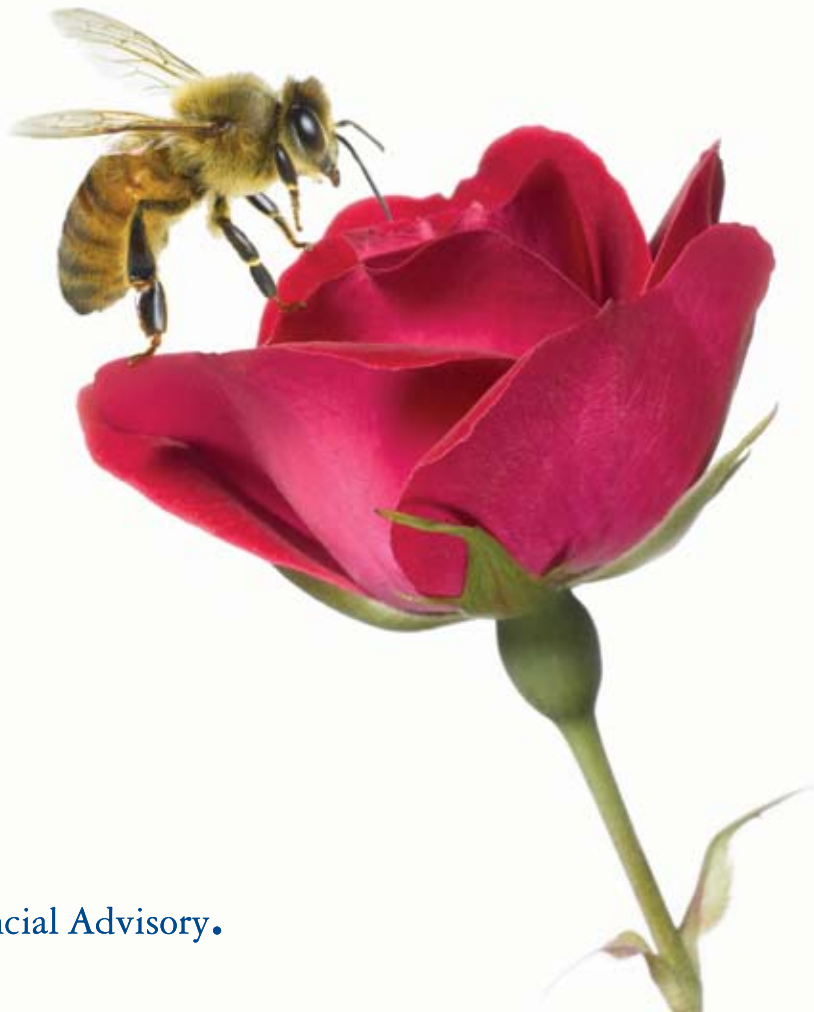


Putting risk in the
comfort zone

Nine principles
for building the Risk
Intelligent Enterprise™



Preface

The publication represents the first installment in Deloitte's series on the fundamental principles of Risk Intelligence. The papers in the series are intended to offer plain-English descriptions of the foundational elements of a Risk Intelligence program, as well as insights and practical steps you may consider for incorporating the concepts within your own organization.

On each of the following pages, you will find a statement describing a single principle of a Risk Intelligence program, along with an elaboration on the topic. In aggregate, we believe application of these principles will help create what we consider the epitome of enlightened risk management: The Risk Intelligent Enterprise.

Keep in mind that the application of these principles will differ based on your industry practices, regulatory schema, and organizational maturity. For example, in the financial services and energy industries, many of these principles have been discussed for over a decade and thus may seem elementary; but for many other industries, we see these principles just starting to be embraced. Regardless of what industry you are in, the Fundamental Principles still apply.

Although this paper is the first in our "Fundamental Principles" series, it is by no means our initial words on the subject of Risk Intelligence. In fact, we've published over a dozen related titles as well as numerous podcasts and webcasts. You may access all of this material free of charge at www.deloitte.com/RiskIntelligence.

Open communication is a key characteristic of a Risk Intelligent Enterprise. Consider sharing this whitepaper with the other executives, board members, and key managers in your organization. The issues and concepts outlined herein should provide an excellent starting point for a crucial dialogue on enhancing your organization's Risk Intelligence.



Uncomfortable risk

Like politics and religion, risk can be an uncomfortable topic of conversation. Understandably so, because many people unintentionally limit the parameters of the discussion.

