Deloitte.

The Risk Intelligent Enterprise
ERM done right

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.

Ask any business leaders selected at random to define "enterprise risk management," and chances are each will offer a different interpretation. That's because despite the ubiquity of the term "ERM" in the business lexicon, a standard definition remains elusive. And notwithstanding the growing awareness of the need to effectively manage risk, the range of practices falling loosely under the ERM heading is vast and growing.

ERM, broadly speaking, has been around for at least a decade. In some business sectors, notably financial services and energy, most industry-specific risks are managed with a high level of finesse, using complex probability modeling and sophisticated analyses. Other companies, such as some in the services and consumer business sectors, may have a less refined approach to risk management, and the need for more systematic practices is just now emerging.

But it is the rare company, we contend, that intelligently manages the full spectrum of risk; that adequately assesses and addresses risk from all perspectives and quarters; that breaks through the organizational barriers that obscure a view of the entirety of risks facing a company; and that systematically anticipates and prepares an integrated response to potentially significant risks. Yes, financial services companies may have a comprehensive grasp of interest rate, currency, and credit risk, but how many of them have suffered significant losses from severe events — such as natural disasters, terrorist attacks, and other threats to business continuity — by failing to develop contingency plans for such occurrences? True, many companies anticipated the transition to e-commerce, but how many endured reputational and customer losses because they failed to adequately protect online customer data?

Since it occurs so infrequently, we believe that when ERM is done right it deserves special designation. As such, we call such model companies *Risk Intelligent Enterprises*.

Of course, the path to this lofty designation is long and sometimes arduous. Every company that charts its progress will find itself in a different location on the map, depending on the unique business challenges it faces and the competencies and capabilities it possesses. But every organization that attains the status of the *Risk Intelligent Enterprise* will find that they 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 vulnerability
- 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.

Some of these bulleted items may be unfamiliar to you. But all, we contend, are essential characteristics of the *Risk Intelligent Enterprise*. Each will be discussed in detail below.

Risk Intelligent Enterprises come in all sizes and industries, and each organization tailors its risk management practices to its particular circumstances and needs. Yet every *Risk Intelligent Enterprise* shares this insight:

Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so. Simply put, companies make money by taking risks and lose money by failing to manage them.

Risk profile

Various forces have converged to push risk management into the consciousness of management and boards. Most prominent may be the recent spate of corporate scandals: Multimillion dollar judgments in the Enron and WorldCom shareholder suits forced board members to draw upon personal assets to settle; other directors surely hope to avoid digging into their own pockets. At the same time, images of executive "perp walks" have been splashed across newspapers and TV screens; no executive wants to serve as chum for the next media feeding frenzy.

Regulatory actions have also shined a spotlight on risk. The Securities and Exchange Commission, Public Company Accounting Oversight Board, and New York Stock Exchange all require or encourage risk management-related activities. A renewed focus on the Foreign Corrupt Practices Act of 1977 has further heightened awareness, as has the advent of the Sarbanes-Oxley Act of 2002 (although some observers contend that SOX has actually reduced the attention given to the full spectrum of risks due to the Act's intense focus on financial statement risks).

Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so.

Of course, potential risks extend well beyond financial misstatements and acts of fraud: Terrorist attacks expose business continuity risks. Computer hacking heightens awareness of security and privacy risks. Expensive asbestos settlements illustrate the dangers of public health and safety risks. Poor preparation for and clumsy responses to corporate crises highlight reputational risks.

The rewards of Risk Intelligence

The competitive benefits of improved Risk Intelligence include:

- Improved ability to prevent, quickly detect, correct, and escalate critical risk issues
- Reduced burden on business operations by standardizing risk management principles and language
- Reduced cost of risk management by improved sharing of risk information and integration of existing risk management functions
- A means to improve strategic flexibility for both upside and downside scenarios
- The ability to provide a "comfort level" to the board and other stakeholders that the full range of risks is understood and managed.

