Deloitte.

The Risk Intelligent chief audit executive
Mission possible

Risk Intelligence series

Contents

Preface

This publication is part of Deloitte's series on Risk Intelligence — a risk management philosophy that focuses not solely on risk avoidance and mitigation, but also on risk-taking as a means to value creation. The concepts and viewpoints presented here build upon and complement other publications in the series that span roles, industries, and business issues. To access all the white papers in the Risk Intelligence series, visit: www.deloitte.com/risk.

Open communication is a key characteristic of the Risk Intelligent Enterprise™. We encourage you to share this white paper with your colleagues — executives, board members, and key managers at your company. The issues outlined herein will serve as useful points to consider and discuss in the continuing effort to increase your company's Risk Intelligence.

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

The Risk Intelligent chief audit executive

Of our many human foibles, complacency and denial rank among the most pervasive. Examples of evidence ignored and realities refuted abound in politics, business, and on an individual level, often leading to unfortunate outcomes.

The concept of risk offers a prime case in point. Despite the fact that risk permeates virtually every aspect of our personal and professional lives, calamity is often perceived as something that happens to the other guy, not to ourselves.

For businesses, this perception can be dangerous indeed. In a time of intense competition, increased scrutiny, and escalating threats[1], a broad perspective and lucid thinking about the true risks facing a company become more important than ever. Yet, in our experience, few enterprises openly consider the possibility and consequences of failure, of bad luck, or of catastrophic loss.

This situation provides an opening for the chief audit executive (CAE). In today's environment, as a CAE, you have a unique opportunity to help make significant improvements in enterprise risk management effectiveness and efficiency. Your mission — should you choose to accept it — is to fight complacency and denial by enabling the enterprise to acknowledge, understand, and address relevant risks and thereby seek to reduce costs.

Your challenge? To lead the charge for change; to galvanize support for an ambitious agenda; and to overcome the doomsayers and the "negative thinkers" (without being portrayed as one yourself!).

Characteristics of The Risk Intelligent Enterprise™

We describe that rare breed of company that has attained the pinnacle of efficiency and effectiveness in risk management as "Risk Intelligent Enterprises™." Although these companies vary widely by size and industry, they all share similar characteristics, including the following:

- Risk management practices that encompass the entire business, creating connections between the so-called "silos" that often arise within large, mature, and/or diverse corporations
- Risk management strategies that address the full spectrum of risks, including industry-specific, compliance, competitive, environmental, security, privacy, business continuity, strategic, reporting, and operational
- Risk assessment processes that augment the conventional emphasis on probability by placing significant weight on residual risk or vulnerability (see sidebar, "Glossary: Inherent vs. Residual Risk," page 8)
- Risk management approaches that do not solely consider single events, but also take into account risk scenarios and the interaction of multiple risks
- Risk management practices that are infused into the corporate culture, so that strategy and decision-making evolve out of a risk-informed process, instead of having risk considerations imposed after the fact (if at all)
- Risk management philosophy that focuses not solely on risk avoidance, but also on risk-taking as a means to value creation.

For more information, see "The Risk Intelligent Enterprise™" at www.deloitte.com/risk.

[1] Colvin, Geoffrey, "Managing in Chaos," Fortune, October 2, 2006. This study of S&P 500 companies showed that overall risk levels more than doubled between 1985 and 2006. In 1985, only 35 percent of the S&P 500 faced high risk and highly volatile long-term earnings growth. By 2006, that number had risen to 71 percent. During the same period, the number of companies enjoying low risk and volatility fell from 41 percent to 13 percent.

The nature of risk

We define risk as the potential for loss or the diminished opportunity for gain caused by factors that can adversely affect the achievement of a company's objectives.

Note that this definition encompasses risk's dual nature, representing at the same time the potential for both loss and reward. The distinction is key: We believe that companies that focus solely on risk avoidance may survive but rarely thrive; only those that intelligently manage risk-taking as a means to value preservation and value creation will excel in today's perilous yet opportunity-rich business environment.

