

Insights on
governance, risk
and compliance

February 2013


Ten key IT considerations for internal audit

Effective IT risk assessment
and audit planning

Contents

Introduction.....	2
Information security	4
Business continuity management.....	6
Mobile	8
Cloud.....	10
IT risk management	12
Program risk.....	14
Software/IT asset management	16
Social media risk management.....	18
Segregation of duties/identity and access management.....	20
Data loss prevention and privacy.....	22
Conclusion.....	24





Identifying and addressing risk is singularly one of an organization's most important duties for its employees, shareholders, suppliers and customers. Considerations related to information technology are central to any organization's effort to ensure that issues are addressed quickly and thoroughly.

The jagged economic landscape – complicated by advancing technologies, such as cloud, social media and mobile devices – can challenge the ability of an IT internal audit to provide comfort to executives already overwhelmed with rapidly expanding opportunities and pressures caused by shrinking margins.

Further, considerations around continuity management, information security, regulatory compliance and the execution of major complex programs can also muddy the waters, reducing executives' clarity and limiting an organization's ability to address risk and, ultimately, grow.

Regardless of the rigor of a strong risk assessment process, audit leadership is often left with lingering questions: What did we miss? What audits best address our risks? How should we answer questions that might be posed from the audit committee about how we are addressing a specific risk?

Helping to provide clarity, this thought leadership lists 10 considerations to consider related to information technology. Knowing these considerations, sharing and discussing them with clients and mapping out a strategy to make sure they are addressed is a simple, yet crucial step toward generating confidence that the IT audit function is doing its job. Armed with strong data and new technology, and leveraging leading practices and strong collaboration with the organization's risk function, IT internal audit executives can use this list to help enrich clients' understanding of the dangers that could imperil their very survival, and build a strategic plan to address them.

As you execute your own risk assessment, and ultimately develop the audit plan, consider the following IT considerations and audit topics. Our hope is this information will allow you to perform a more effective risk assessment and create a robust annual audit plan.

Introduction



Increasing quality and confidence in the IT internal audit risk assessment

Ernst & Young's recent thought leadership and research publication *Turning risks into results: how leading companies use risk management to fuel better performance* indicates that organizations achieve results from risk in three interrelated ways:

1. Some companies focus on mitigating overall enterprise risk
2. Others focus on efficiency, reducing the overall cost of controls
3. Still others look to create value, often through a combination of risk mitigation and cost reduction



Increasing your level of confidence in the risk assessment process is one of the most fundamental ways to focus on mitigating overall enterprise risk, determining appropriate levels of effort and resources and identifying where to add value. In a worst-case scenario, an organization's risks can proliferate at a far faster rate than its ability to provide coverage. Organizations need to have the ability to identify and address key risk areas and the agility to quickly close the gaps through:

- ▶ Identifying and understanding the "risks that matter"
- ▶ Differentially investing in the risks that are "mission critical" to the organization
- ▶ Effectively assessing risks across the business and driving accountability and ownership
- ▶ Demonstrating the effectiveness of risk management to investors, analysts and regulators

As many organizations prepare for risk assessment discussions, consider our perspective on the leading practices that will help increase your organization's level of confidence in addressing these critical questions:

- ▶ How do we look around the corner?
- ▶ How do we know we identified all the right risks?

As many companies face considerations in their internal audit processes, thoughtful executives will need to understand which IT trends to consider in their critical internal audit plans, including which of the following IT risk assessment techniques apply to their organizations' respective challenges and assessment needs. The 10 key IT internal audit considerations outlined in this paper are aligned with, and provide connection to, leading practices designed to help ensure robust performance in the IT internal audit process.

What increases confidence in the IT internal audit risk assessment?

- ▶ Diversity in data, stakeholders and participants leads to greater risk insight
- ▶ Technology, used in the right way, is a game changer
- ▶ Making the assessment process collaborative and embedded within the business