Also coming into play are increasing stakeholder expectations and activism. Today, many large institutional investors are demanding strong risk management practices, and market capitalization can take a severe and immediate hit if companies fail to protect their existing assets or the integrity of their financial statements. Some investor rating and credit rating services, notably Moody's and Standard & Poor's, have added enterprise risk management capabilities to their evaluation criteria. Companies deemed deficient in their risk management capabilities can face an increase in the cost of capital.

Risk redefined

Before we can improve our *Risk Intelligence*, we must first understand the key terminology and concepts. Most significant, of course, is the word "risk" itself.

Many definitions exist, with varying degrees of detail and precision. We have analyzed and assimilated several, combined them with our own perspective, and distilled the result:

Risk is the potential for loss caused by an event (or series of events) that can adversely affect the achievement of a company's objectives.

Note that this definition accommodates both the protection of existing assets and the enhancement of future growth objectives. That is, intelligent risk management involves not just the desire to avoid something negative (prevent a hacker from stealing your customer database) but also the need to attain something positive (successfully integrate an acquired company). The *Risk Intelligent Enterprise* views risk not just as *vulnerability* to the downside, but also *preparedness* for the upside.

The distinction is key: *Risk Intelligent Enterprises* consider the ability to anticipate and react to a market opportunity to be as important as readiness for a potentially devastating business disruption.

If a risk is both relevant and has extremely high impact, it should be addressed, regardless of "remote" likelihood.

Probability, vulnerability, and risk interaction

Another significant attribute of the *Risk Intelligent Enterprise* can be found in its linking of probability with vulnerability and risk interaction. Probability, of course, is important and well-established in traditional risk management programs. Indeed, many risk events occur with regularity and thus can be effectively modeled using statistical techniques. However, probability has less value for risks that occur outside the normal fluctuations, i.e., where the event is rare or unprecedented, where the rules are unknown or rapidly changing, or where causes are driven by external factors beyond any individual's or company's control.

Consider the Hurricane Katrina example: Probabilistic modeling clearly demonstrates that New Orleans will likely suffer at least three major hurricanes every century. But these models can't state with any degree of certainty which particular year a devastating storm will blow ashore, nor have they always done a good job of predicting the outcome when multiple risk factors converge.

In such instances, the notions of vulnerability and risk interaction should assume prominence in the risk assessment and risk management processes.

In the case of Katrina, the city's vulnerability to such an event proved exceedingly high in virtually every respect, including process (e.g., poor evacuation plans), people (e.g., unclear chains of command), and systems (e.g., lack of backup communication systems).

Katrina was also characterized by the failure to consider the correlation of several interrelated risk factors. In particular, a significant portion of the damage associated with the storm was due to flooding caused by the levee breaks, and to a lesser extent by the storm surge (which was a contributing factor). The wind and rain were, in fact, lesser factors. The flooding caused by the levee breaks was exacerbated by the fact that the evacuation left virtually no one to operate the systems that were in place to pump water back into the lake or to repair the breaks in a timely manner. Consequently, the pump failures turned out to be highly correlated with the storm and its flood consequences.

Of course, while the consideration of vulnerability and interaction should be elevated, this is not to imply that probability is not important. Probability works well in many applications, including industries such as banking, which uses probability to manage market, credit, and operational risk; and insurance, which uses actuarial data to set rates and establish reserves.

But, depending on the variables, vulnerability may also need to play a role in the overall risk assessment. The simple fact is — and this applies as equally to business as it does to emergency management — if a risk is both relevant and has extremely high impact, it should be addressed, regardless of "remote" likelihood.[1] But note that "addressed," in this context, does not necessarily

[1] For the purpose of this article, the terms "probability" and "likelihood" are used only in the context of risk management. No relationship to these terms as defined and used in Statement of Financial Accounting Standards No. 5, Accounting for Contingencies, by the Financial Accounting Standards Board is intended, stated, or implied.

mean "mitigated." An organization surely cannot devote all its attention (and dollars) to managing and mitigating a few low likelihood/high impact risks to the exclusion of higher probability/lower impact threats. Rather, a balance needs to be attained. Vulnerability should be weighed alongside probability, as appropriate to the circumstances, and a *Risk Intelligent* decision should be made. Possible responses may vary widely, and may include simply keeping the risk on the radar screen and tracking changes in course and severity without taking any other mitigating action. Resource availability and allocation will, of course, need to be primary factors in these considerations.