Your role as today's CAE, then, is to help determine that management is keeping the enterprise's risk/reward picture in balance, both preserving and creating value, by taking a holistic approach to the management of risks across the enterprise. As a top-performing, high-value CAE, you can help develop a common understanding of the different types of risks, including regulatory and contractual compliance, competitive, environmental, security, privacy, business continuity, strategy and execution, reporting, and operational. (See sidebar for more detail on types of risk that should be on the CAE's radar screen.)

You can also help evaluate the efficiency and effectiveness of how risk information is shared and managed across business activities and functions, while helping improve the enterprise's capability to prevent, detect, correct, and escalate critical risk issues. This approach can reduce the cost of risk management by sharing risk information and coordinating the responses of existing risk management functions. In so doing, the overall effectiveness and efficiency of risk management can be improved.

We believe that companies that focus solely on risk avoidance may survive but rarely thrive; only those that intelligently manage risk-taking as a means to value preservation and value creation will excel in today's perilous yet opportunity-rich business environment.

Types of enterprise risk

There are various types of enterprise risk, including the following:

- **Governance risks** — risks related to the structure, policies, procedures, and authorities in which the key directions and decisions of the company are overseen. For example, independence and oversight; ethics; corporate social responsibility; delegation of authority; shareholder relations; stakeholder activism; corporate policy.
- **Strategy and execution risks** — risks associated with the ability to formulate and/or execute a successful business strategy. They relate largely to the company's future initiatives, such as plans to enter new markets, launch new products, or form new alliances. For example, acquisitions and divestitures; succession planning; capital planning/allocation; research and development; brand and marketing; pricing; customer demands; customer concentration; product; and technology.
- **Operational risks** — risks affecting controls and the controls infrastructure relating to the protection and utilization of existing assets and operations, including how they may be leveraged for future growth. For example, sourcing; manufacturing; distribution and logistics; sales; franchises and licenses; privacy; quality; information technology; and security. Operational risks also flow from all of the preceding situations where the entity relies on another party in a business relationship.
- **Infrastructure risks** — risks relating to the performance of people, processes, and systems that support the company's operations. For example, legal/intellectual property/litigation; tax; finance and accounting; reporting; treasury; compliance; human resources/culture; change management; personal safety and physical security; insurance/business continuity; environmental; and facilities management.
- **External risks** — risks associated with the environment in which the company operates or external factors beyond the company's control. For example, competition; legal and regulatory; stakeholder relations; geopolitical; climatic, economic conditions/industry trends; hazards; terrorism, war, climatic, and civil unrest.

As stated in the first whitepaper in our Risk Intelligence series, "The Risk Intelligent Enterprise: ERM Done Right," "companies that are most effective and efficient in managing risks to both the existing value-creation activities and to future profitable growth opportunities will, in the long run, outperform those that are less so[2]."

Risk and growth

The risks shown in the sidebar (page 5) are related to your company's ability to meet its value and growth objectives. These objectives are typically achieved by focusing on the following areas:

- **Revenue growth**: customer, product, or market goals
- **Margin**: cost reduction, including restructuring of costs and provision of services and supply chain efficiencies
- **Assets**: asset turnover, flexibility, effectiveness and efficiency targets
- **Expectations**: various expectations of stakeholders (including shareholders, investors and analysts), regulators, rating agencies, creditors, banks, employees, customers, partners, and suppliers

Value and growth is the language of management, and attaining success in this area is how managers get compensated. Because risk management has traditionally focused on the protection of existing assets — largely through risk avoidance and insurance — management expects that when CAEs talk of risk, they are talking about risk avoidance and not about the risk taking that is essential for the company to prosper and grow. Managers typically see risk management as a cost to the business and potentially an impediment to growth. Frankly, they often see risk management as a source of pain and burden to the business.

As a CAE, you can bridge the gap with operating management by speaking their language, framing the risk discussion in terms of growth, profitability, and shareholder value creation. Risk Intelligent CAEs understand their companies' value and growth objectives and how the different types of risks, when not effectively and efficiently managed, can contribute to a failure to achieve these objectives. You can help focus and steer the activities of internal audit and other functions involved with risk management toward a more integrated and holistic approach to help the company manage the risks most critical to the achievement of its objectives —- that is, to make more money and to reduce the burdens of risk management and compliance.

