of the internal threats organizations face. Externally, it's not just about the lone hacker who strikes for kicks. Overall, the risk environment is changing. Often, security professionals complain that they are too busy reacting to immediate issues and have no time to anticipate what may be lurking around the corner. To have any hope of protecting your organization's critical assets, the business and security teams need to understand where your information lives, inside or outside. Identifying what your organization classifies as its most important information and applications, where they reside and who has or may need access to them will enable the business to understand which areas of the security program are most vulnerable to attack.

Although organizations have been dealing with opportunistic cyber attacks for years, many now find themselves the target of more sophisticated and persistent efforts. These attacks are focused on a single objective, often lasting over a long period of time and until the desired target is obtained. They leave few signs of disturbance because they are designed to remain hidden to acquire as much sensitive information as possible. In our experience, those at the greatest risk are information-intensive entities or organizations with intellectual property that is most attractive in emerging economies. Unfortunately, many organizations have no idea they are compromised until it is too late.

In considering the audits below, IT internal audit can play a critical role in evaluating the organization's information security strategy and supporting program and partnering to improve the level of control.

The audits that make an impact	Key questions to evaluate during audit
Information security program assessment — Evaluate the organization's information security program, including strategy, awareness and training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies and reporting.	▸ How comprehensive of an information security program exists? ▸ Is information security embedded within the organization, or is it an "IT only" responsibility? ▸ How well does the organization self-assess threats and mitigate the threats?
● **Threat and vulnerability management program assessment** — Evaluate the organization's threat and vulnerability management (TVM) program, including threat intelligence, vulnerability identification, remediation, detection, response and countermeasure planning.	▸ How comprehensive of a TVM program exists? ▸ Is the TVM program aligned with business strategy and the risk appetite of the organization? ▸ Are the components of TVM integrated with one another, as well as with other security and IT functions? ▸ Do processes exist to address that identified issues are appropriately addressed and remediation is effective?
Vulnerability assessment — Audit should perform, or make certain IT performs, a regular attack and penetration (A&P) review. These should not be basic A&Ps that only scan for vulnerabilities. Today we suggest risk-based and objective-driven penetration assessments tailored to measure the company's ability to complicate, detect and respond to the threats that the company is most concerned about.	▸ What mechanisms are in place to complicate attacks the organization is concerned about? ▸ What vulnerabilities exist and are exploits of these vulnerabilities detected? ▸ What is the organization's response time when intrusion is detected?

● *Audit was frequently mentioned in survey of leading IA organizations*

Business continuity management

As organizations grow in size and complexity within the world of the "extended enterprise," the impact of non-availability of any resources has 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 shrunk 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. Ernst & Young's 2012 Global Information Security Survey found that BCM was once again viewed as the "top priority" in the next 12 months by survey respondents.

While BCM should be viewed as an enterprise-wide risk and effort, 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, and thus, IT audit is well positioned to evaluate broader BCM procedures.

Recommended reading

Ready for the challenge: integrated governance – the key to effective business continuity management

www.ey.com/GRCinsights

The audits that make an impact	Key questions to evaluate during audit
Business continuity program integration and governance audit – 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.	▸ Does a holistic business continuity plan exist for the organization? ▸ How does the plan compare to leading practice? ▸ Is the plan tested?
Disaster recovery audit – Assess IT's ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.	▸ Are disaster recovery plans aligned with broader business continuity plans? ▸ Do testing efforts provide confidence systems that can be effectively recovered? ▸ Are all critical systems included? Are critical systems defined?
Crisis management audit – 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.	▸ 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?

Opportunities for integrated audits between IT and operational audit

Mobile

Recommended reading

Mobile device security: understanding vulnerabilities and managing risk

www.ey.com/GRCinsights

Mobile computing devices (e.g., laptops, tablet PCs, smartphones) are in widespread use, allowing individuals to access and distribute business information from anywhere and at any time. With the increase in mobile device capabilities and subsequent consumer adoption, these devices have 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. With any technological advancement comes new challenges for the enterprise, 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 the device due to the 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

IT internal audit's knowledge of the organization's mobile strategy needs to evolve as quickly as the mobile landscape. Evaluating these risks and considering the audits below will help audit add value to the organization while confirming key risks are well managed.

The audits that make an impact	Key questions to evaluate during audit
Mobile device configuration review — Identify risks in mobile device settings and vulnerabilities in the current implementation. This audit would 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.	▸ 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 do we manage lost and stolen devices? ▸ What vulnerabilities exist, and how do we manage them?
Mobile application black box assessment — Perform 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.	▸ What vulnerabilities can be successfully exploited? ▸ How do we respond when exploited, and do we know an intrusion has occurred?
Mobile application gray box assessment — 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.	▸ How sound is the code associated with the mobile applications used within the organization? ▸ What vulnerabilities can be exploited within the code?