But it bears noting that sometimes improbable events do occur with devastating effect, while other times probable events fail to materialize. The *Risk Intelligent Enterprise* understands the possible, not just the probable, and responds accordingly.

Scenario planning

One way to evaluate high impact/low probability events is through scenario planning, which can augment statistical models and help companies prepare for specific events. Scenario planning enables executives to answer the questions: "What could disrupt our plans? And how vulnerable are we to it?"

Companies have long engaged in budgeting and forecasting, albeit often in a restricted manner that considers only a narrow range of outcomes (e.g., assumptions about the stability of commodity prices) and focuses primarily on direct, bottom line impact. Unfortunately, this limited view can leave the company unprepared when significant unexpected variations — both good and bad — occur.

The *Risk Intelligent Enterprise* considers indirect or longer-term effects due to, for example, loss of reputation and customers (a "downside" scenario) or lack of production capacity for demand increases (an "upside" scenario). Similarly, these companies weigh a wider range of causes and effects beyond just near-term financial impact. Once potential scenarios are identified, then a range of "triggers" (events such as a currency dropping below a certain value or competitors gaining a specific market share) are established, which alerts the company to a situation requiring further assessment and response.

A company can build its ability to respond to different scenarios by selectively investing in the requisite capabilities needed should the event occur. For example, a manufacturing firm might take a partial equity stake in a company in another market or region with the option to migrate to full ownership. Or a media company could simultaneously support different technologies for online media distribution until standards become well-defined; by initially supporting multiple technologies, the vendor in effect takes a "real option" to adapt quickly to future market conditions. Or instead of building a plant, a company may enter into a production sharing agreement (even with a competitor) at a pre-negotiated price that allows them access to excess capacity in the event of a market upturn. This protects them on the upside and saves the immediate cost of building a plant in the event that the upturn does not materialize.

However, one problem can arise with scenario planning: it is often difficult to address envisioned scenarios within the existing risk management infrastructure (i.e., within functional divisions). Management must be aware of and attempt to overcome this problem. To do so, the functional leaders should be involved in the scenario development process and should collaborate to develop cross-divisional mitigation plans, as necessary. Any possible scenarios that cannot be satisfactorily addressed should be elevated to the appropriate management level so that rectifying actions can be determined and responsibility assigned.

Scenario planning enables executives to answer the questions: "What could disrupt our plans? And how vulnerable are we to it?"

Silos and outsourcing

Exacerbating the silo problem is the increasingly common practice of outsourcing business functions, such as payroll, order fulfillment, and benefits administration. Outsourcing can be risky, and companies that employ outside parties for such work may find that a comprehensive view of their risk profile becomes more difficult to attain. At the same time, outsourcing can represent a strategic response to upside risk when it is undertaken to exploit certain opportunities. But if not managed properly (due to a siloed approach) it can create more harm than good. To address this problem, some companies are pulling back certain outsourced activities; others are employing strengthened contract risk and compliance programs to ensure their business partners are adhering to high standards of risk management.

Silo state

The term "silo" describes the tendency of organizations to separate into autonomous segments based on geography or business function. When risk management becomes "siloed," each of these units — such as internal audit, treasury, HR, and IT — brings to bear different philosophies and approaches. In the extreme, silos become miniature ecosystems, with multiple cultures, jargons, and practices.

From the "silo state" a host of problems can arise: duplication of effort; increased burden on the business; lack of appropriate reliance on one another's work; lack of standardization in methodology; and absence of *Risk Intelligence* sharing. All of which can make it difficult — if not impossible — to obtain an accurate and comprehensive view of the nature and level of risk that the entire company is actually exposed to.

And, of course, without this comprehensive view (what is sometimes referred to as a "portfolio" view), you can't really understand and manage the totality of risks facing the company.

