Deloitte.

RiiR
The Tom Vesey Group
Managing Risk to Reputation

A Risk Intelligent view of reputation

An outside-in perspective

Risk Intelligence Series
Issue No. 22

Preface

This publication is the 22nd whitepaper in Deloitte's series on Risk Intelligence. The concepts and viewpoints it presents build upon those in the first whitepaper in the series, The Risk Intelligent Enterprise™: ERM Done Right, as well as subsequent titles. The series includes publications that focus on roles (The Risk Intelligent CIO, The Risk Intelligent Board, etc.); industries (The Risk Intelligent Technology Company, The Risk Intelligent Energy Company, etc.); and issues (The Risk Intelligent Approach to Corporate Responsibility, Risk Intelligence in a Downturn, etc.). You may access all the whitepapers in the series free of charge at www.deloitte.com/us/RiskIntelligence.

This particular paper in the series has been developed in collaboration with RiiЯ Ltd., a firm specializing in managing risk to reputation issues for businesses and other organizations. It contains ideas and concepts from RiiЯ.

Unfettered communication is a key characteristic of the Risk Intelligent Enterprise. We encourage you to share this whitepaper with colleagues – executives, board members, and key managers at your company. The issues outlined herein will serve as the starting point for the crucial dialogue on raising your company's Risk Intelligence.

Contents

"Who steals my purse steals trash…But he that filches from me my good name, robs me of that which not enriches him, and makes me poor indeed."

— William Shakespeare

The strategic importance of reputational risk

Quick-glance overview

- Reputational risk is now regarded as a "meta risk," standing at the forefront of key strategic and operations concerns, right alongside new competition, technology failures, talent issues, and changing regulations
- Traditional risk approaches often don't work — they focus too much on risk avoidance or minimizing asset losses, and exclusively on an "inside-out" view of circumstances; a Risk Intelligent approach takes an "outside-in" perspective, relating enterprise reputation matters to strategic outcomes, value protection *and* value creation
- Effective management of risks to reputation involves a three-step process of internal discovery, analysis of stakeholder and marketplace threats and opportunities, and proactive management of actions designed to protect and enhance reputation and value
- New, specialized diagnostic tools can help map "hot spots," gauge impacts, and measure effects
- A Risk Intelligent, proactive course of action helps harness both known and unknown hazards and can help ensure that your reputational risk strategy aligns with your business direction

A number of large, respected companies — and their decision makers — have come under fire in recent years for their handling of product or service failures and other management or compliance problems that garnered high-profile media coverage. Few, if any, industries have escaped such scrutiny. Since much of the press and Internet attention these incidents receive is due to the familiarity of the brands involved, it would not be surprising if the leaders of those affected companies cited *reputational damage* as the most costly loss coming out of these misfortunes — topping liability payouts or declining sales and disappointing profits that may also have followed.

Despite evidence that corporate leaders have been aware of the seriousness of reputational threats for some time, a number of companies have only recently begun to take action. For example, an Economist Intelligence Unit[1] study underscored significant concern about reputational risk among members of senior management in 2005. A total of 269 chief executives were given a choice of 13 categories of potential risk to their organization's business operations. Categories ranged from natural hazards to IT system failures, new or existing regulations, human capital issues, crime, and threats to company reputation. Respondents indicated that reputational risk, or events that undermine public trust in products or brands, stood squarely at the forefront of business concerns, beating out the next closest contender by more than 10 percentage points.

[1] Economist Intelligence Unit, white paper, 2005

Reputation as a meta risk

As executives in the study recognized, reputation, quite simply, can make — or break — a company. Reputation is an important factor across all four major risk areas of the Risk Intelligent Enterprise — strategic, operational, financial, and compliance — particularly of the former two, strategy and operations, because it is a constantly evolving and fully embedded part of why and how the company achieves its objectives. This catapults reputational risk to what we call a meta risk, or a potential menace to fundamental business strategy, a prospective peril of otherwise stalwart operations, and possibly an even greater hazard to organizational survival than a financial restatement or problematical findings in a compliance report. Traditional risk management techniques aren't adequate for countering today's killer risks, because they focus almost exclusively on risk avoidance and an inside-out perspective on threats.