Cloud

Many organizations are 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. This is attained by shifting to a user of IT services, as organizations no longer need to build and maintain complex internal IT infrastructures. Cloud computing is evolving at a fast pace, giving companies a variety of choices when looking to restructure their IT organization. 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. These risks and challenges include:

- Providers not living up to service level agreements (SLAs), resulting in cloud architecture or deployment challenges
- Evolving cloud standards increasing the risk that a company's systems won't work with the provider's
- Legal and regulatory risk in how information is handled in the cloud
- Information security and privacy risks around the confidentiality, integrity and availability of data
- Cloud adoption and change management within an organization

IT internal audit needs to understand how the organization is embracing cloud technologies and the risks the business faces based on the adopted cloud strategy.

Recommended reading

Ready for takeoff: preparing for your journey into the cloud

www.ey.com/GRCinsights

The audits that make an impact	Key questions to evaluate during audit
Cloud strategy and governance audit — Evaluate the organization's strategy for utilizing cloud technologies. Determine if 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.	▸ 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?
Cloud security and privacy review — Assess the information security practices and procedures of the cloud provider. This may be a review of their SOC 1, 2 and/or 3 report(s), a review of their security SLAs and/or an on-site vendor audit. Determine if 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.	▸ 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?
Cloud provider service review — 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, internal audit should 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.	▸ 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, both sponsored within IT or direct by the business units?

IT risk management

As the IT risk profile and threat landscape rapidly changes and risks increase, companies need to change their mindset and approach toward IT risk to address a new normal. Now more than ever, IT issues are issues of importance to the C-suite. Boards of directors, audit committees, general counsels and chief risk officers need to work alongside IT leaders and information security and privacy officers to fully address their organization's risk management level of due care, approach and preparedness and to implement an IT risk management program that is adequate and effective in managing cyber risks. It is critical that IT functions are able to effectively address the following questions:

- Can you articulate your strategy to identify, mitigate and monitor IT risks to the audit committee?
- How do you know that you have identified all key IT risks that would prevent the company from achieving corporate strategies, objectives and initiatives?
- How do you make sure your risk framework continues to be relevant and continues to identify pertinent risks to keep the company out of trouble?

The Securities and Exchange Commission, other regulators and the audit committee have increased their focus on companies managing risks holistically. Company stakeholders/ shareholders expect the company to focus risk management activities and resources on areas with the greatest impact. Internal audit is uniquely positioned to help drive growth and create value to the company through reviewing IT risk management activities.

Recommended reading

The evolving IT risk landscape: the why and how of IT risk management today

www.ey.com/GRCinsights

Use governance, risk and compliance technology to turn risk into results

www.ey.com/5

The audits that make an impact	Key questions to evaluate during audit
IT risk management strategy assessment — Assess the framework and process IT has embedded within the function to assess and manage risks. Evaluate the actions taken to mitigate risks and the level of accountability within the process.	▸ How well does IT identify risks? ▸ What is done once a risk is identified? ▸ Are IT risk management processes followed? ▸ Does your IT risk program cover all of IT including shadow IT? ▸ Is responsibility for risk coverage clearly defined? ▸ How are IT risks identified, remediated or accepted?
IT governance audit — Evaluate the processes IT has in place to govern capital allocation decisions, project approvals and other critical decisions.	▸ Do formalized processes to govern IT exist? ▸ What can be done to increase business confidence in IT governance? ▸ Are your IT governance processes and requirements applicable across all of IT? ▸ Are there formal charters, mandates and responsibilities documented and followed by key steering committees?
● **IT risk assessment** — As an advisory audit, participate in IT's own risk assessment (as opposed to the independent IT internal audit risk assessment). Evaluate the risks identified and provide insight given your unique perspective of the IT organization.	▸ Is there a comprehensive risk assessment performed to identify all IT risks? ▸ Is the IT risk assessment process effective? ▸ How can the process be enhanced? ▸ Is there an opportunity to coordinate the IT internal audit risk assessment with IT's own risk assessment?
Technology enablement/GRC package selection — Evaluate the organization's current use of GRC software or the GRC software selection process. Provide value-added insight on critical business requirements.	▸ How can GRC software be effectively used within the organization? ▸ How mature is the organization's use of existing GRC software? Do we use all functionality available to us? ▸ What are the key business requirements for GRC software? ▸ How many GRC technology solutions are in use across the organization? Is there an opportunity for solution convergence? ▸ What is the level of risk reporting provided to stakeholders to support IT risk decisions?

● *Audit was frequently mentioned in survey of leading IA organizations*

Technology risk management in a cyber world: a C-suite responsibility

www.ey.com/5

Program management

Program complexity is increasing at a faster rate than companies can adapt. While companies have been cautious with investments over the last few years, investment portfolios are now being expanded to keep up with emerging trends (e.g., shared service centers, system implementations). As organizations continue to look for ways to take costs out of the business, they are undertaking significant initiatives to redesign and standardize business processes.