Yet, despite these disadvantages, silos also represent an essential component of intelligent risk management — risk specialization. Today, more than ever, a thorough knowledge and understanding of the specific risks that affect these business silos is required.

Unfortunately specialization without collaboration creates problems, because many risks transcend the silo boundaries. To illustrate, consider the Deloitte Research study, "The Value Killers."[2] This in-depth analysis of value loss at a number of global 1000 companies revealed that, during the past decade, more than half of these businesses experienced a sudden and precipitous drop in share price (a loss of 20 percent or more in one month or less). *More than 80 percent of the losses were due to the interaction of multiple, cross-silo risks.*

The *Risk Intelligent Enterprise* is aware of the silo tendency and takes concrete steps to break down the institutional barriers that can inhibit collaborative risk management. This may include the creation of cross-functional teams that share information, perform joint analyses, and engage in scenario planning.

However, care should be taken to avoid over-centralization. Some companies that have tried to put all of their risk management silos under a single "czar" have failed because they attempted either to homogenize the silos or to assume central control of a process that more properly should have been managed by the specialists. While there should be a central point of coordination (such as a chief risk officer), this role should not be one of overarching control. The business units should always remain responsible for taking and managing risk and maintaining ownership for the risks they assume.

Silo scenarios

The implications of operating within organizational silos can be significant. For example, acting in silos, an operating company might fail to use both its legal and treasury departments to grant price guarantees to its customers or suppliers, resulting in unnecessary risk and liability. Ideally, employing appropriate Risk Intelligence, treasury would evaluate and price the risk of the guarantee, while legal would mitigate governance and liability risks.

[2] "The Value Killers," Deloitte Research, 2005, www.deloitte.com/us/valuekillers.

Properly executed, silo "busting" is about understanding the need to develop common risk methodologies, terminology, and metrics to ensure consistent risk management and reporting while at the same time allowing the different functions sufficient autonomy to exploit their specialized knowledge and expertise.

Parsing risk

Some executives mistakenly perceive their responsibility to address risk as a duty to avoid risk. This is a recipe for failure. Avoid risk and you will also avoid success. *Intelligent risk-taking for reward is a building block of capitalism and essential for competitive advantage.*

Note that the decision to embrace or avoid risk should not be viewed as an either/or choice. Differing circumstances call for different responses. Sometimes you bet all your chips; sometimes you walk away from the table; but most often you act between these two extremes and make careful, measured wagers in consideration of the odds. Indeed, in some respects, the extremes represent easy options. Picking the best course of action when the choices are not so clear-cut presents a more formidable challenge.

Part of an executive's responsibility involves understanding the nature of risk. Unlike the proverbial rose, a risk is not a risk is not a risk. Critical distinctions must be made between various types of risk: unrewarded vs. rewarded, and inherent vs. residual.

Sometimes you bet all your chips; sometimes you walk away from the table; but most often you act between these two extremes and make careful, measured wagers in consideration of the odds.

In enterprises where risk management capabilities are not fully developed, **unrewarded risk** often represents the full extent of their risk management activities. Unrewarded risk gets its name from the fact that there is no premium to be gained for taking certain kinds of risks (for example, risks affecting operations, integrity of financial statements, and compliance with laws and regulations).

Conversely, **rewarded risk** focuses on value creation; it involves managing risks to future growth, including putting capital at risk and making profitable bets. In rewarded risk-taking, a company receives a premium for taking and managing risks — and receiving approval in the marketplace — associated with new products, markets, business models, alliances, and acquisitions.

Consider, for example, merger and acquisition activities. While every company that engages in M&A does so with the intent of building shareholder value, oftentimes the expected gains fail to materialize.

The desired outcome is much more likely to be achieved when the full array of integration risks has been identified, assessed, and managed intelligently. This contention is supported by a recent study by London's Cass Business School and Towers Perrin, which found that improvements in corporate governance, selection of deals, and post-merger integration have reduced the risks of M&A failure and have contributed to improved value creation by out-performing the market.[3]

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. Companies can only understand residual risk if they have first addressed inherent risk.