A Risk Intelligent approach recognizes that value protection and value creation depend on the enterprise's ability to avoid unrewarded, or downside, risks and pursue rewarded, or upside, risks successfully; protecting what you have by being more resilient, and creating new value by being more agile. This approach begins with constructively challenging one's own assumptions. It is refined by determining whether potential unexpected events are threats, opportunities, or both. Risk Intelligent solutions differ from conventional solutions in that they: recognize the unprecedented levels of uncertainty and turbulence that confront business decision makers; know that loss or harm may be financial or non-financial (e.g., reputational); and understand that there is a price to be paid for lost or missed opportunities, as well as for damaged or lost assets. In the case of reputational risk, Risk Intelligence focuses on identifying key drivers of, or impediments to, the desired reputation, links rather than separates value and risk, and introduces a process for raising awareness and improving opportunities for success.

"Traditional risk management techniques aren't adequate for countering today's killer risks, because they focus almost exclusively on risk avoidance and an inside-out perspective on threats."

A case of reputational risk consequences

It seems that nearly every business day brings news of an oversight or misstep that shines a bright light on the need for a new way of looking at reputational risk. When tragedy and misfortune strike, some of the largest and most otherwise well-equipped organizations have realized that they overlooked reputation as a performance indicator and therefore a serious risk condition. Yet decision makers at some companies don't seem to be focused on branding issues or threats. Polling conducted with more than 1,100 executives from around the U.S. during a Deloitte webcast on brand resilience in May 2011, for example, revealed that only 24% of the companies represented by participants formally measure and report on brand value. Furthermore, fewer than 22% of the webcast participants thought it either likely or highly likely that negative information about their brand will show up on social media, such as Twitter, Facebook, or YouTube, in the coming year.[2]

This may have been the belief of executives at a major pizza delivery chain before an unexpected social media event created major disruptions to their operations. On a slow delivery night, two bored kitchen employees "pranked" the company's food handling practices (explicitly depicting them as unsanitary) via a faked video viewed by more than one million people on YouTube — and further shared with millions more through social media and press coverage.[3] Management at first resisted taking an aggressive response. But consumer reaction was so strong that many observers thought the company might suffer serious financial consequences for some time, or possibly even fail. A seemingly innocent stunt caused a precipitous dip in share price and had loyal customers second-guessing the reputation of — and their relationship with — the company.

But with the use of some effective reputation assessment and strongly proactive stakeholder engagement tools, management countered the company's misfortune with an effective, proactive campaign involving customers and employees. Ultimately, actions taken helped boost the chain's stock price with a level of growth unmatched by any other quick service restaurant in the same time frame. In fact, as of late 2010, they had continued to out-pace their competition.

While this response was a rare event in reputational damage control, very few companies proactively manage the link between risks to reputation and company strategy, or know how to incorporate reputational risk concepts into their strategic risk program. Yet a damaged reputation has serious implications that can include negative impact on share price, costly regulatory investigations, and measurable decline in employee and customer loyalty — among many other undesirable outcomes.

Responsibility for managing risk to reputation should reside with the board of directors and senior executive management — and not be delegated to public relations or marketing departments. Managing risk to reputation is about *fundamental perceptions of the company's contributions, value, and strategic direction*. It is up to the board and senior management to be a driving force in optimizing an organization's "readiness" for reputation issues — looking "outside" of the company for reputational risk issues that may generate impact from a regulatory, competitive, supplier, investor, or media perspective, developing and embedding reputation "danger detection" systems throughout the enterprise, and proactively fine-tuning the speed and quality of the organization's response to an unexpected and potentially damaging development.

[2] Deloitte webcast, "Brand Resilience: Protecting Your Brand Assets from Saboteurs in a High-Speed World," May 18, 2011.
[3] *Brand Resilience: Managing Risk and Recovery in a High Speed World*, by Jonathan Copulsky, 2011

Re-thinking risk management: an outside-in view

This paper offers insights for shaping an effective strategy and program around reputation risk. This first section sets the stage for why the right perspective is critical, and the second part provides a roadmap for establishing a reputational risk program.

In particular, we hope board members and senior executives will use it as a springboard for developing a more complete understanding of the role of enterprise reputation as it relates to both value-killer risks and game-changing opportunities — and that this knowledge will serve them well in not being blindsided by the unexpected.