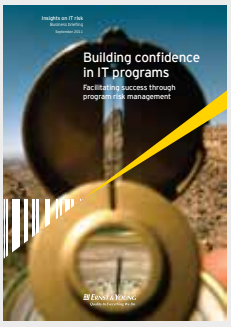
Specific to IT, Gartner predicts spending will increase at an average rate of 5.3% per year through 2015. Gartner also indicates that approximately 20% to 50% of a company's IT spending will be focused on programs and projects – depending on an organization's initiatives. However, organizations continue to fail to deliver on their large IT programs. Approximately two out of three programs are not on budget, delivered too late and/or do not deliver the expected benefits. Lastly, 70% of the major enterprise resource planning (ERP) programs fail to realize at least 50% of business benefits.

While companies have invested significantly in increasing their knowledge and capabilities in program and project management, this is not visible in the success rates. In our opinion, the lack of improvement is mainly due to increased complexity in business processes and the emerging technology landscape. Organizations are still failing to properly adapt their program approaches to this increased complexity. Research indicates a strong link between program maturity capabilities and program execution and market competitiveness. Internal audit can play an effective role in confirming the right processes are in place to manage programs and those processes and controls are being executed appropriately.

Recommended reading

Building confidence in IT programs: facilitating success through program risk management

www.ey.com/GRCinsights



Strategy deployment through portfolio management: a risk-based approach

www.ey.com/GRCinsights

The audits that make an impact	Key questions to evaluate during audit
Project management methodology audit – Assess the design of processes and controls in place to manage projects against leading practices.	▸ Are the right processes and controls in place to provide that projects are delivered on time, on budget and with the right resources? ▸ Are controls in place to measure achieved benefits against intended benefits after project completion?
Project and program execution audit – Evaluate common areas of high risk on programs (e.g., third-party contracting, business change, test strategy, data migration). Outputs provide confidence to management that high-risk areas have been independently checked and verified to leading practice.	▸ Is project/program management methodology being followed correctly? ▸ What is done when projects are underperforming? ▸ How is project risk assessed and managed?
Portfolio risk review – Review strategy, projects and programs to assess alignment. This review focuses on assessing the prioritization of the project portfolio in support of increasing value and reducing the risk that the transformation portfolio exposes.	▸ Do the right governance processes exist to provide that projects/programs align to company strategy? ▸ How is the portfolio managed as corporate objectives change?
Shared service center review – Evaluate the processes and controls related to a shared service center implementation. In-scope processes are assessed to verify that control points are in place and have also been optimized to leverage available technology (e.g., automated controls).	▸ What is the process for transitioning to the shared service center? ▸ What processes are in-scope? Has the control framework been reviewed as part of the transition process? ▸ Is there a controls workstream for the implementation? ▸ What technology is being utilized as part of the transition?
Process redesign review – Assess the business's plan for redesigning its business processes as part of a major initiative (e.g., system implementation). The internal audit team focuses on the project plan, management structure and approach to redesigning the control framework for the in-scope processes.	▸ Who are the project team members and what are their roles? ▸ Is there a documented controls workstream? ▸ What is the process for leveraging automation and system controls in the redesigned process?

Opportunities for integrated audits between IT and operational audit

Software/IT asset management

With increased focus on cost reduction in a global economy struggling to recover, effective software asset management and IT asset management can have a very positive impact by helping to reduce license-related expenses, improve IT service management by more efficiently managing IT asset inventories, better manage compliance-related risk and even improve overall operating efficiencies. Leading IT directors and the chief information officers to whom they report are realizing that effectively managing software assets can be a strategic advantage. For example, effective asset management:

- Potentially reduces liability risk by maintaining license compliance and avoiding related penalties
- Lowers potential costs by helping to avoid license and other IT asset "overbuying"
- Helps to more efficiently manage the otherwise resource-draining and labor-intensive compliance processes
- Limits potential reputational risks associated with license violations or compliance-related conflicts with vendors

Software licenses currently account for about 20% of typical IT costs, and the already pervasive use of software continues to rise. At the same time, many IT directors are noticing that their software vendors have become more diligent in ensuring that their customers remain in compliance. IT leaders, members of the C-suite and shareholders have come to expect increasingly more from their investments, including those which rely on IT functions.

As IT auditors, it is critical that software and IT asset management processes and controls are well understood. It's not just about cost management — strong IT asset management processes affect the following, as examples:

- **IT service management** — IT asset management is critical to effectively locate and service assets, replace and retire existing assets, etc.
- **Information security** — Without a clear view of existing IT assets and software, it's difficult to prioritize and evaluate the associated security risk of those assets.
- **IT contract management** — It is understandable that without an effective way to manage an organization's IT assets, it may be equally difficult to understand what contracts exist with vendors for those assets, whether they are managed in a cost-effective manner and whether any violations from contracts may exist.