[3] "Current M&A Cycle Creates Shareholder Value," Cass Business School and Towers Perrin, April 2006.

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.

Decent exposure

And, of course, determining an acceptable level of exposure represents the gist of the matter, for management and boards alike. Whether filing 10-K disclosures, responding to investors' questions at an annual meeting, or, in the nightmare scenario, replying to an opposing attorney in a trial, your diligence around risk should be unimpeachable. You should be able to state unequivocally and document clearly that your company's risk exposure was known and analyzed, and the decision to accept that exposure was made on an informed and deliberate basis.

Nobody can reasonably expect you to be right all the time; inevitably, some of the careful bets you place will lose. But every stakeholder can reasonably expect and insist that you make the best decision you can, weighing the information *(Risk Intelligence)* available at the time and the options at your disposal.

Quite simply, the success of the enterprise depends on it. We've said it before, but it bears repeating: *Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so.*

Every stakeholder can reasonably expect and insist that you make the best decision you can, weighing the information available at the time and the options at your disposal.

The road ahead

By design, this document provides a high-level view of *The Risk Intelligent Enterprise*, addressing broad concepts rather than detailed steps. As such, many readers who reach this point will ask the questions: "Where are other companies in their stage of development — especially within my specific industry?" and, of course, "Where do I go from here?"

The answer: Where you go next depends on where you are now. The *Risk Intelligent Enterprise* Maturity Model (figure 1, below) shows the journey that most companies will travel to become *Risk Intelligent Enterprises*.

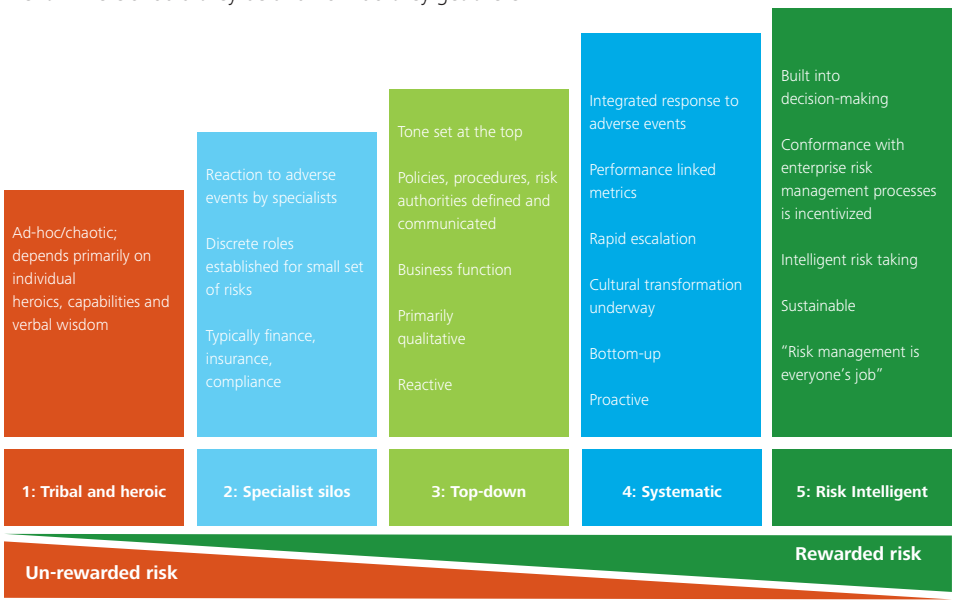
Companies at the earliest stages can begin by addressing the fundamental steps posed in the appendix of this document. Organizations further along the scale will benefit from the Deloitte's *Risk Intelligent Enterprise* whitepaper series that provides industry-specific benchmarks and a roadmap for addressing the people, process, and technology how-to's of effective risk management. The series provides a programmatic approach to *Risk Intelligence* from industry and functional perspectives. Contact your Deloitte practitioner for more details on this whitepaper series.

For additional information on the *Risk Intelligent Enterprise*, please visit www.deloitte.com/risk.