For many companies, this will require re-evaluating their current risk management program. Traditional ERM approaches have focused boards and C-Suite executives on avoiding risks and protecting assets. These are important objectives, of course, and necessary for preserving the enterprise, but they focus too much on risks *within* (that can be seen or foreseen by) the organization and do little to take an outside-in view, that is, those risks that can be seen and foreseen by observers from outside the company — an organization's stakeholders. Time and again, catastrophic risk arrives completely unexpectedly. This is generally because only the inside-out perspective has been considered. Think, for example, of food companies dealing with obesity or automobile manufacturers addressing product flaws. An outside-in approach helps prepare the organization for unexpected developments or for spotting game-changing possibilities prior to such developments gaining momentum and velocity. What is new today is the need for a 360-degree risk overview that effectively incorporates an outside-in risk perspective with inside-out Risk Intelligence.

The 2011 Edelman Trust Barometer, the 11th annual edition of this trust and credibility study ("Study") by the Edelman global public relations firm, pointed out how trust factors and perceptions can seriously impact corporate reputation. Results in their 2011 Study demonstrated that when a company is trusted, 51% of stakeholders will believe positive information about the company after hearing it one or two times, while only 25% will believe negative information about the company after hearing it one or two times. Distrusted companies, however, do not fare so well: 57% of stakeholders will believe negative information and only 15% will believe positive information upon hearing either negative or positive information about the company once or twice. The same Study also highlights how trust in a company can drive key bottom-line decisions including proclivity to buy products or services from, or stock shares in, a trusted company, and propensity for recommending those products, services, and investments to friends or colleagues. There was a proportionate negative response in these areas for distrusted companies. In short, there is a very real, commercial value in trust and reputation issues.

In a December 2010 paper developed by COSO called "Developing Key Risk Indicators to Strengthen Enterprise Risk Management,[4]"the authors concluded that classic ERM and inside-out approaches are not enough to maintain a sharp focus on emerging risks in today's business world. Rather, they emphasized the criticality of external objectivity and of gathering and analyzing data and insights from all key stakeholders. Outside-in perspective is vital and external data is highly relevant, the authors said, noting that "many root-cause events and intermediate events that affect strategies arise from outside the organization."

[4] See *Developing Key Risk Indicators to Strengthen Enterprise Risk Management*, developed by COSO, 2010.

Figure 1: Key stakeholders of reputational risk

Illustrates the key stakeholders of reputational risk that boards and c-suite executives should consider in their 360-degree approach to risk management and their potential areas of impact on the organization. These will vary according to each organization, but serve here as a base for reflection.

Traders	• React fast and could initiate downhill spiral in share price
Analysts	• Question future financial results and change recommendation (buy/sell)
Shareholders	• Sell holdings and provoke fall in share price
Partners/suppliers	• Upstream, quality suppliers/subcontractors turn to others
Customers	• Downstream, clients/customers look elsewhere to fulfill needs
Staff	• Top talents can be lost to competition due to demotivation • Unable to hire needed competencies
Regulators	• Increased scrutiny leads to undue burden on all staff and stress on the organization
Investors	• Money becomes scarce for long-term project development • Cost of finance (if available) rises sharply
Rating agencies	• Place company on alert, leading to potential downgrade • Cost of finance goes up

Source: RiiЯ Ltd.

"What is new today is the need for a 360-degree risk overview that effectively incorporates an outside-in risk perspective with inside-out Risk Intelligence."

