

# Rethinking Risk – Strategies for Today’s Changing Business Climate

David Moschella, Research Director, [dmoschella@csc.com](mailto:dmoschella@csc.com)

In the aftermath of the recent financial industry crash, many firms have taken a fresh look at their risk management approach. The formal Enterprise Risk Management (ERM) systems in the financial services industry were considered the most sophisticated in the world. That these systems failed spectacularly is clear. What is less clear is what these failures mean for the evolution of risk management across a broad range of non-financial industry sectors. More recently, the giant oil surge into the Gulf of Mexico has raised additional fears about the risks of using advanced technologies in challenging environments such as deep-water drilling. These two major disasters have raised many questions about the ability of both businesses and government to effectively manage complex economic and technological risk.

Yet even before these dramatic events, forward-thinking companies were already feeling the need to rethink their risk management approach in order to more effectively respond to rapidly changing business conditions. Whereas many companies once manufactured standalone products or provided discrete services, today they must deliver constantly changing technology-enabled offerings that are closely integrated into global supply chains and ecosystems. These ever-changing and technology-driven demands are creating very different and much more pervasive business risks that call for very different organizational responses.

From an IT perspective, the need to rethink risk has also been increasing for some time. Even before the financial crash, notions of IT risk were beginning to shift away from the traditional focus on system integrity and security, toward safely supporting emerging business requirements such as smart products, global collaboration and empowered employees. Whereas IT used to *support* business processes, increasingly, IT functionality *is* the business process. Additionally, IT, and particularly the internet, continue to generate their own rapidly changing risks as businesses become ever more dependent on IT, even as the risks of malware, misuse and cyber-warfare continue to grow.

These emerging business and technological challenges have made the topic of risk management timely, but also complex and pervasive. In our Rethinking Risk research project<sup>1</sup>, we have assessed the state of business/IT risk management today. First, we identified the lessons of the financial and oil spill disasters, as well as the new dangers coming from the internet. We then showed how companies are responding to these challenges, and how we see the topic of risk management evolving as business and technology become increasingly inseparable. The report concludes with a glimpse of some of the frontiers of advanced risk analysis, and some of the thinkers whose work we most admire. Below, we summarize two of our main findings: 1) the narrowing of the gap between business and IT, and 2) the pre-eminence of bottom-up cultural forces compared to formal risk management governance.

---

1. David Moschella, *Rethinking Risk – Strategies for Today’s Changing Business Climate*, CSC LEF, July 2010.

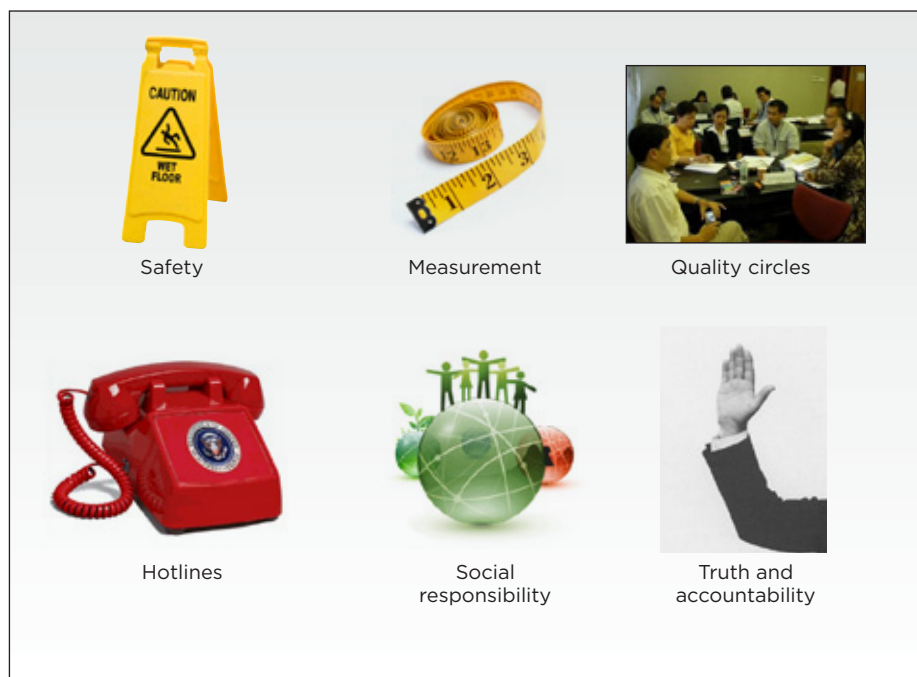
## 1. Narrowing the business/IT gap

In our report, we emphasize the distinction between *security risks* and *business risks*. The former can be greatly reduced; the latter really can’t. Business and risk are inseparable, especially in fast-moving markets, and thus firms that become too risk-averse will inevitably see their competitive position erode over time. Business people are used to trading off potential rewards against losses as the basis for taking calculated risks, but in the end they know that a certain amount of risk must be accepted. In contrast, Enterprise IT has too often viewed risk and security as nearly synonymous. This is one reason why it is often seen as the land of “No” – that is, no PCs, no LANs, no internet access, no iPhones, no Facebook etc.<sup>2</sup>