The audits that make an impact	Key questions to evaluate during audit
IT and software asset management process and control audit – Assess the design and effectiveness of processes and controls that IT has deployed related to software and IT asset management. Review the impact of these processes on related IT processes such as IT service management, IT contract management and information security.	▸ Do we have a comprehensive approach to IT asset and software management? ▸ How well do we manage software license costs? ▸ Is there an IT and software asset management technology solution in place to support these processes? If not, should there be?
Software license review – Perform a review of significant software license agreements (e.g., ERPs) and evaluate the effectiveness of IT's software asset management process in practice. Assess opportunities for cost reduction from improving the management of software licenses.	▸ Are there opportunities to renegotiate software licensing agreements based on the way we actually utilize software versus the way original contracts were negotiated? ▸ Are we violating any existing contractual agreements?
IT contract management assessment – Evaluate the IT organization's ability to manage contracts and how effectively IT and supply chain coordinate to manage costs and negotiate effective agreements.	▸ Are IT asset and software contracts planned, executed, managed and monitored effectively? ▸ Are there "shadow IT" contractual agreements executed in other parts of the organization?

Opportunities for integrated audits between IT and operational audit

Recommended reading

Effective software asset management: how to reap its benefits

www.ey.com/GRCinsights

Social media risk management

The social media elements that generate business opportunity for companies to extend their brands are often the same elements that have created IT-related risk. Like the borderless nature of social media itself, the various risks surrounding social media can be borne by multiple enterprise functions at the same time, challenging companies to understand how, when and where to engage their IT functions or plug risk coverage gaps. Legal, compliance, regulatory, operational and public relations issues are at the top of the list of potential IT-related social media risks that can ultimately cause erosion of customers, market share and revenue. For example, on most of the popular sites (Twitter, Facebook and LinkedIn), users are able to create company profiles and communicate on behalf of the organization through social media channels. This can create marketplace confusion because of multiple messages and different audiences, policies and practices. Other more specific headline-grabbing examples of social-media-related risks include:

- Employees involved in social media inadvertently leaking sensitive company information
- Criminal hackers "re-engineering" confidential information (e.g., log-ins and passwords) based on information obtained from employee post
- Employee misuse of social applications while at work
- Hacked, faked or compromised corporate or executive Twitter or Facebook fan page or individual accounts
- Multiple platforms creating more access for viruses, malware, cross-site scripting and phishing
- Damage to a brand or company reputation from negative, embarrassing or even incriminating employee or customer posts, even those that are well-intended
- Failure to establish complete and fully compliant archiving and record-retention processes for corporate information shared on social media, especially in the health care, financial services and banking industries

IT is heavily relied on to enable social media strategies in coordination with marketing strategies. It is critical that IT audit has an understanding of the organization's social media strategy and the related IT risk and adds value by providing leading practice enhancements and assurance that key risks are mitigated.

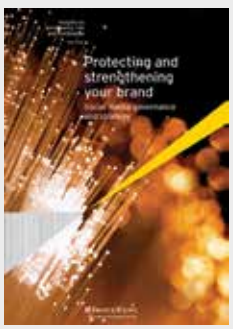
The audits that make an impact	Key questions to evaluate during audit
Social media risk assessment – Collaborate with the IT organization to assess the social media activities that would create the highest level of risk to the organization. Evaluate the threats to the organization's information security through the use of social media. This audit may be combined with a social media governance audit to then confirm policies have been designed to address the highest risks to the organization.	▸ Does the organization understand what risks exist related to social media? ▸ How well are the identified risks managed?
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.	▸ Does a governance process exist for social media within the organization? ▸ How well are policies related to social media known among employees?
Social media activities audit – Audit the social media activities of the organization and its employees against the policies and procedures in place. Identify new risks and assist in developing policies and controls to address the risks.	▸ Are social media activities aligned to policy? ▸ What corrective actions need to be put in place for any of the activities? ▸ How do existing activities affect brand and reputation?

Opportunities for integrated audits between IT and operational audit *Audit was frequently mentioned in survey of leading IA organizations*

Recommended reading

Protecting and strengthening your brand: social media governance and strategy

www.ey.com/GRCinsights



Social media strategy, policy and governance

www.ey.com/Publication/vwLUAssets/Social_media_strategy_policy_and_governance/$FILE/Social_media_strategy_policy_governance.pdf

Segregation of duties/identity and access management

While segregation of duties (SoD) is considered by many to be a fundamental control that organizations have developed strong processes, the complexity of today's enterprise systems leaves many companies struggling. As the sophistication of tools available to audit firms has increased, new issues and challenges with the systematic enforcement of SoD have come to light.

SoD is top of mind for many professionals, from compliance managers to executive-level officers. The increased interest in SoD is due, in part, to control-driven regulations worldwide and the executive-level accountability for their successful implementation. However, the underlying reason for these regulations is more important: no individual should have excessive system access that enables them to execute transactions across an entire business process without checks and balances. Allowing this kind of access represents a very real risk to the business, and managing that risk in a pragmatic, effective way is more difficult than it seems. If this concept is common sense, why do so many companies struggle with SoD compliance, and why does it repeatedly stifle IT, internal audit and finance departments? In large part, the difficulty rests in the complexity and variety of the systems that automate key business processes, and the ownership and accountability for controlling those processes.