You probably think of risk in terms of threats — bad things happening to your business. Not a pleasant subject of conversation.

But the discussion can flow freely if you consider the other side of risk, the one that applies to value creation — risk taking for reward.

Introducing new products; entering foreign markets; acquiring competitors — all are challenging endeavors, and if you don't properly manage the associated risks, you may not reap the potential rewards.

So consider adopting a more expansive definition of risk, one that gives equal weight to managing the risks related to growth and profitability:

Risk is the potential for loss or harm — or the diminished opportunity for gain — that can adversely affect the achievement of an organization's objectives.



Principle #1: In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.

A framework is a coat rack

When it comes to keeping your parka off the parquet or your cape off the carpet, the solution may seem deceptively simple: All you need is a hook.

But what's holding up that hook? In fact, the support structure will vary, depending on whether you're hanging heavy winter gear or gauzy summer fashions.

It might be helpful to think of your risk management framework in the same manner: something to hang your risk management program on.

A risk framework — such as COSO ERM, Turnbull, and ISO — provides a structure that helps you decide which opportunities to pursue and which hazards to avoid.

But the framework must be sturdy enough to support your risk management objectives. It must accommodate your unique strategies, initiatives, and organizational structure. And it must be adaptable to your industry and regulatory requirements.

There's no need to overanalyze. Don't get snagged on the selection of your risk framework. Just make sure it's something you can hang your hat on.



Principle #2: In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.

Symphonic risk management

Done right, risk management is a coordinated effort, as finely tuned as a symphony orchestra. In both risk and music, multiple roles are played simultaneously in often complex arrangements.

Of course, some people in your organization may not even realize they are part of the band. Your product development manager, IT supervisor, or deputy vice president responsible for M&A probably considers risk management somebody else's job.

Changing that mindset is a precursor to promoting Risk Intelligence in your organization. You'll need clear messaging at the individual level to convey what Risk Intelligence means; why it is important to the organization collectively and to employees individually; and what your people actually need to do on a daily basis.

This effort requires clear communications; a strong risk-focused culture; reward programs that incorporate risk-related objectives; and learning programs to promote intelligent risk management.

In sum, it's needs to be a harmonious collaboration. Here's what the score looks like:

- The board sets the tone (see page 6).
- The executive wields the baton (page 7).
- The business units play the music (page 8).
- Certain functions (HR, finance, IT, legal, tax) support the concert backstage (page 9).
- Other functions (internal audit, risk, and compliance) monitor the performance (page 10).



Principle #3: In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.

Follow the same map



Risk specialists tend to behave like any subculture: They stick together. They share similar beliefs, rituals, and habits. They develop their own dialect.

But practices that sustain, say, an indigenous people may not be ideally suited to the risk managers of a multinational corporation.

Not to say that specialization is unnecessary. Quite the contrary: effective risk management would not be possible without it. Rather, risk specialists just need to poke their heads outside their silos once in a while. Risk doesn't exist in isolation, so risk managers can't either.

To effectively and efficiently manage risks and reap the rewards, organizational silos must be bridged. The bridging process means creating a common infrastructure; it means that all the business units and functions use the same supporting technologies and processes where possible and practicable. It involves *synchronizing* — coordinating across institutional boundaries; *harmonizing* — ensuring that risk managers all speak the same language and define risk in the same manner; and *rationalizing* — eliminating duplication of effort.

Use tools like The Risk Intelligence Map™¹ to facilitate your discussions; it may get you thinking and talking about risk in ways you never envisioned. Draw upon your risk framework to help standardize your approach. Develop a risk catalog to inventory your most critical risks.

Common technology, metrics, processes, and terminology will transcend your siloed subculture.

Principle #4: In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.

¹For information on Deloitte's Risk Intelligence Map, contact your Deloitte practitioner. See page 13.

The mushroom treatment

Some boards of directors are subjected to “The Mushroom Treatment,” an approach that is summarized, in abridged form, below:

“Keep ‘em in the dark ...”

Such treatment should obviously be avoided. In the U.S., boards have a fiduciary responsibility to ensure that management has appropriate processes in place to manage risk. This duty cannot be executed in the absence of light.