Recent events appear to be narrowing this gap. On the one hand, the ongoing recession as well as the financial and oil spill disasters have seriously dented business confidence and appetite for risk, making many business leaders much more likely to just say “No”. At the same time, accelerating technological progress and related business pressures for smarter, cheaper and more connected organizations are making it necessary for Enterprise IT to learn to say “Yes” more often. Taken together, these shifts suggest that the traditional separation between the lands of “Yes” and “No” could shrink considerably and perhaps permanently – an important step toward the true co-evolution of business and IT.

One thing both business and IT agree upon is that the word ‘risk’ is being used with increasing frequency inside their organizations, and that because of the financial and oil spill disasters, societal tolerance for business failures and trust in business values have been seriously shaken. A decade ago, the dot.com crash and the scandals at Enron, Worldcom and others led directly to Sarbanes-Oxley. The net effect was burdensome, but not transformative, regulation. Exactly what will come of today’s debacles remains to be seen, but the consequences will likely be much more significant. Companies, especially in America, are already preparing for a more regulated and punitive environment. This will have serious effects on both business and IT.

## 2. Bottom-up leadership



**Effective ERM leverages employee awareness**

While we are used to thinking about risk management in terms of formal corporate governance structures and processes, our research showed that these top-down efforts are less than half of the solution. While effective formal systems are certainly required – for auditing, compliance, insurance and many other reasons – most of the companies we spoke to said that no amount of top-down management could truly cover the myriad risks their firms face every day. It was essential that risk awareness and mitigation be deeply embedded into the operational culture of the firm.

2. See the LEF Research Commentary, *Leaving Behind The Land of No – Aligning Business and IT Risk*, April 2010

Some of the key components of such cultures are shown in the figure above. While the balance of these and other cultural aspects will clearly vary by both firm and industry, just about every organization can relate to these concepts. Having a culture of safety, where defects and problems are tracked and measured, and where employees drive improvements in quality and raise red flags when necessary, seems like common sense. But, as recent events have shown, sustaining a socially responsible business culture where employees are not afraid of speaking the truth to those in power, and where individuals are actually held accountable, is much easier said than done.

As always, lived values are more important than written rules. If the behaviours and systems of the firm put profits above all else, there should be no surprises when the incidents occur. Similarly, we have also seen how a company’s true values are inevitably exposed after a crisis occurs, and the inability of market leaders such as BP, Citicorp and Goldman Sachs to satisfactorily explain the ethics and values behind their behaviour has put their firms at even greater risk. This is why we believe that a company’s executives, employees and IT organization must see risk management in a consistent, informed and highly ethical manner. We hope our research helps toward this end.

### **Growing societal importance**

Both the financial meltdown and oil spill crises have shown that the challenges of risk management extend far beyond their meaning for any one firm. Our increasingly interconnected society faces risks on countless political, technical, environmental, demographic, military and cultural fronts. The huge disasters of the last few years, whether one sees them as criminal or not, have clearly changed government and societal tolerance toward both business and technological risk, and in many ways businesses have only themselves to blame. While there will always be business and industrial accidents, it’s hard to avoid the conclusion that the common denominator of both disasters was irresponsible levels of human greed.

Looking ahead, the big question is whether today’s understandable societal anger and distrust will prove transformative or temporary.

America, in particular, has historically had a willingness to accept large business and technology risks. Recent events have clearly diminished, but (hopefully) not permanently damaged this spirit. In contrast, China and other emerging nations have largely grown in confidence and ambition over the last few years. Whether these changes are temporary or permanent is now a matter of much intellectual debate. While history nearly always runs in cycles, the length of these cycles can be years, decades, or even centuries.

For better or for worse, the modern (at least Western) world has bet its future on the belief that a combination of moderately regulated private enterprise and major technological progress is the best way to both address ever-changing societal challenges and pursue a more prosperous future for all. Given the dizzying array of technological advances that are all but certain to come, it is important that confidence in this philosophy be successfully restored. This will require sustained but responsible risk taking, a balance that can only be achieved through a combination of top-down risk governance and the bottom-up operational culture of the firm. While issues of values, ethics and integrity will always be paramount, information technology will play an increasingly important role.

#### **Leading Edge Forum**

*CSC’s Leading Edge Forum (LEF) is a global thought leadership community that assesses the growing intersection between business and IT.*

*The research memorandum above is part of a monthly series of market commentary from the LEF Executive Programme, an annual retainer-based research and advisory service for CIOs and other business/IT leaders from large organizations. LEF Executive Programme members enjoy access to a global network of world-class subject matter experts, peer-level executive conferences, in-depth study tours and on-going advisory services.*

*For more information about the LEF Executive Programme, visit [lef.csc.com](http://lef.csc.com).*