Compounding the problem, a lack of investment in identity access management (IAM) or GRC software often requires finance, IT and audit to manually control SoD risk following a complex and cumbersome process that is prone to error. Manual controls designed to mitigate SoD risks can be time-intensive and costly. Automated SoD controls are more efficient and reliable in optimized control environments.

Many IT audit departments rely on the businesses' review of IT access reports from ERP systems; however, the reality is that many business professionals lack the necessary knowledge of ERP role definitions to truly understand what they are certifying. Therefore, a comprehensive SoD review is an audit that should be on all IT audit plans on a periodic basis.

Recommended reading

A risk-based approach to segregation of duties

www.ey.com/GRCinsights

The audits that make an impact	Key questions to evaluate during audit
Systematic segregation of duties review audit — Evaluate the process and controls IT has in place to effectively manage segregation of duties. Perform an assessment to determine where segregation of duties conflicts exist and compare to known conflicts communicated by IT. Evaluate the controls in place to manage risk where conflicts exist.	▸ How does IT work with the business to identify cross-application segregation of duties issues? ▸ Does business personnel understand ERP roles well enough to perform user access reviews? ▸ While compensating controls identified for SoD conflicts may detect financial misstatement, would they truly detect fraud?
Role design audit — Evaluate the design of roles within ERPs and other applications to determine if inherent SoD issues are embedded within the roles. Provide role design, role cleanup or role redesign advisory assistance and pre- and post-implementation audits to solve identified SoD issues.	▸ Does the organization design roles in a way that creates inherent SoD issues? ▸ Do business users understand the access being assigned to roles they are assigned ownership of?
Segregation of duties remediation audit — Follow up on previously identified external and internal audit findings around SoD conflicts.	▸ Does the organization take appropriate action when SoD conflicts are identified? ▸ Have we proactively addressed SoD issues to prevent year-end audit issues?
IAM/GRC technology assessment — Evaluate how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes.	▸ Is IAM or GRC software currently used effectively to manage SoD risk? ▸ What software could be utilized to improve our level of SoD control, and what are our business requirements?

Data loss prevention and privacy

Over the last few years, companies in every industry sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. A wide range of high-profile data loss incidents have cost organizations millions of dollars in direct and indirect costs and have resulted in tremendous damage to brands and reputations. Many types of incidents have occurred, including the sale of customer account details to external parties and the loss of many laptops, USB sticks, backup tapes and mobile devices, to name a few. The vast majority of these incidents resulted from the actions of internal users and trusted third parties, and most have been unintentional. As data is likely one of your organization's most valuable assets, protecting it and keeping it out of the public domain is of paramount importance. To accomplish this, a number of data loss prevention (DLP) controls must be implemented, combining strategic, operational and tactical measures. However, before DLP controls can be effectively implemented, your organization must understand the answer to these three fundamental questions:

- What sensitive data do you hold?
- Where does your sensitive data reside, both internally and with third parties?
- Where is your data going?

In *Ernst & Young's 2010 Global Information Security Survey,* 81% of executives interviewed indicated that managing privacy and protecting personal data was very important or important to their organization. And no wonder: highly publicized incidents of data leaks or identity theft pose huge brand and reputation risks for businesses. These remain top concerns today. In *Ernst & Young's 2012 Global Information Security Survey,* data leakage and data loss prevention remained ranked as a top three priority for IT and IT security executives. As a result, executives are investing more money to protect the privacy of personal information — to respond to ever-increasing government regulation and enforcement and to stem the rising tide of risk. But are they spending it in the right places? Internal audit is well positioned to help the organization address this question.

Recommended reading

Data loss prevention: keeping your sensitive data out of the public domain

www.ey.com/GRCinsights

Privacy trends 2013: the uphill climb continues

www.ey.com/GRCinsights

The audits that make an impact	Key questions to evaluate during audit
Data governance and classification audit — Evaluate the processes management has put in place to classify data, and develop plans to protect the data based on the classification.	▸ What sensitive data do we hold — what is our most important data? ▸ Where does our sensitive data reside, both internally and with third parties? ▸ Where is our data going?
DLP control review — Audit the controls in place to manage privacy and data in motion, in use and at rest. Consider the following scope areas: perimeter security, network monitoring, use of instant messaging, privileged user monitoring, data sanitation, data redaction, export/save control, endpoint security, physical media control, disposal and destruction, and mobile device protection.	▸ What controls do we have in place to protect data? ▸ How well do these controls operate? ▸ Where do our vulnerabilities exist, and what must be done to manage these gaps?
Privacy regulation audit — Evaluate the privacy regulations that affect the organization, and assess management's response to these regulations through policy development, awareness and control procedures.	▸ How well do we understand the privacy regulations that affect our global business? For example, HIPAA is potentially a risk to all organizations, not just health care providers or payers. ▸ Do we update and communicate policies in a timely manner? ▸ Do users follow control procedures to address regulations?