To fulfill their responsibilities and to provide value, board members should:

- *Put risk on the agenda.* Make time for risk before risk demands it. Every board meeting is not too often to discuss risk.
- *Inventory the current risk structure.* How are risks managed? Are silos being bridged?
- *Summon the management team.* Engage in periodic risk dialogue. Identify risks that will prevent the organization from executing on its key strategies.
- *Discuss risk scenarios.* Where do the greatest opportunities lie? What could thwart the organization’s strategic objectives?
- *Check organizational appetite — and diet.* Determine how much risk the organization is able to take on. How much is it *willing* to take on? And how much is it *actually* taking on? Are these in line?
- *Get reasonable assurance.* Ask management: How confident are you? Why?
- *Get independent reassurance.* Have internal audit or an outside consultant evaluate the effectiveness of the full risk management program. Can management’s assurances be relied upon?



Principle #5: In a Risk Intelligent Enterprise, governing bodies (e.g., boards, audit committees, etc.) have appropriate transparency and visibility into the organization’s risk management practices to discharge their responsibilities

“We manage risk every Friday”



Don't laugh — that's an actual quote from a real business executive. And here's the sobering reality: If you treat risk management as a part-time job, you might soon find yourself looking for one.

We noted earlier that everyone has responsibility for risk. But if you're a member of the executive team, this obligation is ratcheted even higher. You are tasked with tone, direction, design, and metrics.

Inherent in your executive role is leadership and authority. And you need to exercise it: To get people thinking about risk taking for reward. To push risk management through all the layers of the organization. To set expectations. To ensure accountability. To engage the board. To drive change. To establish a Risk Intelligent culture.

An ambitious agenda, to be sure. How can you get it all done? Here's a good place to start: Form a Risk Intelligence group — an executive-level risk committee — to bring better risk insights to your management team and help create a Risk Intelligence program.

In some organizations, a key member of this executive-level Risk Intelligence group is the chief risk officer. Sitting at the table with other top executives, the CRO helps develop policy and common approaches that are rolled out to business units; communicates and monitors the organization's risk appetite; and reports risk information to the management and board-level oversight functions. Some organizations may choose a more expansive role. The style of the CRO varies considerably and needs to match that of the organization and its risk philosophy. Some may choose a business partner, some a facilitator, some a traffic cop.

Whatever the role, you can be sure: None of them work only on Fridays.

Principle #6: In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.

Risk lives here

OK, so everyone's responsible for risk. But who "owns" it? In our view, the business units hold the title and deed.

The ownership question causes plenty of confusion throughout organizations, so it might be helpful to state it in simple terms:

If you own the business unit, you own the risk.

In other words, if you are accountable for the success of a business unit, you have primary responsibility for the day-to-day management of the risks associated with that unit. (Of course, this does not absolve other members of the business unit from carrying out their risk-related responsibilities.)

What does ownership entail? Among other things, risk owners have the responsibility to identify, measure, monitor, control, and report on risks to executive management; promote risk awareness; and reprioritize activities as dictated by effective risk analyses.

Yet, just as a property owner must abide by municipal zoning regulations, business unit managers must operate under certain constraints. For example, they don't choose the framework — they live within it. They don't determine the organization's risk appetite — they stick to the diet. And they don't unilaterally "bet the farm" — they tend to the crops. In fact, if they can place that bet without oversight or limits, you've got a serious risk infrastructure issue.



Principle #7: In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.

The risk support system

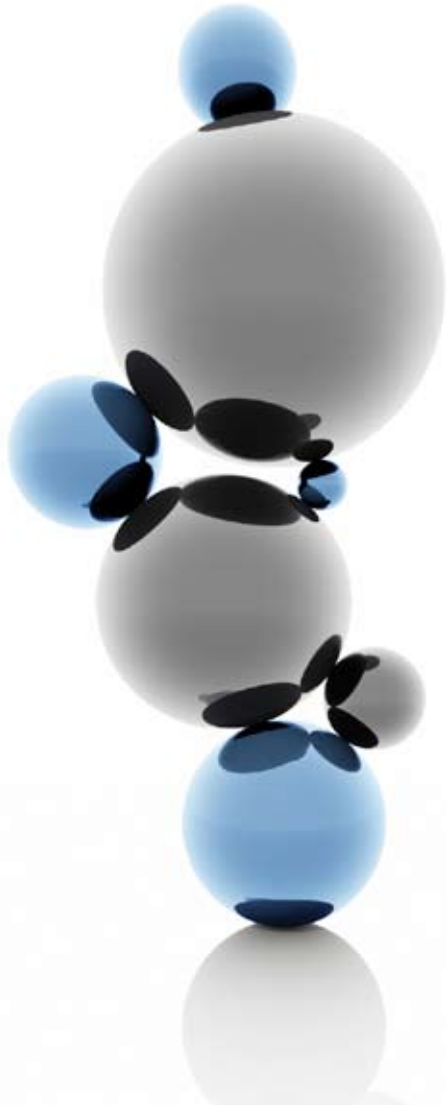
Certain functions, including finance, legal, HR, tax, and IT, differ from the business units in that they don't just *own* risk management — they also help *support* it. The role of these functions is inherently different than either that of the risk “comforters” (described on the next page) or the business units (discussed on the previous page).