Techniques of IT risk assessment

Data and inputs reviewed

Data analytics

Stakeholder engagement

Interview/survey techniques

Collaboration

Audit prioritization

Outputs



IT risk assessment techniques: leading practices

Basic versus leading practice IT risk assessment techniques to consider

Basic	Degree of confidence		Leading
	Low	High	
<ul style="list-style-type: none"> IT Internal audit issues IT Sarbanes-Oxley (SOX) and external audit issues 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> Root causes from past IT issues Competitor and peer risks Industry trends Third-party external IT risk data Analyst reports
<ul style="list-style-type: none"> Analytics run but limited summarization of data Business and IA leadership struggle to spot trends in data 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> Risk analytics based on most critical questions IT, business and IA need to answer Trending and period-to-period comparisons can identify emerging risks or changes to existing risks Efforts aligned with other "big data" initiatives
<ul style="list-style-type: none"> Focus on IT stakeholders Heavy emphasis on "home office" stakeholders Point in time engagement primarily during annual IT risk assessment IT and business leaders not trained on risk management 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> Includes operational and global stakeholders beyond IT Risk management embedded in IT leadership training Risk scenario planning workshops for significant IT risks Continuous dialogue with stakeholders (monthly, quarterly meetings) Risk committee utilized to review risk assessment changes
<ul style="list-style-type: none"> Inconsistent documentation of interviews Surveys used for SOX 302 certification purposes or not at all 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> IT subject matter resources participating in select interviews to draw out key risks Surveys used to confirm risk assessment results with lower-level IT management not interviewed Stakeholders self-assessing risk based on IT governance, risk and compliance (GRC) solution containing dynamic risk database
<ul style="list-style-type: none"> IT internal audit attending interviews with little participation from other risk management functions or operational audit IT risk assessment viewed as "IT internal audit's risk assessment" 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> IT risk assessment collaboratively developed by internal audit (operational and IT) and other risk management functions and IT SOX, external audit and other risk management functions participating in interviews Risk assessment embedded within strategic planning process
<ul style="list-style-type: none"> Impact and likelihood utilized for prioritization Audits prioritization based heavily on IT competencies available in IA department 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> Categorize IT risks within each of following: availability, confidentiality, integrity, effectiveness and efficiency Relevance to strategic objectives utilized to prioritize IT risks Audits executed based on value to organization and connection to strategic objectives
<ul style="list-style-type: none"> Relatively static internal audit plan 	● ● ● ● ●	● ● ● ● ●	<ul style="list-style-type: none"> Dynamic IT internal audit plan that changes throughout the year and is reset at selected milestones (e.g., quarter, trimester, bi-annually) IT internal audit plan addressing unified framework of all IT compliance needs beyond just SOX (e.g., PCI, FISMA, HIPAA, ISO27001) External IT audit plan and internal audit reliance strategy integrated and optimized

Information security



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.

Recommended reading

*Fighting to close the gap:
Ernst & Young's 2012 Global
Information Security Survey*

www.ey.com/giss2012





The audits that make an impact	Key IT internal audit considerations
<p>Information security program assessment – Evaluates the organization’s information security program, including strategy, awareness and training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies and reporting.</p>	<ul style="list-style-type: none"> ▶ How comprehensive is the existing information security program? ▶ 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?
<p>Threat and vulnerability management program assessment – Evaluates the organization’s threat and vulnerability management (TVM) program including threat intelligence, vulnerability identification, remediation, detection, response, and countermeasure planning.</p>	<ul style="list-style-type: none"> ▶ How comprehensive is the existing TVM program? ▶ 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 make sure identified issues are appropriately addressed and remediation is effective?
<p>Vulnerability assessment – 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.</p>	<ul style="list-style-type: none"> ▶ 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?

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 2011 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. These big disasters, as well as the 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, thus IT internal audit is well positioned to evaluate broader BCM procedures.

Recommended reading

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

<http://www.ey.com/GL/en/Services/Advisory/Integrated-governance---effective-business-continuity-management---Ready-for-the-challenge>





The audits that make an impact	Key IT internal audit considerations
<p>Business continuity program integration and governance audit – Evaluates the organization’s overall business continuity plan, including program governance, policies, risk assessments, business impact analysis, vendor/third-party assessment, strategy/plan, testing, maintenance, change management and training/awareness.</p>	<ul style="list-style-type: none"> ▶ Does a holistic business continuity plan exist for the organization? ▶ How does the plan compare to leading practice? ▶ Is the plan tested?
<p>Disaster recovery audit – Assesses IT’s ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.</p>	<ul style="list-style-type: none"> ▶ Are disaster recovery plans aligned with broader business continuity plans? ▶ Do testing efforts provide confidence systems that can be effectively recovered? ▶ Are all critical systems included? Are critical systems defined?
<p>Crisis management audit – Reviews the organization’s crisis management plans, including overall strategy/plan, asset protection, employee safety, communication methods, public relations, testing, maintenance, change management and training/awareness.</p>	<ul style="list-style-type: none"> ▶ Are crisis management plans aligned with broader business continuity plans? ▶ Are plans comprehensive and do they involve the right corporate functions? ▶ Are plans well communicated?

