



The Institute of
Internal Auditors
Indonesia

2014 ACIIA CONFERENCE BALI, INDONESIA

ASIAN CONFEDERATION OF INSTITUTE OF INTERNAL AUDITORS

The Stones Hotel - Legian, Bali

24 - 25 November 2014

Organized by:



Supported by:



A light purple silhouette of a person in a dynamic, expressive pose, possibly a dancer or performer, with one arm raised and the other extended. The silhouette is positioned on the left side of the slide, partially overlapping the white background and the blue curved border at the bottom.

TC1: Mitigation of Technology Risks for Internal Auditors

Isnaeni Achdiat

**Partner, EY
President, ISACA Indonesia**



Contents

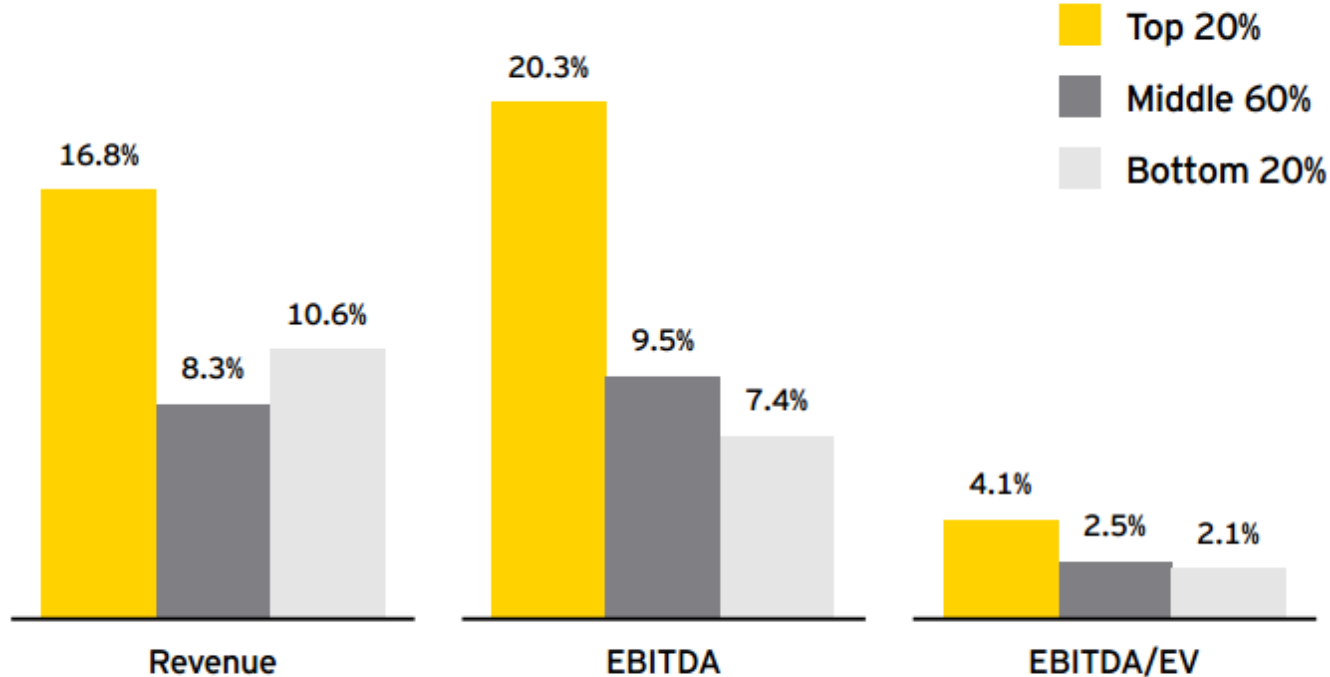
- 1. Turning risk into result - Survey**
- 2. Realizing strategic alignment of the Internal Audit function**
- 3. IT Audit plan and risk assessment process**
- 4. Ten key IT considerations for internal**



Mature risk management drives financial results

In our extensive experience with our clients, we see that companies with more mature risk management practices outperform their peers financially. Our research suggests this translates to competitive advantage: we found that companies with more mature risk management practices generated the highest growth in revenue, EBITDA and EBITDA/EV.

Compound annual growth rates 2004-11* by risk maturity level



* 2011 YTD reported as of 18 November 2011.