Risk Intelligent CAEs understand their companies' value and growth objectives and how the different types of risks, when not effectively and efficiently managed, can contribute to a failure to achieve these objectives.

"Assurance" and "Reassurance"

It is management's responsibility to lead the enterprise, including the identification, assessment, and management of attendant risks. As part of these responsibilities, management provides *assurance* to the board and third parties that such risks are appropriately addressed and are within the risk appetite of the enterprise.

Yet, as commonly defined, internal audit also has assurance responsibilities — to conduct its audit plan and then report to executive management and the board that management's reports on the effectiveness and efficiency of risk mitigation and control are reliable and that management's confidence is justified.

We believe that this use of the same term to define different activities can be a source of confusion. As such, we have introduced a clarifying word — "reassurance" — to more accurately describe the role of internal audit.

We consider the term "reassurance" to be a useful way to contrast internal audit's responsibilities with those of management.

[2] To access all the white papers in the Risk Intelligence series, visit: www.deloitte.com/risk.

The role of the CAE and Internal Audit

A Risk Intelligent Enterprise depends on the internal audit function for reassurance (see sidebar on page 6), facilitation, and consultation to identify opportunities for business improvement and cost savings. As CAE, you have the opportunity to provide reassurance on the risk management process: that risks are effectively identified and evaluated; that risk management processes are both effective and efficient; and that key risks are appropriately reviewed and reliably reported to those who need to know.

While increasing attention is being paid to improving effectiveness, many enterprises (especially those that are highly regulated) are looking both to improve efficiencies and reduce the costs of effective governance, risk, and compliance (GRC) activities.

You can help drive toward the dual goals of effectiveness and efficiency, and in doing so, you can broaden the role and increase the value of both the CAE and the internal audit function. Your scope of activity can be broadened to include facilitating identification and evaluation of relevant risks across the enterprise; coaching management in appropriate responses to risks; reporting on consolidated risks and management's responses; and championing the establishment of Risk Intelligent practices.

The capital markets reward the ability to create and sustain future profitable growth, which requires taking risks that have the potential to generate such growth. After spending the last few years coping with regulatory compliance, a forward-thinking CAE now has the opportunity to break out of these restrictive aspects of his or her job. Now is an opportune moment to turn your attention to value-adding risk-management activities, including identifying or confirming risks associated with management's strategic plans and objectives for positive stakeholder return, and improving the efficiency and effectiveness of governance, risk management, and compliance.

At the same time, the role of internal audit in risk management is not all-encompassing. The understandable tendency to see a problem and want to "fix" it, or to see an opportunity and want to seize it, may have to be resisted in some instances. Certain activities do *not* properly fall within the domain of internal audit. First and foremost, according to the Institute of Internal Auditors (IIA), internal audit should not set the enterprise's risk appetite (the type and level of risk it is willing to accept), which must be established at the highest levels (by executive management and the board). Furthermore, according to the IIA, internal audit should not impose risk management processes; you must not perform management's assurance role related to risks; you cannot make decisions (recommendations are encouraged) on risk responses; nor should you assume accountability for risk management.

Understand vulnerabilities

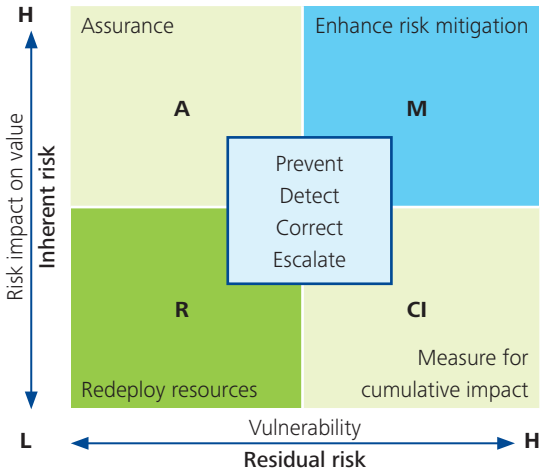
Many companies base their risk management program on the probability of certain negative events occurring. This approach is especially well-established in the internal audit profession and in the financial services and energy industries.