Opportunities for integrated audits between IT and operational audit

Mobile



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 come new challenges for the enterprise, including:

- ▶ Potential loss or leakage of important business information
- ▶ Security challenges given 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.

Recommended reading

*Mobile device security:
understanding vulnerabilities
and managing risk*

http://www.ey.com/GL/en/Services/Advisory/Advisory-Services_Information-Security-Services





The audits that make an impact	Key IT internal audit considerations
<p>Mobile device configuration review – Identifies 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.</p>	<ul style="list-style-type: none"> ▶ How has the organization implemented “bring your own device” (BYOD)? ▶ Are the right policies/mobile strategies in place? ▶ Are mobile devices managed in a consistent manner? ▶ Are configuration settings secure and enforced through policy? ▶ How do we manage lost and stolen devices? ▶ What vulnerabilities exist, and how do we manage them?
<p>Mobile application black box assessment – Performs audit using different front-end testing strategies: scan for vulnerabilities using various tools, and manually verify scan results. Attempts to exploit the vulnerabilities identified in mobile web apps.</p>	<ul style="list-style-type: none"> ▶ What vulnerabilities can be successfully exploited? ▶ How do we respond when exploited, and do we know an intrusion has occurred?
<p>Mobile application gray box assessment – Combines traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical areas of functionality and for symptoms of common poor coding practices. Each of these “hot spots” in the code should be linked to the live instance of the application where manual exploit techniques can verify the existence of a security vulnerability.</p>	<ul style="list-style-type: none"> ▶ How sound is the code associated with the mobile applications used within the organization? ▶ What vulnerabilities can be exploited within the code?

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 using 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 they're 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 performing as needed to meet 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

<http://www.ey.com/GL/en/Industries/Technology/Cloud-computing-issues---impacts-and-insights---A-fundamental-shift-in-the-industry>





The audits that make an impact	Key IT internal audit considerations
<p>Cloud strategy and governance audit – Evaluates the organization’s strategy for utilizing cloud technologies. Determines whether the appropriate policies and controls have been developed to support the deployment of the strategy. Evaluates alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organization.</p>	<ul style="list-style-type: none"> ▶ Is there a strategy around the use of cloud providers? ▶ Are there supporting policies to follow when using a cloud provider? Are policies integrated with legal, procurement and IT policies?
<p>Cloud security and privacy review – Assesses 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. Determines whether IT management worked to negotiate security requirements into their contract with the provider. Reviews procedures for periodic security assessments of the cloud provider(s), and determine what internal security measures have been taken to protect company information and data.</p>	<ul style="list-style-type: none"> ▶ Has a business impact assessment been conducted for the services moving to the cloud? ▶ Does your organization have secure authentication protocols for users working in the cloud? ▶ Have the right safeguards been contractually established with the provider?
<p>Cloud provider service review – Assesses 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.</p>	<ul style="list-style-type: none"> ▶ What SLAs are in place for uptime, issue management and overall service? ▶ Has the cloud provider been meeting or exceeding the SLAs? What issues have there been? ▶ Does the organization have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units?

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, elevating the need for boards of directors, audit committees, general counsels and chief risk officers 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 critically important 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 for the company through reviewing IT risk management activities.

Recommended reading

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

<http://www.ey.com/GL/en/Services/Advisory/Technology-risk-management-in-a-cyber-world--a-C-suite-responsibility-Whats-the-fix>





The audits that make an impact	Key IT internal audit considerations
<p>IT risk management strategy assessment – Assesses the framework and process IT has embedded within the function to assess and manage risks. Evaluates the actions taken to mitigate risks and the level of accountability within the process.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>IT governance audit – Evaluates the processes IT has in place to govern capital allocation decisions, project approvals and other critical decisions.</p>	<ul style="list-style-type: none"> ▶ Do formalized processes for governing 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?
<p>IT risk assessment – Participates in IT's own risk assessment (as opposed to the independent IT internal audit risk assessment) as an advisory audit. Evaluates the risks identified and provide insight given your unique perspective on the IT organization.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Technology enablement/GRC package selection – Evaluates the organization's current use of GRC software or GRC software selection process. Provides value-added insight on critical business requirements.</p>	<ul style="list-style-type: none"> ▶ 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?

Program risk



Program complexity is increasing at a faster rate than companies can adapt. While companies have been cautious with IT investments over the last few years, investment portfolios are now being expanded to keep up with emerging technology trends or to master costly legacy issues.