Summary of key findings

Using a global, quantitative survey (based on 576 interviews with companies around the world and a review of more than 2,750 analyst and company reports), we assessed the maturity level of risk management practices and then determined a positive relationship between risk management maturity and financial performance. We identified the leading risk management practices that differentiated the various maturity levels and organized them into specific risk components.

Our **findings** suggest that:

- **The top-performing companies** (from a risk maturity perspective) **implemented on average twice as many of the key risk capabilities** as those in the lowest-performing group.
- Companies in the **top 20% of risk maturity generated three times** the level of EBITDA as those in the bottom 20%.
- Financial performance is **highly correlated** with the **level of integration** and **coordination across risk, control and compliance functions**.
- **Effectively harnessing technology** to support risk management is the **greatest weakness or opportunity** for most organizations



What differentiates top performers?

The RISK Agenda: research study leading practices

Enhance risk strategy

- ▶ Organizations conduct two-way, open communications about risk with external stakeholders.
- ▶ Communication is transparent and timely, providing stakeholders with the relevant information that conveys the decisions and values of the organization.
- ▶ The board or management committee plays a leading role in defining risk management objectives.
- ▶ A common risk framework has been adopted and implemented across the organization.

Embed risk management

- ▶ There is a formal method for defining acceptable levels of risk within the organization.
- ▶ Stress tests are used to validate risk tolerances.
- ▶ Leadership has put in place an effective risk management program.
 - ▶ Planning and risk reporting cycles are coordinated so that current information about risk issues is incorporated into business planning.

**Turning
risk into
results**

Improve controls and processes

- ▶ Lines of business have established key risk indicators (KRIs) that predict and model risk assessment.
- ▶ Self-assessment and other reporting tools are standardized across the business.
- ▶ Controls have been optimized to improve effectiveness, reduce costs and support increased business performance.
- ▶ Key risk and control metrics have been established and updated to address impacts on the business.

Optimize risk management functions

- ▶ Completion of risk-related training is incorporated into individual performance.
- ▶ Risk monitoring and reporting tools are standardized across the organization.
- ▶ Integrated technology enables the organization to manage risk and eliminates or prevents redundancy and lack of coverage.
- ▶ The reporting system notifies all stakeholders affected by a risk, not just those in the function or area where the risk was identified.

Enable risk management

- ▶ Issue tracking, monitoring and reporting are regularly performed using GRC software.
- ▶ Risk identification and assessment are regularly performed using GRC software.