Like the business units, these functions bear primary responsibility for the risks that originate within their operations. For example, finance takes the lead on Sarbanes-Oxley-related risk, IT on technology-related risk, legal on litigation risk, and HR on talent and human resource risks.

At the same time, they also have risk responsibilities that transcend their functions. For example, finance, through its Sarbanes-Oxley role, may have a broad and sophisticated risk assessment capability that can be leveraged. Meanwhile, IT is pervasive and thus can play a role in helping other parts of the business monitor and mitigate their risks. HR may use employee engagement surveys, exit interview results, and other information to identify risk areas of emerging concern.

These ubiquitous functions are responsible for developing and enforcing company-wide policies, procedures, and controls that help mitigate risk. They support each business unit and help them understand their requirements for intelligent risk taking for reward. They collect key information for management and perform risk mitigation analyses.

It is important that these key functions join the risk team by having articulated roles in the risk framework and by participating in risk committees and other key risk forums.



Principle #8: In a Risk Intelligent Enterprise, certain functions (e.g., finance, legal, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.

The comforters

When it comes to risk management, certain groups carry a unique mandate — namely, the internal audit, compliance, and risk management functions. One might describe “comfort” as one major responsibility of these functions: to provide reassurance that the internal control and risk structure operates effectively (thereby helping the executive team and board members sleep at night).

This role sets them apart from every other entity within the organization. These comfort groups are not operational in nature: They have no responsibility for setting and directing the operations of the business. Rather, they exist to monitor and enhance the effectiveness of the organization’s risk management activities.

Of course, specific roles and responsibilities vary from one organization to another. Some groups do far more than provide reassurance; others are more proscribed in their activities. Potential roles that expand the job description include the following:

- *Visionary*: assessing not only the current state of risk management, but peering ahead to help management divine future risks and opportunities.
- *Dietician*: determining whether the organization’s risk diet matches its appetite.
- *Aggregator*: ascertaining whether the organization is appropriately considering how risks interact and cascade.
- *Efficiency expert*: investigating means to eliminate inefficiencies in risk management.

- *Champion*: advocating for resources related to risk-taking for reward: addressing those risks associated with increasing profitability and increasing shareholder value.
- *Advocate*: drawing attention to and advocating for resources to address risk areas deemed insufficiently covered.
- *Subject matter resource*: providing deep knowledge and expertise in key risk areas, such as fraud.
- *Troubleshooter*: getting involved in control remediation and design; helping to conduct and interpret risk assessments.



Principle #9: In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization’s risk program to governing bodies and executive management.

Be risk intelligent



In the recent past, finance and energy industries have been perceived as paragons of sophisticated risk management. Then the subprime crisis swept billions from corporate balance sheets and Katrina knocked platforms and derricks offline in the Gulf.

Books have been written on what went wrong. But here's a quick summary:

- 1) The potential interaction of multiple risks was underestimated or disregarded.
- 2) Probabilistic modeling was overemphasized; shortcuts were taken; scenario planning was underutilized; transparency into potential issues was absent.
- 3) Risk managers were isolated in silos.
- 4) Warnings were ignored; those who delivered them were dismissed as naysayers or criticized for not being team players.
- 5) A short-term perspective with a single-minded focus on making the quarterly numbers predominated.
- 6) Companies lacked a comprehensive approach to firm-wide risk management; authority and responsibility were poorly controlled and defined.
- 7) Risk management often focused on compliance rather than performance, leading to inadequate assessments and responses.

All were significant breakdowns, to be sure, yet it would be an even greater failure if companies responded by turning risk averse. Risk taking for reward is a fundamental precept of capitalism and should be encouraged. But the pursuit of organizational success must be handled skillfully.

In other words: It's time to become Risk Intelligent.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.