Three steps to prepare for a HIPAA audit: being unprepared could cost far more than higher civil money penalties. It could cost you your reputation.

www.ey.com/5

Human resources

Organizations are more challenged than ever to attract and retain the best resources while simultaneously attempting to manage costs. The competition for talent has only increased in the turbulent current state economy. Forward-thinking organizations are using innovative talent-management approaches and service delivery structures to gain a competitive advantage, to assist them in riding out the downturn and in creating a strong platform for recovery and growth. This is especially important as organizations look to identify and implement employee cost reduction initiatives while still holding on to and continuing to develop top talent.

This challenge exists in the context of the following global mega trends related to human resources:

- Advancement of global HR and payroll transformation
- Expanding regulation and legislation, including executive regulatory compliance and data privacy requirements
- Alignment of talent with strategic organizational needs
- Focus on remuneration governance and oversight
- Pension funding gap and requirements of FAS 158 reporting

The responsibility to assess and manage the risks associated with these trends resides in many places throughout an organization, but these efforts must be centrally coordinated — under the guidance of the HR function. Key HR-related risks organizations are focused on include:

- **Managing the skills gap** — The risk organizations are most consistently struggling with is the skills gap. In some countries, such as Japan and the US, the gap is driven by an aging workforce, while in other countries the effectiveness of the education system creates challenges. In emerging markets such as Brazil and China the level of growth creates a talent gap that must be filled by importing talent, at higher costs to the organization. Organizations must have a strong plan to manage this strategic risk globally.
- **A mobile workforce** — To meet the skills gap, companies are increasing the mobility of their workforce globally. This creates risk from a reporting and tracking standpoint — do we have the appropriate processes and controls to track our workforce? Do we have frequent business travelers that have become an "accidental expatriate"? More strategically and significantly, companies struggle with how to repatriate their global employees. A formal process must be in place to determine how expatriate employees will return to their home countries so these talented employees do not need to leave the organization to return.
- **Talent management and succession planning** — The risk that organizations deploy informal career and succession planning increases the likelihood that top talent will exit the organization unsure of their future. The need for formality is more important than ever given the skills gap risk that is real for organizations. Additionally, organizations need to be focused on the entire process, from hire to retire.
- **Pension risk** — Organizations continue to focus on managing risk presented from pension plans. Many organizations have developed and executed pension de-risking strategies during the economic downturn. All organizations must ask how they will manage their pension risk, and any action requires consideration of: the impact on workers and the ability to retain talent; investor and credit rating views; and, most importantly, the proper execution of a well-thought-out strategy.
- **A global HR organization** — As organizations become more global than ever and utilize a mobile workforce to address the skills gap, it is critical that HR organizations become more global as well. The risk that different processes exist to manage the workforce becomes a greater risk as more employees move from region to region. Standard processes and controls will help the organization efficiently move members of the HR organization as well as other employees.

Other hot risk topics for HR include traditional payroll (and an ever-changing set of regulatory requirements), data privacy and balancing risk and value creation associated with incentive compensation. As mentioned, it takes a coordinated approach, led by HR, to manage these risks, but internal audit can be a key partner in assisting the organization through the execution of value-add audits.

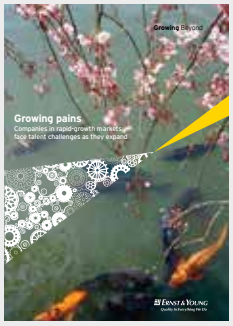
Recommended reading

Managing today's global workforce: elevating talent management to improve business

www.ey.com/GL/en/Issues/Driving-growth/Globalization---Looking-beyond-the-obvious

Growing pains: companies in rapid-growth markets face talent challenges as they expand