Communicate risk coverage

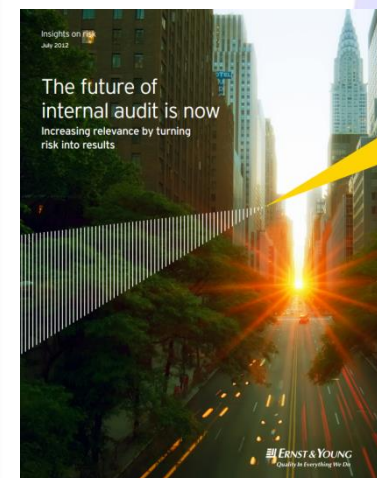
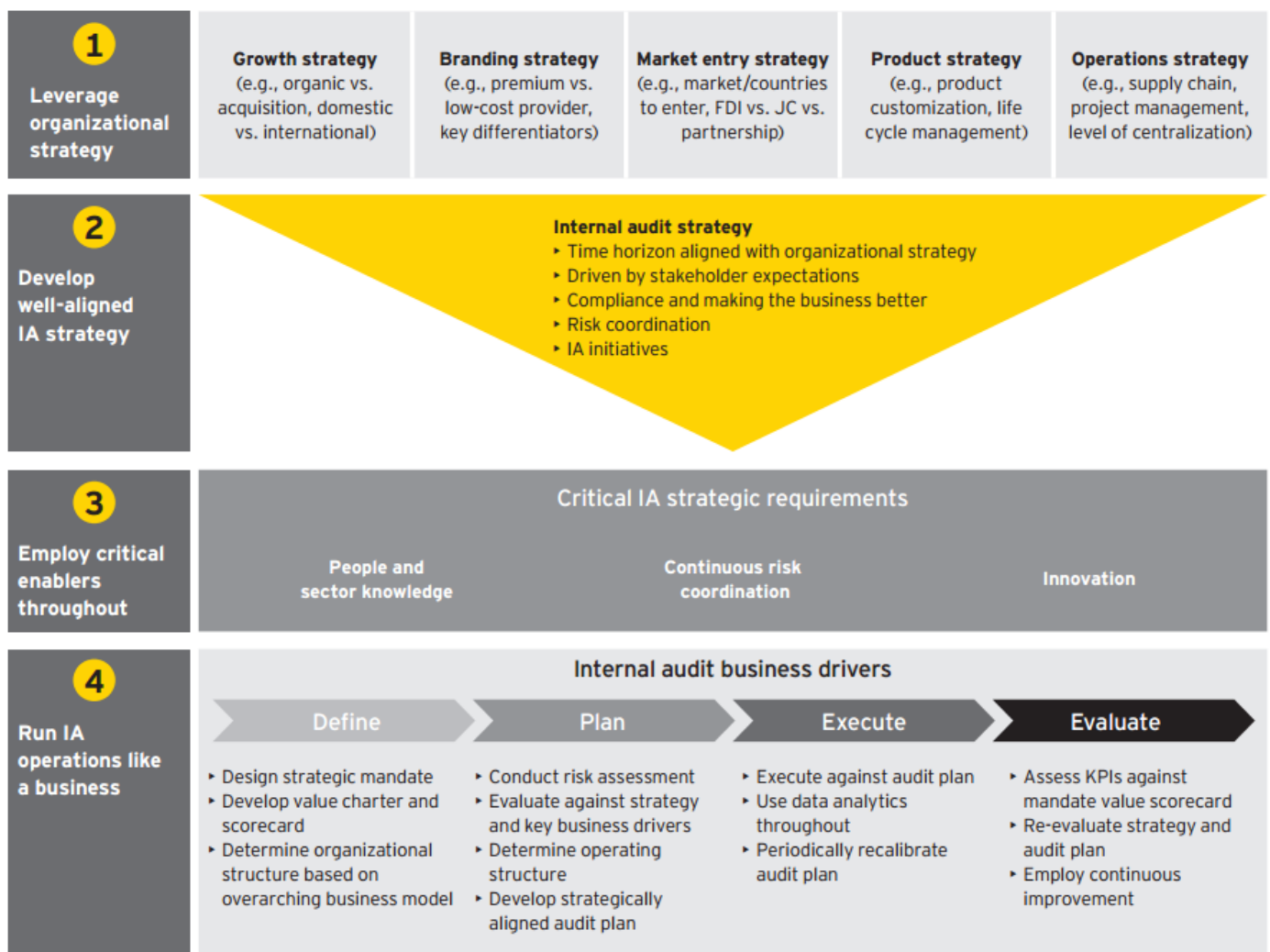
- ▶ Organizations talk about their risk management and control framework in their annual report.
- ▶ Organizations provide assurance to their customers and other stakeholders using independent reports (e.g., SOCR).

Our study found that while most organizations perform the basic elements of risk management, the top performers do more. We found specific risk practices that were consistently present in the top performers (i.e., top 20% based on risk maturity) that were not present in the bottom 20%. These risk practices can be organized into the following challenge areas, as depicted in the chart opposite.

Our study findings suggest that these components are critical to transforming risk and driving better business performance