The Risk Intelligent Enterprise™ framework

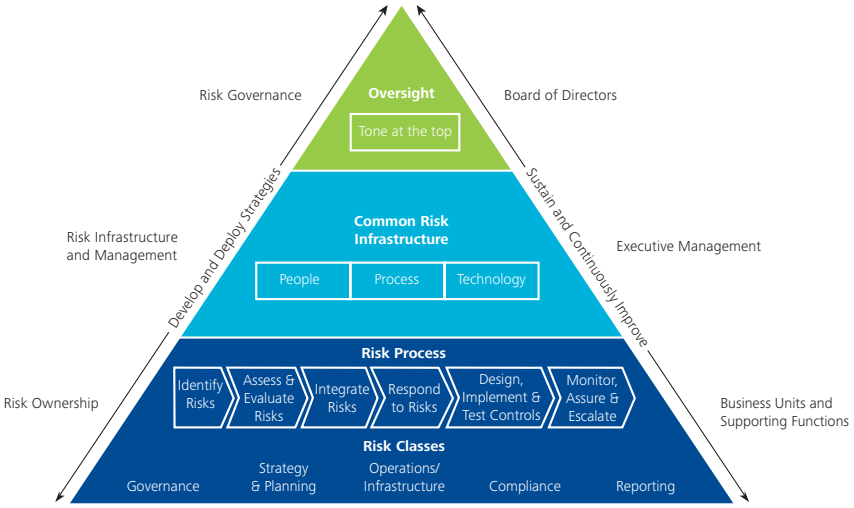
The Risk Intelligent Enterprise approach offers a practical framework, or roadmap, for enabling directors and management to focus simultaneously on value protection and value creation. Deloitte's framework and insights are based on *Nine fundamental principles of a Risk Intelligence program*, which are listed on the inside back cover of this publication. Effectively, Risk Intelligence takes a dynamic view of all the dimensions of risk, imbuing decision makers with a special skill set that helps build uncommon awareness and flexibility, such as a bias against assumptions, vigilance for rooting out perceptual "blind spots," and a keen ability to connect trends, people, and entities in ways that expose threats and exploit opportunities —either of which may predictably or unexpectedly materialize.

A Risk Intelligent Enterprise focuses not solely on risk avoidance, but also on risk-taking as a means to value creation. This approach recognizes the need for an integrated risk management program that embeds capabilities throughout all levels of the organization. The framework shown in Figure 2 below depicts a Risk Intelligent organization where:

- Leaders incorporate a broad outlook on risk into strategic decision making
- The board ensures that appropriate risk management controls and procedures are in place
- Systems, processes, and people are in place to act on intelligence in a timely and coordinated manner
- A consistent approach is used across the enterprise to manage all types and classes of risk effectively and efficiently

More than ever, business leaders must adopt the watchwords "expect the unexpected" and prepare their organizations accordingly to meet whatever challenges the unforeseen may present. So-called "bolt-on" risk management solutions no longer work. The way forward starts at the top of the governance/management "pyramid" with directors and senior executives establishing the organization's risk appetite and tolerances and putting in place the philosophy, framework, tools, and methods that drive the risk management approach through every level and role in the organization. Everyone becomes to some degree a "risk analyst," being alert to signals about shifts in reputation or reputational drivers. The better everyone understands where the company is going and how it plans to get there, the better everyone will be at recognizing potential strategy killers.

Figure 2. The Risk Intelligent Enterprise™ framework



Effectively managing risk to reputation

Setting up a program to manage risk to reputation

In our experience, a successful approach to managing "risk to reputation" is to build the methods and processes developed by RiiR into the Deloitte Risk Intelligent Enterprise™ framework. The RiiR program has three phases which are described below. The true value of a risk to reputation program is to integrate an outside-in perspective into the enterprise risk program, providing a holistic overview of major and potential risks.

Phase 1. Discovery

To be successful in understanding the outside-in perspective, it is crucial to start by understanding clearly the view from the inside of the organization. So, key to the discovery phase is a detailed examination of the firm's current view of its strategies, risks, and vulnerabilities. This helps ensure that, when the program is launched, the "known knowns" and the "known unknowns" are fully explored through a series of in-depth interviews conducted with C-Suite executives:

- CEO: The major enterprise strategies and their underlying assumptions (this informs the risk to and of the strategies)
- CFO: The financial profile of the organization, its record with the markets (under/over-delivery on expectations); outlook for sector and firm
- CRO: The key risks the firm is monitoring; key industry threats and opportunities
- COO: The major vulnerability points that exist within the organization; this could range from facilities, to outsourcing partnerships or even sales channel over-dependence
- CMO/CCOs (Chief Marketing Officer/Chief Communications Officers): The competitive positioning and pressures in the industry
- CHRO: Exposure to the battle for talent, as well as weaknesses in recruitment or staffing profiles
- OGC: Regulatory and IP exposures are critical to integrate as well

From these exchanges, the organization's key stakeholders are identified, those who will provide the outside-in perspective. Desk research complements this to identify other stakeholders (sustainability indices, Non-Governmental Organizations, Department of Justice, etc.), whose impact on sector and corporate reputation might be vital. What RiiR calls "Listening Posts" are then indentified to harvest the opinion of all stakeholders from such diverse sources as staff and analyst blogs, industry forums, academic papers, media commentary, direct interviews, and the full range of social media.