Figure 1

The Risk Intelligent Enterprise maturity model

How capable is your company today? How capable does it need to be? Every industry, company and division is probably at a different stage of development. Where should they be and how do they get there?



Appendix — Fundamental steps

As noted previously, every company is unique, and intelligent risk management practices must be tailored to specific circumstances and needs. Some companies may find themselves well-along *The Risk Intelligent Enterprise Maturity Model* (see figure 1, page 11), while others may be in the initial stages.

As such, some of the steps included here may apply to your situation; others may have been addressed long ago. But all are key to creating the *Risk Intelligent Enterprise*.

1. Establish an overall framework, policy, and process for assessing and managing risk.
Does your company have an overall risk framework that addresses the risks the company is exposed to, how it views those risks, and how it manages them? Does your company have a risk policy? If it is listed on the New York Stock exchange, it must. The NYSE requires that the audit committee discuss with management the major financial risk exposures and the steps taken to monitor and control such exposures; also that the audit committee should be satisfied with the company's risk assessment and risk management processes. Risk factors that affect business, operations, industry or financial position should be described in plain English.

Do you have a process? Policies alone won't create a *Risk Intelligent Enterprise*. Directors should challenge management to demonstrate a systematic and disciplined process for risk identification, assessment, and prioritization; risk response; and risk monitoring and reporting. Executives should provide regular updates to the board and audit committee to demonstrate that their risk processes perform as expected and that reports on risk are reliable.

2. Identify key risks and vulnerabilities and the plans to address them. Assess value and determine where risks could impact value.
Engage in scenario planning: What are the alternative futures? What could cause you to fail? What are the mission-critical risks that could have the highest adverse impact on company value and strategic objectives? Where are you most vulnerable? What are the early warning signals and how will you recognize them? A key characteristic of effective *Risk Intelligence* is the ability to separate irrelevant from relevant information.

An important consideration in this area is the problem of multiple risks in combination. Consider how risks may interact, keeping in mind that risks don't respect organizational boundaries. What are you doing to address those risks? And how do you know it's working?

(Remember the lesson of the Deloitte Research study cited earlier: Most major losses at the global 1000 companies surveyed were the result of multiple high-impact but low–likelihood risks.)

3. Establish your risk appetite. Determine how much risk you have taken on. Decide whether you can take on more or should reduce risk.
Once you have decided to take a risk, how much risk is your company willing to accept? What is your capacity to bear risk? How much of your capital or existing assets are you willing to put at risk at any one time? How much risk are you willing to take to achieve future growth? How resilient are you in the face of an extreme event?

The key question that is often overlooked: Are you intelligently taking enough risk? The implications of practicing risk avoidance without pursuing rewarded risk-taking may include missed business opportunities, decreased competitiveness, and, ultimately, the demise of the business. Businesses must take risks to be competitive.

4. Decide who has responsibility and authority to take risk on behalf of the company.

Surprisingly, a number of companies fall short in this area; the roles and responsibilities around risk are often unclear and misunderstood. How will responses be integrated and coordinated across the entire enterprise? Specificity is a necessity: What powers are reserved for the board? Who can commit the company? When can authority be delegated? What are the escalation procedures for "red flag" risks? Who, if anyone, has the ability to "bet the farm"?

5. Determine your capability to manage risk on an integrated and sustainable basis.

The *Risk Intelligent Enterprise* cannot be achieved overnight. In most cases, organizations will move through distinct stages of development, as shown previously in figure 1 on page 11. The lowest state of risk management capability is characterized by an ad hoc (if not chaotic) approach that depends highly on individual responses and often "heroic" efforts in the absence of more systematic approaches. Once specializations have emerged, subsequent stages will involve moving risk management out of "silos" and toward a fully integrated and coordinated response. The highest state of capability will build risk considerations into corporate strategy and the decision-making process, with an emphasis on risk-taking for future growth and reward as well as the protection of existing assets. In the fully developed *Risk Intelligent Enterprise*, risk management is viewed not as a project but part of the culture, the way of doing business. *Risk Intelligence is all about enterprise management.*

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.