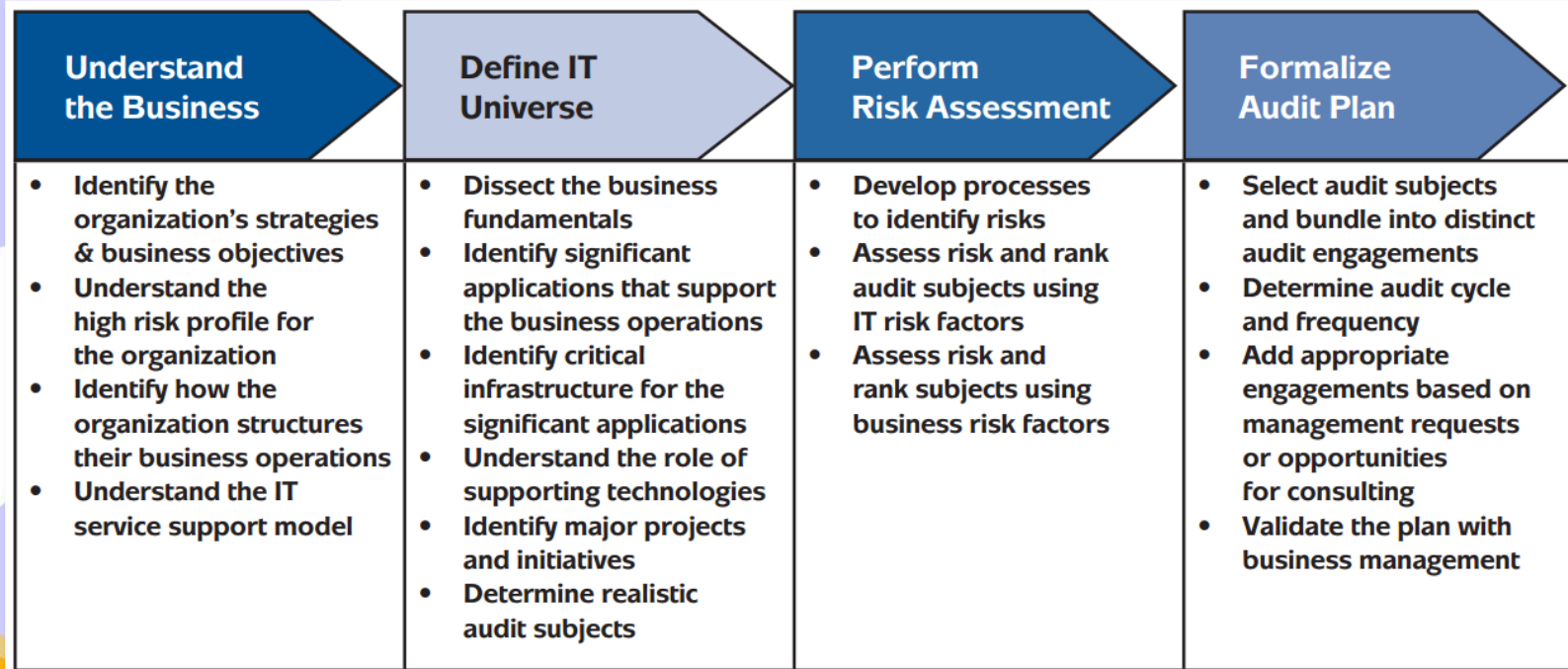
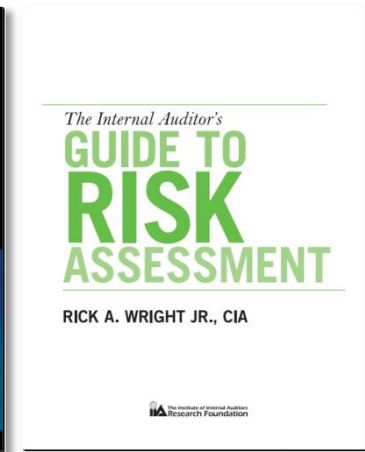
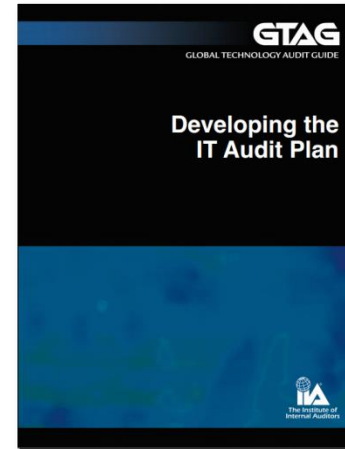
Realizing strategic alignment of the Internal Audit function