Discovery culminates in a presentation to management of the inside-out perspective and the overall program is ready for launch.

Phase 2. Baseline

In the second phase, key stakeholders are engaged to help assess the first outside-in perspective. Typically, this might cover regulators, financial and sector analysts, and local communities based around partners, customers, staff, suppliers, legislators, NGOs and other agencies.

A variety of techniques can be deployed to gather intelligence from the different audiences involved. The key is to gauge, from the various perspectives, the perceived impact of the firm's reputation drivers on major enterprise strategies. For example, is an organization's weakness in environmental care jeopardizing its strategy to explore an eco-sensitive area? Or, is there emerging concern over an organization's products relative to impact on the public health?

The baseline report focuses on the known knowns and the known unknowns. It analyzes threats and opportunities to strategy on an enterprise level, the breakdown of those threats by stakeholder, and by reputation driver. It looks at interconnected threats across the various listening posts and stakeholder groups, which might individually seem innocuous but, when viewed together, represent threats requiring action.

During the baseline phase, analysis of the unknown unknowns begins and includes searching Internet web dialogue — from blogs, forums, websites, or other social media platforms — to detect potential threats and opportunities to strategic execution and relating those findings to reputation drivers.

The key output of the baseline phase is a gap analysis of how the organization's stakeholders view reputational impacts on strategies, versus management's objectives. It sets the agenda for a program of proactive management of threats to strategic execution and opportunities for advancement. It provides a benchmark for bridging the gap over time.

Baseline culminates in a presentation to management of the outside-in perspective.

Phase 3: Proactive management of risk to reputation
By this time, the techniques of outreach and research are established and the learnings of the discovery and baseline phases are put into action. There are three areas of focus at work:

- Anticipation: Of threats to strategy and opportunities for enhancement
- Analysis: Of trends which may lead either to threats or opportunities
- Action: On reputational levers and corporate behaviors to assure successful strategic execution

This is effected through three reporting mechanisms:

- An alert service of emerging risks, picked up by software and vetted by humans, for operational management
- Online reporting or Risks to Reputation and opportunities for strategic enhancement for senior management
- Quarterly presentations to top management of major trends requiring change to corporate behavior that could impact strategic outcomes

The pay-off for effective management of the risk to reputation program is greater confidence in strategic execution by understanding and integrating the external risks and opportunities. The goal is to end up with a program that puts the board and senior executives on the leading edge of knowing what might inhibit — or advance — the company strategy and then be prepared to act accordingly.

One key distinction between leading-edge risk management approaches and outdated ones is whether the organization takes an inside-out or an outside-in view of itself. As described above, whereas an inside-out perspective ("how we view the world") once dominated risk management, today an outside-in perspective ("how the world views us") is the preferred approach to protect and enhance reputation. We believe that it is the absence of outside-in perspective that leads many organizations to be surprised when bad things happen — surprised by the event itself and then surprised again later at how the situation was handled. And because the entity's reputation can be either adversely or beneficially impacted by any

action, event, or situation, it is particularly important that risks to reputation are fully integrated into the core risk management framework. It is equally critical that everyone realizes that inaction can be as destructive as the wrong action. Regardless of the issue, it is not a good thing when key stakeholders recognize a risk to reputation before management acknowledges it. Efforts should go beyond customers of the affected product or service, too, encompassing employee engagement (they are both your first and last line of defense), providing reassurance to investors and analysts, and involving the broader public by using social media as a platform for reputational advocacy.

Risk Intelligence can be instrumental in supporting an outside-in perspective, identifying sources of opportunities and threats on an ongoing basis. A Risk Intelligent approach formalizes the system for assessing marketplace/ stakeholder perceptions of company strategies and how those perceptions align with the vision of the board and management. A Risk Intelligent approach identifies key drivers of, or impediments to, the desired reputation, and introduces powerful diagnostic tools and methodologies for raising awareness, monitoring progress, and enhancing opportunities for success.