www.ey.com/GL/en/Issues/Driving-growth/Growing-pains---Finding-the-right-balance



The audits that make an impact	Key questions to evaluate during audit
Global mobility review – Evaluate the organization's strategy and approach to remain compliant with immigration laws, foreign income tax regulations, social security laws, potential double taxation and "accidental" expatriates. In addition, assess the organization's tracking and reporting capabilities as they relates to mobile employees. More strategically, understand how the organization repatriates employees (formal vs. informal) and what can be done to improve the management of the mobile workforce.	▸ Does the organization have an international assignment policy in place covering all types of assignments offered? ▸ How does the organization address the tax and legal obligations to the business travelers who travel abroad for an extended period of time? ▸ What is the process for monitoring the changes in laws and regulations of host countries? ▸ Do we have the ability, or a plan, to quickly remove expatriate employees in the case of a political crisis or uprising in a foreign country?
● **Talent management process and succession planning audit** – Assess the processes in place to define clear career paths and perform succession planning across the organization. Evaluate whether succession planning occurs consistently and where risk exists that adequate succession plans are not in place. Often a subject matter resource (SMR) is utilized to evaluate the level of maturity associated with these processes and to understand what external best practices can be leveraged to improve processes.	▸ Do formal processes exist for career and succession planning? ▸ How well is succession planning executed globally? ▸ What best practices exist across the organization or externally that can be leveraged to improve processes? ▸ What are the company's key performance indicators for talent management purposes? ▸ Does the company have succession strategies for areas affected by retirement or skill shortages?
● **Culture audit** – This is an innovative audit that internal audit organizations have started to partner with HR to complete. This allows organizations to assess the organization's cultural characteristics (e.g., open, honest, listen and accountable) and how deeply embedded the characteristics are throughout the organization globally. One technique that can be used is a survey of the organization's workforce, allowing them to provide direct feedback on different categories impacted by culture (e.g., compensation, ethics, communication). Beyond the survey, internal audit will often assess the processes HR has in place to proactively understand cultural characteristics of the organization, manage and develop those characteristics and share this information with executive management so it is considered in key decisions.	▸ What culture categories are important to the organization and how does it measure their success? ▸ How does our culture compare with those of our competitors? ▸ How is our culture helping us achieve our strategic goals? How is it hindering us and what is the mechanism to mitigate our culture gap? ▸ How do we proactively understand and manage our culture?
Incentive compensation audit – Evaluate the process for fairly and adequately compensating the employees of the organization. Determine if the compensation practices align with the company's strategic objectives and a correlation exists between the incentive period and the time horizon of the organization's underlying risks.	▸ What is the company's definition of an acceptable risk threshold? ▸ Do the current performance metrics encourage excessive or inappropriate risk-taking by employees that could have a material adverse effect on the company? ▸ What risk mitigation features are built into the current incentive compensation programs and policies?
Affordable Care Act compliance review – The internal audit team focuses on the organization's finance, human resources, information technology and tax functions' approach to compliance with the Affordable Care Act (ACA). The internal audit team reviews the company's understanding of its obligations under the ACA, as well as the processes to adhere to its reporting requirements. There is a focus on the tax process and the controls in place to mitigate the potential liabilities that the ACA imposes for noncompliance.	▸ Who at our organization is responsible for adherence with the ACA? ▸ What requirements does our organization face under the ACA? ▸ What is the company's approach to meet the compliance deadline of 1 January 2014?

● *Audit was frequently mentioned in survey of leading IA organizations*

Supply chain and operations

The economic downturn and lack of meaningful growth in developed markets has many organizations searching for ways to not only improve their margins, but also seek additional growth opportunities, primarily in emerging markets. As a result of this trend, expectations and demands of the organization's supply chain have increased significantly. Supply chain functions are increasingly being asked to:

- Reassess their strategy to support management's mandate to increase shareholder value
- Reduce costs to enable margin growth in developed markets
- Be the engine for growth in emerging markets

Companies are able to meet these mandates by focusing on the supply chain agenda:

- Optimizing global spend
- Improving operational agility and responsiveness
- Managing environmental and sustainability expectations
- Establishing an effective supply chain model and infrastructure
- Enabling new revenue sources
- Managing operational, tax and regulatory risks
- Reconfiguring the supply chain to create cost competitiveness

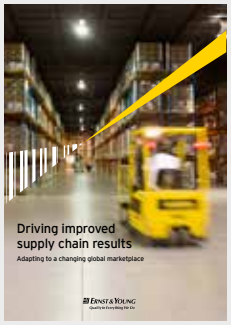
In a stagnant economy that is more difficult than ever to predict, companies are focusing on developing strong sales and operations planning (S&OP) processes to adjust production to customer demand in a more dynamic way. We have also seen much more focus on supplier collaboration, as well as procurement transformation focused on making the organization's procurement function a true business partner. Given this context, key risks in the areas of supply chain and operations include the following:

- **A lack of integration between sales, supply chain and operations** — Where sales and operations are disconnected, the risk that what is produced will not mirror customer demand is increased. The level of rigor required to integrate sales, pricing, supply chain, procurement and operations is extensive and must be supported by strong executive support, policies and procedures and audits to ensure the sustainability of processes.
- **Procurement risk** — The variety of risks related to procurement continues to be a top priority for organizations. Key risks within the procurement function include the following:
  - Conflicts of interest with suppliers, anti-corruption and fraud
  - Failure to diversify the supply base, resulting in interruption of the supply chain when preferred suppliers cannot deliver
  - Poor supplier risk management and evaluation of supplier capabilities prior to negotiation
  - A focus on material cost as opposed to total cost of the supplier relationship
  - Failure to segment suppliers based on clearly defined criteria to determine the characteristics of the supplier relationship
  - Poor negotiations and contract management that exposes the company to raw material price changes and other risks
  - Keeping up with evolving regulatory compliance
  - Failing to take advantage of low-cost country supply bases, resulting in excess costs for the organization
- **Failure to achieve operational efficiencies and productivity gains** — Organizations are continuously trying to improve operations and focus on areas such as waste and overall equipment effectiveness (OEE) to achieve productivity gains. Poor governance or a lack of standards can prevent organizations from achieving these gains. Utilizing the right tools, techniques and metrics to engage the workforce and sustain improvements is a significant focus area for many organizations.
- **Environmental health and safety (EH&S)** — Beyond complying with always-evolving EH&S requirements, organizations are focused on ensuring that capital spend related to EH&S truly generates a return and that the right metrics are monitored to proactively measure EH&S performance.
- **Transportation and logistics** — For many organizations, transportation and logistics costs are significant, and poor transparency to these costs is a common challenge. In some industries, optimizing logistics networks can result in significant cost reductions. In other organizations, simply having visibility of costs across the organization leads to gains, by providing a clear view of a supplier's total cost and better information for negotiations.