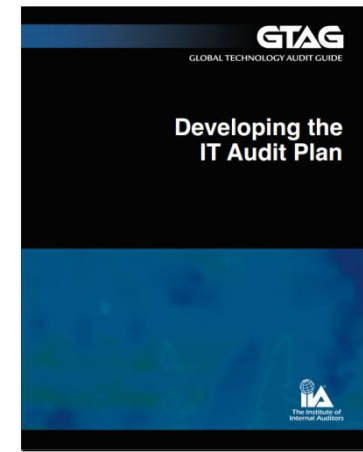
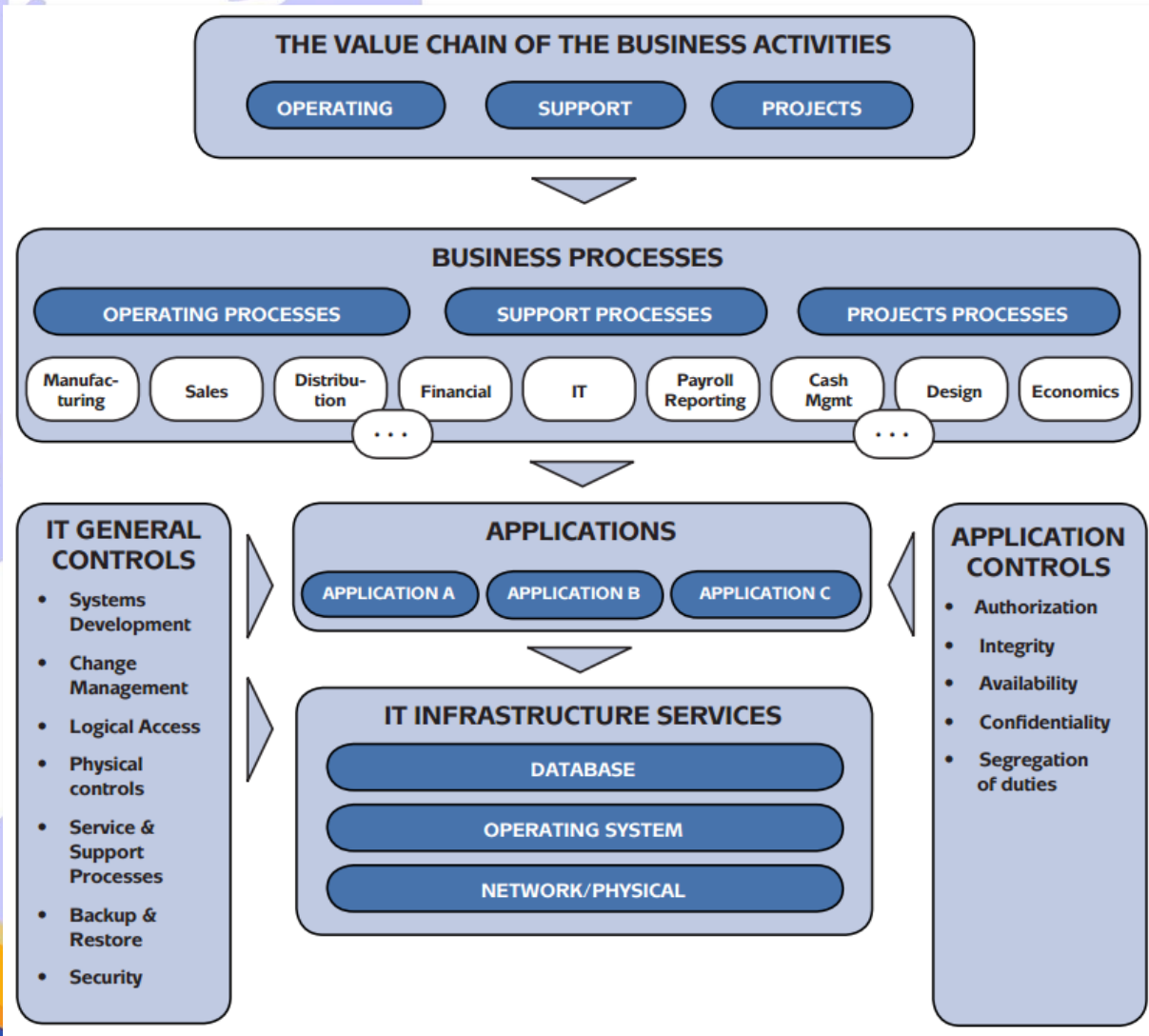
¹ Ernst & Young, *Turning risk into results: how leading companies use risk management to fuel better performance*, 2011.