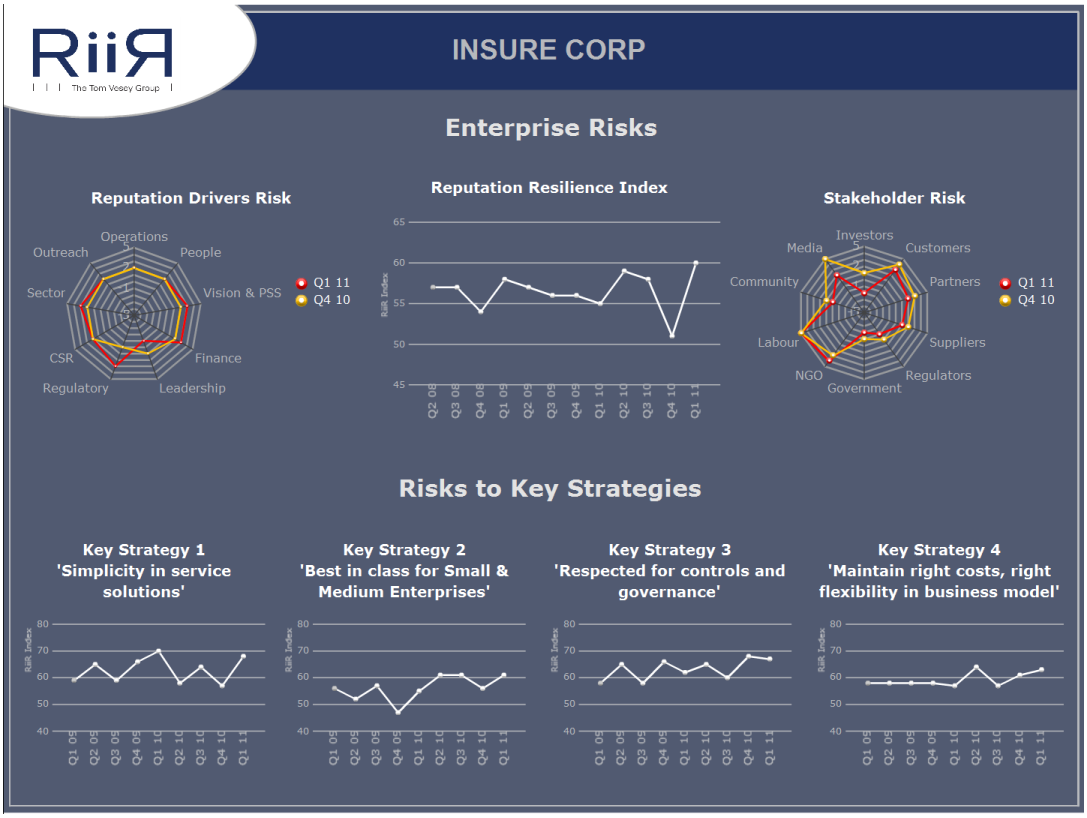
One such tool is the RiiR Reputation Model (see Figure 3 below) that essentially defines the company's key reputation factors (e.g., from vision and promises to regulatory profile and leadership activities) then correlates these factors with who is responsible for them and with the status of the perception of them by individual stakeholder groups (e.g. shareholders, media, employees, consumers). By cross-matrixing these factors — that encompass strategic, operational, compliance, and financial risks — with key time periods (e.g., quarterly reporting), company leadership can see change — good or bad — on an ongoing basis, thus enabling each constituency impacted by these factors to map hot spots that deserve special attention and/or to gauge whether certain employed actions or responses are having the desired effect among stakeholder groups. This model epitomizes the concept of outside-in perspective and ensures that information about risks to reputation is both available within the organization and shared with all the right people. The end result is the ability for boards and the C-Suite to be able to make more informed decisions that impact reputation, faster.

Figure 3 RiiR Reputation Drivers' Chart

The management and governance challenge is often about gaining the most comprehensive view of complex and multifaceted factors that impact the company. It is essential that directors and management are in-sync on risk tolerances, especially when major internal changes occur — such as executive turnover; when business conditions shift — such as an increase in pressure on pricing; or when new strategies are considered — such as product innovations or entry to new geographic markets.

Having a framework that aligns "inside" intentions with outside analysis is a great place to start. Dashboards such as the RiiR model, below in Figure 4, help management make informed and insightful decisions; they also assist directors in providing informed and insightful oversight by asking the right questions and assessing management performance.