Gartner predicts an increase in IT spending will be sustained at an average rate of 5.3% per year through 2015.¹ 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 struggle to deliver on their large IT programs. Most programs do not come in on budget, are delivered too late or do not meet their objectives.

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.

¹ Source: *Building confidence in IT programs: facilitating success through program risk management*, Ernst & Young, 2011.

Recommended reading

Strategy deployment through portfolio management: a risk-based approach

<http://www.ey.com/GL/en/Services/Advisory/Strategy-deployment-through-portfolio-management-Portfolio-management-challenges>





The audits that make an impact	Key IT internal audit considerations
<p>Project management methodology audit – Assesses the design of processes and controls in place to manage projects against leading practices.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Project and program execution audit – Evaluates 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.</p>	<ul style="list-style-type: none"> ▶ Is project/program management methodology being followed correctly? ▶ What is done when projects are under-performing? ▶ How is project risk assessed and managed?
<p>Portfolio risk review – Reviews 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.</p>	<ul style="list-style-type: none"> ▶ Do the right governance processes exist to provide that projects/programs align to company strategy? ▶ How is the portfolio managed as corporate objectives change?

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 make a significantly 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 that rely on IT functions.

It is critical that IT auditors thoroughly understand software and IT asset management processes and controls. 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.

Recommended reading

Effective software asset management: how to reap its benefits

<http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>

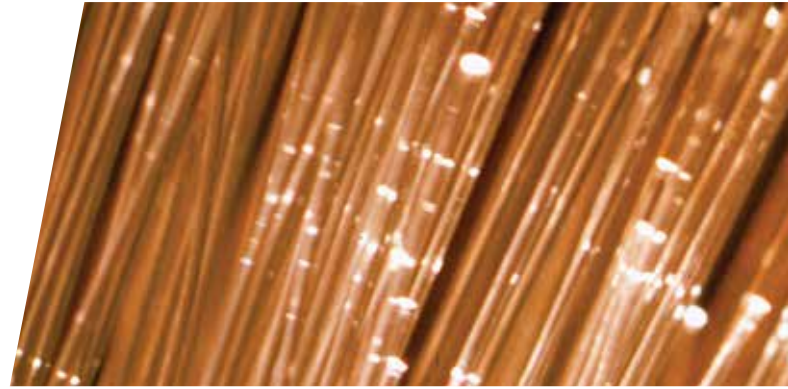




The audits that make an impact	Key IT internal audit considerations
<p>IT and software asset management process and control audit – Assesses the design and effectiveness of processes and controls IT has deployed related to software and IT asset management. Reviews the impact of these processes on related IT processes such as IT service management, IT contract management and information security.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Software license review – Performs a review of significant software license agreements (e.g., ERPs) and evaluate the effectiveness of IT’s software asset management process in practice. Assesses opportunities for cost reduction from improving the management of software licenses.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>IT contract management assessment – Evaluates the IT organization’s ability to manage contracts and how effectively IT and supply chain coordinate to manage costs and negotiate effective agreements.</p>	<ul style="list-style-type: none"> ▶ 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

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 posts
- ▶ 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

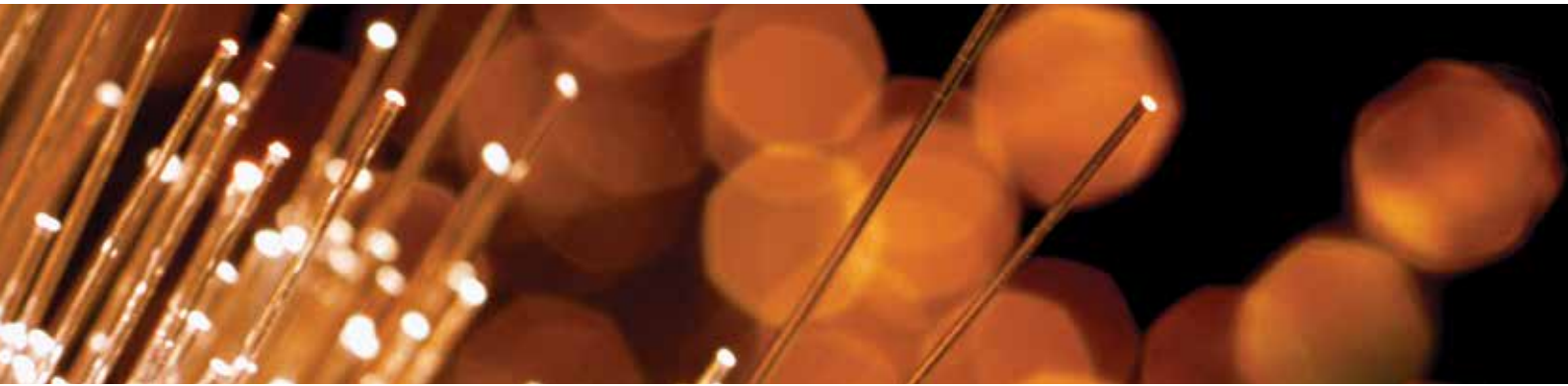
IT is heavily relied on to enable social media strategies in coordination with marketing strategies. It is critical that IT internal audit has an understanding of the organization’s social media strategy as well as the related IT risk. IT internal audit must add value by providing leading practice enhancements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