The IT audit plan process

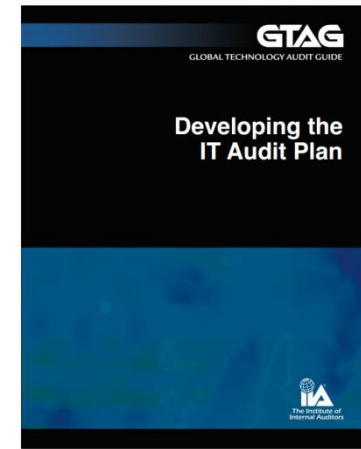


Understanding the IT environment in a business context

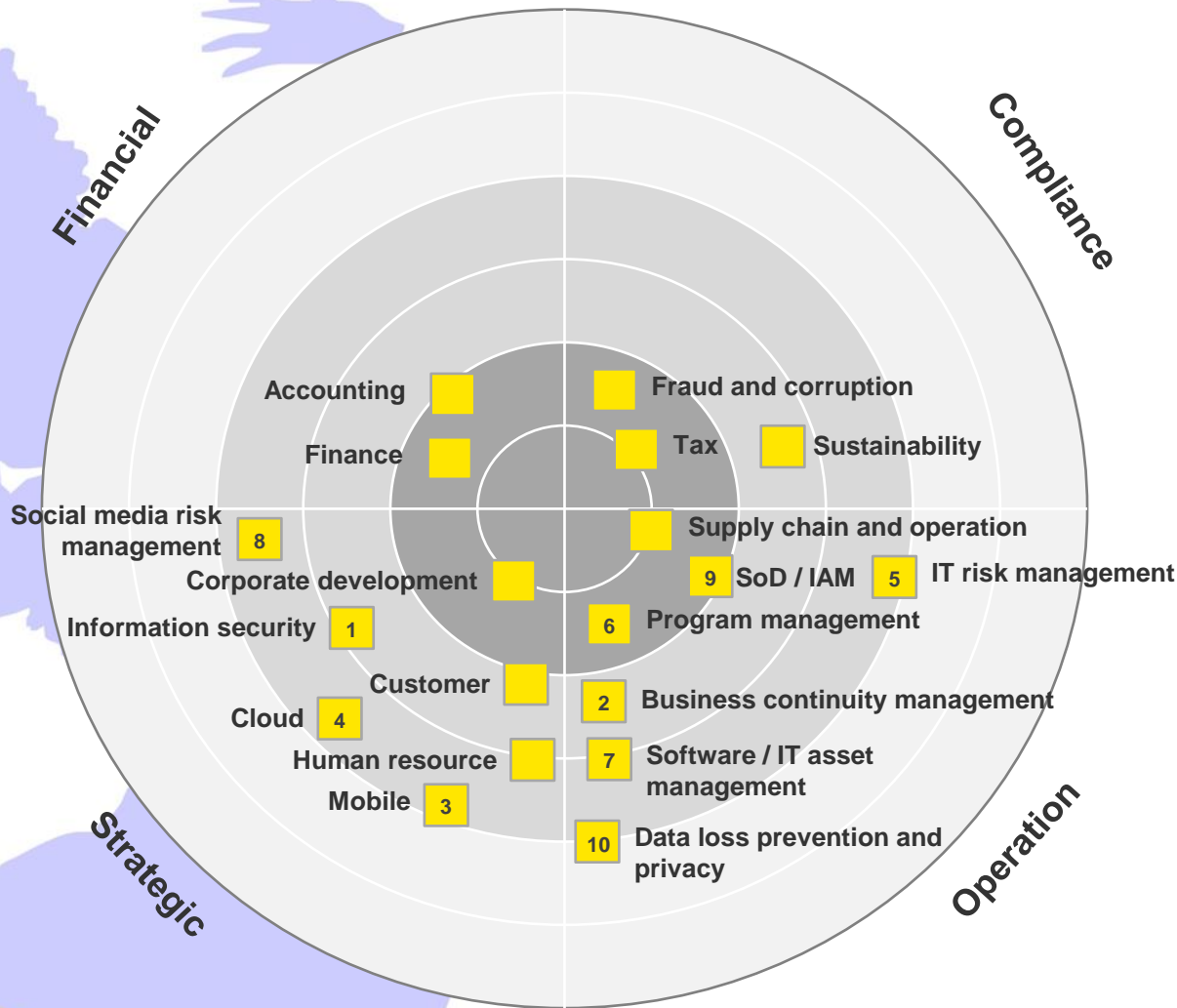


Example of an IT risk-ranking score model

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	2	2	3	2	2	2	41	H
HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
UNIX Administration and Security	2	2	2	3	2	2	3	1	1	1	3	2	24	M
Corp. Privacy Compliance	2	2	3	2	3	3	2	1	2	2	3	3	34	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
SOX Sustainability Review	2	2	2	2	2	2	1	1	2	2	1	2	19	L
Network Administration and Security	2	2	1	1	1	2	2	1	2	2	2	2	17	L
ITIL Deployment Practices	1	1	1	3	2	1	3	1	1	3	3	3	21	M
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L
Application Program Change Control	2	3	1	3	1	1	1	1	1	3	1	2	16	L
Lowest possible score			6											
Highest possible score			54											
Mid point			30											
L = Likelihood I = Impact														



Ten key IT considerations for internal audit



“Understanding the addressed risks is crucial step toward IT internal audit performance success.”