Unfortunately, probability-based risk assessments do not always suffice. As a recent Deloitte Research study noted, major-value losses are often high-impact, low-likelihood events[3].

If senior management is biased toward mitigating high-impact, high-likelihood events, internal audit should draw attention to and advocate for resources to address other events relevant to the business that could have a high negative impact if they do occur (see figure 1, "The New Assessment Paradigm," page 8). Simply stated, if a risk is relevant to the business and is extremely high impact, it should be addressed, regardless of probability. This is particularly true of risks associated with value creation as they have higher uncertainty (such as the development and launch of new products and services, entry into new markets, and mergers and acquisitions). The greater the time horizon, the greater the uncertainty and the less meaningful probabilistic estimates become.

[3] "Disarming the Value Killers," Deloitte Research, 2005.

Figure 1: The new assessment paradigm



In the "A" (Assurance) quadrant, management should be expected to provide reasonable assurance that controls to prevent, detect, correct or escalate a risk are both effective and efficient in managing a risk such that the residual exposure (see sidebar) is within the company's appetite for that type of risk. Internal audit's job is to provide reassurance that management's reports can be relied upon.

When management can only provide "qualified" assurance — meaning that some controls are working while others are not — internal audit should audit those controls that are deemed to be effective and support improvement in other areas as required.

For risks that fall into the "M" (or Mitigate) quadrant, above, management is unable to provide any assurance that controls are either effective or efficient and the exposure is not within the company's appetite for that type of risk. In such cases, management should address risks requiring mitigation, with internal audit providing recommendations to management for consideration in developing and designing controls to reduce exposure and to also track progress on remediation plans.

For "R" (Redeploy) quadrant risks, a leading practices approach is for internal audit to test controls for effectiveness and develop recommendations for management's consideration to improve efficiency.

Finally, for the "CI" (Measure for Cumulative Impact) quadrant, above, a leading practice is for internal audit to assess cumulative impacts and frequency to determine whether these risks could in aggregation have a more significant impact

Management should take a top-down focus on mission-critical risks to strategy and execution while encouraging informed and calculated risk-taking (also called "rewarded risk-taking"). Once more, this reflects the reality that the market rewards companies that successfully take and manage risks associated with new products, markets, business models, alliances, acquisitions, and the like. Again, in a leading practices role, the CAE would provide reassurance that management reports can be appropriately relied on.

Glossary: Inherent vs. residual risk

"Inherent" risk refers to the risk that exists before you address it, i.e., the risk to your company in the absence of any actions you might take to alter either the likelihood or impact. Every company in every industry faces inherent risk; of course, not every company manages it effectively or efficiently.

"Residual" risk is also known as your "vulnerability" or "exposure," i.e., the risk that remains after you have attempted to mitigate the inherent risk.

Risk Intelligent Enterprises consider both inherent and residual risk. This process puts both the executives and the board in a better position to evaluate the level of exposure and then decide whether or not to accept the exposure.

Bridge the silos

Risk management is nothing new. In fact, plenty of sophisticated risk management practices already take place within most companies. The finance department manages credit risk; IT handles security and privacy risks; and so on. Unfortunately, these risk specialists often work in organizational and/or physical isolation: they don't talk in the same business terms and often measure risks using different criteria.

Of course, risks don't exist in isolation. A privacy risk can evolve into a reputational risk, a litigation risk, and a financial risk, all in short order.

Roles and responsibilities should be reviewed and clarified, seeking out gaps and overlaps. This process will produce a portfolio view to better understand and manage risk interactions, improving the ability to rely on other risk specialists' work.

Your challenge as a CAE is to assist the enterprise in integrating risk information across all organizational boundaries. By facilitating the development of a uniform governance, risk, and compliance framework, you can help bring together — often for the first time — an integrated view of the enterprise which can lead to a better understanding and response to risks and how they may interact, while also reducing the burden on the business.