Figure 4. RiiR Dashboard — Insure Corp is a hypothetical entity.
Top line shows high-level trends in enterprise Reputation Resilience, Reputation Drivers, and Stakeholder Risk. Bottom line displays evolutions in risks to key enterprise strategies.



The benefits of an effective risk to reputation program

- To ensure the opinions and perceptions of the key stakeholders who determine reputational value are aligned with company strategy
- To ensure that reputational drivers are supportive of company strategies
- To enable proactive identification of threats and to create constructive reputation opportunities
- To enable inter-linked risks — currently passing under company radar — to be identified and acted on
- To effectively move beyond siloed thinking and behavior within the organization to the important perceptions of those outside by taking a 360-degree view of the organization and monitoring external sources of information
- To establish processes for challenging assumptions about the company strategy and the strategic implications for reputation of that strategy

Conclusion: Managing risk to reputation is a critical success factor

Most business people respect the extraordinary value of a good reputation and understand the inherent challenges of getting and keeping it. Reputation, after all, is one of those intangible attributes that can only be defined by what others perceive. It is won and bestowed, not bought and marketed. Thus, when a reputation is intact or even stellar, it can help keep a company ahead of the curve; on the other side of that coin, when things go wrong, results can be seriously dampened and chances for future growth spoiled.

If the opinions of customers, employees, analysts, regulators and other key stakeholders shift against a company, the negative impact wrought by a bad reputation can send shock waves through nearly every aspect of the organization — from recruiting the best talent to stock value and consumer opinion — up to and including its ability to survive. Companies involved in reputation-damaging events should turn outward, rather than inward, when trying to protect themselves from such events playing out in the marketplace and media.

The increasingly global and interdependent nature of today's marketplace makes management of reputation risks an even greater challenge than a decade ago. Business failures and embarrassments are not uncommon and seem to be getting increasingly difficult to predict or control. Technological interconnectivity via social media and 24/7 news cycles enables bad news to travel much faster than ever before, so controlling exposure and "the message" after the damage is done is equally difficult. Since reputational risks impact planning and decision making at the highest levels of the organization, they must be considered strategic risks, or threats to the company's ability to execute on its vision and operate effectively.

One thing is certain: governance and management leaders can no longer rely on training or experience alone to monitor reputation threats. Borrowing from Shakespeare's terminology at the start of this paper, keeping tabs on those who would filch one's good name in today's rapidly and constantly changing environment is a task far beyond any individual's or small group of individuals' ability to maintain. Risk Intelligence, therefore, is a highly inclusive and multidimensional concept that acknowledges that major shifts happen and provides the philosophy, framework, and tools that drive a proactive course of action that harnesses important marketplace and internal information to help ensure that your reputational risk strategy aligns with your overall business direction.

U.S. Contacts

Donna Epps
U.S Co-Leader
Governance and Risk Management
Deloitte Financial Advisory Services LLP
+1 214 840 7363
depps@deloitte.com

Scott Baret
Partner
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Rita Benassi
Partner and U.S. Tax Leader
Governance & Risk Management
Deloitte Tax LLP
+1 203 761 3740
rbenassi@deloitte.com

Mark Carey
Partner
Deloitte & Touche LLP
+1 571 882 5392
mcarey@deloitte.com

Michael Fuchs
Principal
Deloitte Consulting LLP
+1 973 602 5231
mfuchs@deloitte.com

Henry Ristuccia
U.S. Co-Leader
Governance and Risk Management
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Kevin McGovern
Managing Partner
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 617 437 2371
kmcgovern@deloitte.com

Sandy Pundmann
Partner
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Nicole Sandford
Partner
U.S. Center for Corporate Governance
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com

Nine fundamental principles of a Risk Intelligence program[5]

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.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.
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.
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.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
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.
8. In a Risk Intelligent Enterprise, certain functions (e.g., Finance, Legal, Tax, 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.
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.

[5] "Putting risk in the comfort zone: Nine principles for building the Risk Intelligent Enterprise™," Deloitte Development LLP, 2009. Available online at http://www.deloitte.com/view/en_US/us/article/6b929c9096ffd110VgnVCM100000ba42f00aRCRD.htm.