The **number** associated with **each function** indicates the sequence number on following pages where you can find more information about the **emerging risks** related to the respective function.



1. Information security

Although organizations have been dealing with opportunistic cyber attacks for years, many now find themselves the target of **more sophisticated** and **persistent efforts**. 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

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.

● **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.

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.

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

Key questions to evaluate during audit

- ▶ 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?
- ▶ 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?
- ▶ 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?



2. Business Continuity Management

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. While BCM should be viewed as an enterprise-wide risk and effort, the reality is **IT often 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**.

The audits that make an impact

● **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.

Disaster recovery audit – Assess IT’s ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster.

● **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.

Key questions to evaluate during audit

- ▶ Does a holistic business continuity plan exist for the organization?
 - ▶ How does the plan compare to leading practice?
 - ▶ Is the plan tested?
-
- ▶ 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?
-
- ▶ 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*



3. Mobile

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. **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
<p>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.</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 – 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.</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 – Combine traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical areas of functionality and for symptoms of common poor coding practices. Each of these “hot spots” in the code should be linked to the live instance of the application where manual exploit techniques can verify the existence of a security vulnerability.</p>	<ul style="list-style-type: none">▶ How sound is the code associated with the mobile applications used within the organization?▶ What vulnerabilities can be exploited within the code?



4. Cloud

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

The audits that make an impact

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.

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.

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.


Key questions to evaluate during audit

- ▶ 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?
- ▶ 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?
- ▶ 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?



5. 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. **The Securities and Exchange Commission, other regulators and the audit committee have increased their focus on companies managing risks holistically.** Internal audit is uniquely positioned to help drive growth and create value to the company through reviewing IT risk management activities.

The audits that make an impact	Key questions to evaluate during audit
<p>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.</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 – Evaluate 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 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?
<p>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.</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 – Evaluate the organization's current use of GRC software or the GRC software selection process. Provide 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?
<p> Audit was frequently mentioned in survey of leading IA organizations</p>	



6. Program management

While companies have **invested significantly in increasing their knowledge and capabilities in program and project management**, this is **not visible in the success rates. Lack of improvement is mainly due to increased complexity in business processes and the emerging technology landscape.** 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.

The audits that make an impact	Key questions to evaluate during audit
<p>Project management methodology audit – Assess 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 – 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.</p>	<ul style="list-style-type: none"> ▶ Is project/program management methodology being followed correctly? ▶ What is done when projects are underperforming? ▶ How is project risk assessed and managed?
<p>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.</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?
<p>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).</p>	<ul style="list-style-type: none"> ▶ 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?
<p>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.</p>	<ul style="list-style-type: none"> ▶ 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?
<p>Opportunities for integrated audits between IT and operational audit</p>	



7. 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**. As IT auditors, it is critical that software and IT asset management processes and controls are well understood.

The audits that make an impact	Key questions to evaluate during audit
<p>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.</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 – 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.</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 – Evaluate 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?
<p>Opportunities for integrated audits between IT and operational audit</p>	



8. 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. 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. 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

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.

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.


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.

Key questions to evaluate during audit

- ▶ Does the organization understand what risks exist related to social media?
- ▶ How well are the identified risks managed?

- ▶ Does a governance process exist for social media within the organization?
- ▶ How well are policies related to social media known among employees?

- ▶ 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



9. Segregation of duties/ IAM

The increased interest in SoD is due, to ensure **no individual should have excessive system access** that enables them to execute transactions without checks and balances. **Lack of investment in identity access management (IAM) often requires IT and audit to manually control that is prone to error.** A comprehensive SoD review is an audit that should be on all IT audit plans on a periodic basis.

The audits that make an impact	Key questions to evaluate during audit
<p>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.</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 – 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.</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 – Follow 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 – Evaluate 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?



10. Data loss prevention and privacy

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**. 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**.

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?





THANK
YOU!

“**Risk is good.** The point of risk management **is not to eliminate it.** That would eliminate reward. The point is **to manage it.** That is, to choose where to place bets and where to avoid betting altogether.”

Th. A. Stewart, 'Managing Risk in the 21st Century'

“**More shareholder value** has been **destroyed** as a **result of strategic mismanagement** and **poor execution** than in all of the financial reporting and **compliance scandals combined**”

*Worrying About the Wrong Risks
Paul Kocourek and Jim Newfrock
The Corporate Board Magazine*