Recommended reading

Driving improved supply chain results: adapting to a changing global marketplace

www.ey.com/GL/en/Services/Advisory/Performance-Improvement/Supply-Chain/Driving-improved-supply-chain-results--adapting-to-a-changing-global-marketplace---Improve-margins-in-mature-markets



The DNA of the COO: time to claim the spotlight

www.ey.com/US/en/Careers/EY-Faculty-Connection-Issue-38---3---DNA-of-the-COO

The audits that make an impact	Key questions to evaluate during audit
Waste audit – This audit focuses on confirming waste reported at the plants is accurate and complete. The efficiency and consistency of reporting processes are evaluated as well as the physical control and safeguarding of waste. More strategically, the operations are evaluated to determine common root causes for waste, and tools and techniques to manage waste are evaluated. Finally, the metrics used by the organization to monitor and measure waste are evaluated. This audit often uses an a SMR familiar with operations.	▸ Are the waste numbers reported from plants accurate and complete? ▸ What is already being done to reduce waste in the plants and could anything be done differently? ▸ Are we monitoring the right metrics related to waste? What incentive plans could be used to influence employee behavior? ▸ Is waste being disposed of without being reported?
Supplier risk management assessment – Review the policies, process and internal controls that procurement has in place for supplier risk management to evaluate global suppliers of the organization. Evaluate the decision processes followed for sole source suppliers, as well as the change management process followed to transition business from one vendor to another.	▸ How consistent is the global supplier risk management process? ▸ How embedded is the process in the organization and what functions outside of procurement participate? ▸ Are risk management processes in place for both direct and indirect vendors?
Transportation and logistics audit – This assessment focuses on the processes management has in place to evaluate the procurement of transportation and logistics vendors as well as how transportation and logistics spend is managed. Evaluate how well management optimizes transportation and logistics to reduce spend. Also included in this audit would be an evaluation of import/export regulations and management's ability to comply with varied regulations.	▸ How efficiently are transportation and logistics costs managed? ▸ Are there opportunities for global consistency that would reduce costs? ▸ Are negotiated transportation and logistics agreements followed? ▸ What processes and controls are in place to comply with related regulations?
Sales and operations planning – Evaluate the organizations procedures to integrate sales, supply chain and operations in the S&OP process. Assess compliance with all procedures and identify best practices or inconsistencies globally that can be shared to improve the process. Identify opportunities for increased integration.	▸ How well are sales, supply chain and operations integrated to tailor production to customer needs and forecasts? ▸ Do formal policies and procedures exist? Where are procedures not being followed? ▸ What controls are in place to ensure the sustainability of processes? ▸ Do inconsistencies exist globally or are there best practices that can be shared globally?
Contract management – Evaluate the contract management process specific to contracting with vendors. Assess the processes in place to monitor compliance with contracts (both vendor and internal compliance), how changes in contracts are managed and the approval process for new contracts. Significant supply agreements may be chosen for this audit.	▸ Do we have strong controls in place to ensure contracts receive the right approvals? ▸ How is compliance with terms and conditions monitored? ▸ Are prices on purchase orders accurate, particularly if pricing is tied to indices or volume discounts can be achieved?

Audit was frequently mentioned in survey of leading IA organizations

See also risks and audits related to business continuity, on page 19.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of 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 www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 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 superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific 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 the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. AU1607

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

ED 0114

How Ernst & Young makes a difference

At Ernst & Young, our services focus on our clients' specific business needs and issues because we recognize that these are unique to that business.

Effective risk management is critical to helping modern organizations achieve their goals and it offers the opportunity to accelerate performance while protecting against the uncertainties, barriers and pitfalls inherent in any business. Integrating sound risk management principles and practices throughout operational, financial and even cultural aspects of the organization can provide a competitive advantage in the market and drive cost-effective risk processes internally.

Our 15,000 Risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective support – wherever you are in the world. We work with you to develop an integrated, holistic approach to managing risk and can provide resources to address specific risk issues. We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contact details of our leaders

Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Randall J. Miller	+1 312 879 3536	randall.miller@ey.com
Areas		
Americas		
Brian M. Schwartz	+1 410 783 3885	brian.schwartz@ey.com
Michael L. Herrinton	+1 703 747 0935	michael.herrinton@ey.com
Bernard R. Wedge	+1 404 817 5120	bernard.wedge@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Manuel Giralt Herrero	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Asia-Pacific		
Jenny S. Chan	+86 21 2228 2602	jenny.s.chan@cn.ey.com
Rob Perry	+61 3 9288 8639	rob.perry@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp
Haruyoshi Yokokawa	+81 3 3503 2846	yokokawa-hrysh@shinnihon.or.jp

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**