You can also act as a catalyst and enabler by getting risk specialists talking to one another; developing a common risk language and harmonizing the way risk is identified, assessed, and measured; so that risk intelligence can be shared across specialist silos. For example, if there are multiple risk and control self-assessments being performed today, how valuable would it be to your company to reduce that number and yet get better information and intelligence as a result?

The lack of coordinated gathering, analysis, and response to Risk Intelligence is an almost universal problem. For example, the inability of the CIA and the FBI to share intelligence about terrorist threats prior to 9/11 is often cited as one contributing factor for the failure to prevent the attacks. Those agencies have reportedly made progress toward breaking down their own barriers to intelligence-sharing.

Risk silos can also come into play when dealing with foreign currency exchange exposure. In such cases, a typical risk response calls for the treasury function to implement sound hedging policies and activities. However, if the company sources its raw materials in overseas markets, this would expose it to the risk of foreign currency fluctuation. Thus, a more comprehensive approach would be to include the purchasing and manufacturing departments in the risk analysis and risk response process.

Another example can be found in third-party relationships. When these arrangements are initiated, the legal department typically takes care of the contracts and agreements. Oftentimes, however, the provisions fail to factor in all relevant items, such as accounting and IT requirements and needs. A more holistic view of outsourcing and third-party risks would engage all the relevant functions within the company, resulting in a more efficient and effective risk management process.

As CAE, you can facilitate taking a "portfolio" view of risk, emphasizing cross-departmental sharing of lessons learned. You can support the development of integrated tools to assess all types of risk, a goal not yet achieved by the majority of large companies. The objective is to shift individuals' focus from a local perspective to a more effective enterprise-wide response to major value losses — whether to existing assets or future growth — that cuts across functions.

If Risk Intelligence has to flow up the organizational hierarchy before it can flow back down, it's too late. In any environment where there are risk-related handoffs between functions, potential problems exist. The fabric of Risk Intelligence needs horizontal as well as vertical strands in order to be strong.

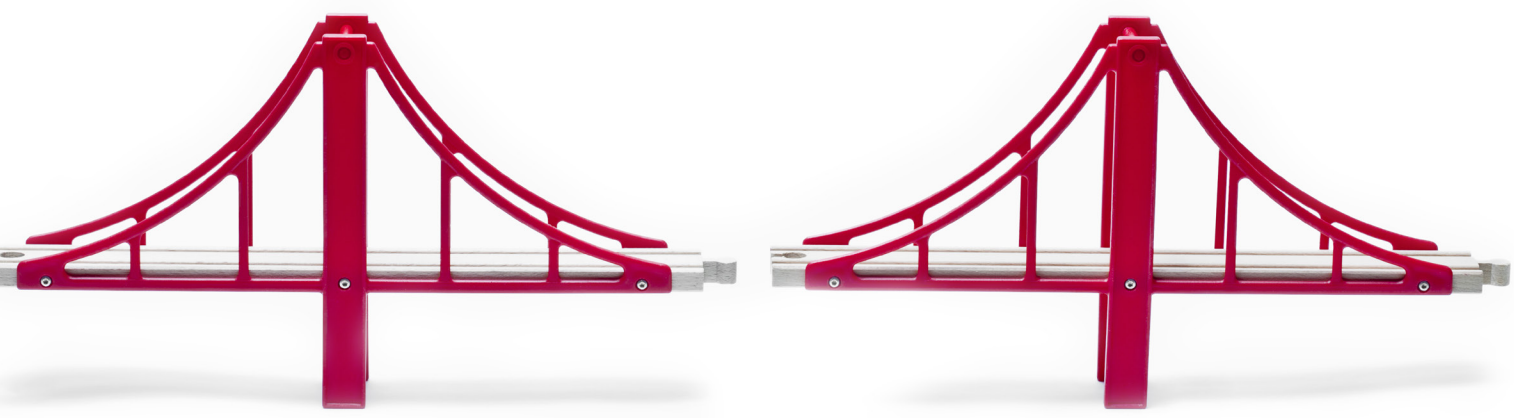
Harmonize, synchronize, and rationalize

The process of bridging organizational barriers to Risk Intelligence is multifaceted and requires the development of a uniform governance, risk and compliance framework.