Recommended reading

Protecting and strengthening your brand: social media governance and strategy

<http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>





The audits that make an impact	Key IT internal audit considerations
<p>Social media risk assessment – Collaborates with the IT organization to assess the social media activities that would create the highest level of risk to the organization. Evaluates 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.</p>	<ul style="list-style-type: none"> ▶ Does the organization understand what risks exist related to social media? ▶ How well are the identified risks managed?
<p>Social media governance audit – Evaluates the design of policies and procedures in place to manage social media within the organization. Reviews policies and procedures against leading practices.</p>	<ul style="list-style-type: none"> ▶ Does a governance process exist for social media within the organization? ▶ How well are policies related to social media known amongst employees?
<p>Social media activities audit – Audits the social media activities of the organization and its employees against the policies and procedures in place. Identifies new risks and assist in developing policies and controls to address the risks.</p>	<ul style="list-style-type: none"> ▶ Are social media activities aligned to policy? ▶ What corrective actions need to be put in place given activity? ▶ How does existing activity affect brand and reputation?

Opportunities for integrated audits between IT and operational audit

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 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 internal audit plans on a periodic basis.

Recommended reading

A risk-based approach to segregation of duties

<http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>





The audits that make an impact	Key IT internal audit considerations
<p>Systematic segregation of duties review audit – Evaluates the process and controls IT has in place to effectively manage segregation of duties. Performs an assessment to determine where segregation of duties conflicts exist and compare to known conflicts communicated by IT. Evaluates the controls in place to manage risk where conflicts exist.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Role design audit – Evaluates the design of roles within ERPs and other applications to determine whether inherent SoD issues are embedded within the roles. Provides role design, role cleanup or role redesign advisory assistance and pre- and post-implementation audits to solve identified SoD issues.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Segregation of duties remediation audit – Follows up on previously identified external and internal audit findings around SoD conflicts.</p>	<ul style="list-style-type: none"> ▶ Does the organization take appropriate action when SoD conflicts are identified? ▶ Have we proactively addressed SoD issues to prevent year-end audit issues?
<p>IAM/GRC technology assessment – Evaluates how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes.</p>	<ul style="list-style-type: none"> ▶ 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 *Fighting to close the gap: Ernst & Young's 2012 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 – a trend that continues today as 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

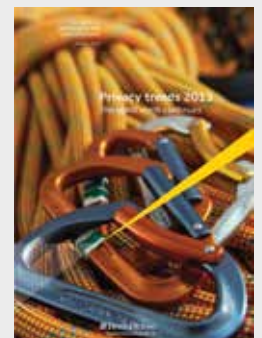
Data loss prevention: keeping your sensitive data out of the public domain

<http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>



Privacy trends 2013: the uphill climb continues

<http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>





The audits that make an impact	Key IT internal audit considerations
<p>Data governance and classification audit – Evaluates the processes management has put in place to classify data, and develop plans to protect the data based on the classification.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>DLP control review – Audits the controls in place to manage privacy and data in motion, in use and at rest. Considers 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.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Privacy regulation audit – Evaluates the privacy regulations that affect the organization, and assess management's response to these regulations through policy development, awareness and control procedures.</p>	<ul style="list-style-type: none"> ▶ 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?

Conclusion

Understanding the risks addressed in this thought leadership, sharing, and discussing them with clients and mapping out a strategy to make sure they are addressed is a simple, yet crucial step toward IT internal audit performance success. Coupled with strong data, new technology, global leading practices and strong collaboration with the organization's risk function, IT internal audit executives can use this list to help provide their clients' organizations with competitive advantage.



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.

© 2013 EYGM Limited.
All Rights Reserved.

EYG no. AU1458



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.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

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**

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 Giralte 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