The first task is **harmonization**, establishing a common language for risk management and standardizing policies, practices, and reports. Roles and responsibilities should be reviewed and clarified, seeking out gaps and overlaps. This process can produce a portfolio view to better understand and manage risk interactions, improving the ability to rely on the work of all risk specialists across the organization.

The next step, **synchronization**, involves cross-functional coordination for improved anticipation, preparedness, first response, and recovery. By developing a coordinated workflow, different constituencies can coordinate the timing of their requests for information. Workload demands should be smoothed out to avoid unmanageable spikes and the burden on the business.

Last is the process of **rationalization**. This is where you, as the CAE, working in conjunction with others, can help to reduce or eliminate duplication of effort related to assessment, testing, and reporting. This goal can oftentimes be attained in part through better utilization of existing technology or deployment of new technology. Once again, rationalizing has the added benefit of reducing the expense burden on the business.



Aligning risk assessment

Most current internal audit risk assessments start with a blank sheet of paper as individual entities, processes, and systems are evaluated. In keeping with the traditional approach, internal auditors audit risks with the highest impact and probability, without necessarily differentiating between inherent risk and residual risk.

A different approach is taken by the Risk Intelligent Enterprise, where management provides assurance and internal audit provides reassurance. Management should be responsible for:

1. assessing the inherent risk (i.e., before mitigation and controls)
2. assessing the effectiveness of existing risk mitigation and controls
3. determining the residual risk (i.e., the risk that remains after mitigation and controls are implemented)
4. determining whether such exposure is within the appetite of the enterprise for that type of risk, and, if not, further mitigating the risk
5. providing reasonable assurance to the board that the controls are both effective and efficient in managing the exposure so that it remains within the board-approved appetite for that type of risk.

While remaining aware that management and the board "own" risk, internal audit can provide guidance and reassurance that risk is being properly and efficiently managed within the company's defined appetites for various risks.

The role of internal audit then is to provide reassurance that management's reports can be relied upon and/or to provide advice about how risk mitigation and control might be improved if the exposure is not within the corporate appetite.

The Risk Intelligent CAE

As the CAE in a Risk Intelligent Enterprise, you can lead a number of value-added risk assessment activities rather than just using traditional methods that depend heavily on probabilities. These include providing reassurance to management and the board that:

- the key risks to both value preservation and creation have been identified
- different scenarios have been assessed and stress-tested
- inherent vs. residual risk has been reliably assessed
- the residual risk appears to be within the appetite of the company for that type of risk
- controls are not only effective but also efficient
- management's reports can be relied upon

Next steps

As a CAE, ask yourself the following questions:

1. Are we speaking the language of management? Are we assessing risks to future growth (value creation) or are we solely focused on the protection of existing assets?
2. Are we assessing risks in isolation or are we looking at how these risks may interact and cascade?
3. Is there a uniform framework to align the various risk specializations regarding governance, risk, and compliance assessments so we can reduce the cost burden on the business? For example, can we reduce the number of risk and control self-assessments?
4. Do existing risk assessments reliably and adequately assess inherent and residual risk exposures?
5. Do we have the means to assess whether residual exposures are within the risk appetite of the company?
6. Is there a robust risk mitigation process?

Your answers to these questions are critical in determining if your current risk assessment model is Risk Intelligent and, if not, where to improve.

The majority of companies today, even the largest and most forward-thinking, can always improve their Risk Intelligence. It does not have to be a complex and multilayered undertaking. As CAE, you can act as an enabler and catalyst to develop an integrated means to improve your company's Risk Intelligence capabilities.

CAEs have a unique role to play in the Risk Intelligent Enterprise. While remaining aware that management and the board "own" risk, internal audit can provide guidance and reassurance that risk is being properly and efficiently managed within the company's defined appetites for various risks.

Your mission, should you choose to accept it, is to help your enterprise become more Risk Intelligent. This, we believe, is "Mission Possible."

Contact us

To learn more about Deloitte's governance and risk services or to contact one of our global leaders, please visit: www.deloitte.com/risk.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2013 Deloitte Development LLC, All rights reserved
Member of Deloitte Touche Tohmatsu Limited