



## **Becoming Risk Intelligent**

**by Henry Ristuccia and Donna Epps**

What separates the businesses that survive-and even thrive-in troubled times from those that fare poorly? Simple: an enlightened approach to risk management.

The following principles, which form the bedrock of a risk intelligent enterprise, can shore up an organization's resilience to risk and improve its agility when it comes to identifying and seizing opportunities. Regardless of your industry, global footprint or market cap, applying these principles can increase your company's odds of survival and improve its potential for the future.

1. Adopt a more expansive definition of risk and use it consistently throughout the organization. There are two sides to risk: one side deals with threats to your business; the other deals with risk-taking that leads to rewards. The risk intelligent organization considers and manages both value preservation and value creation.
2. Select a common risk framework that supports your risk management objectives. This risk framework-be it COSO ERM, Turnbull or ISO-must accommodate your organization's unique strategies, initiatives and organizational structure. It must also be adaptable to industry and regulatory requirements.
3. Define and delineate key roles, responsibilities and authority related to risk management. Risk management is a team effort. But some people in the organization are unaware that they even have a role to play. That is why clear communications, a strong risk-focused culture, learning programs that promote risk intelligent management and reward programs that incorporate risk-related objectives are required.
4. Support the risk responsibilities of the business units and functions by employing a common risk management infrastructure. Risk does not exist in isolation; therefore, risk managers cannot operate in secluded silos. The effective and efficient management of risk calls for a common infrastructure of shared technology, metrics, processes and terminology that transcends a siloed culture.
5. Provide boards and audit committees with the appropriate transparency and visibility into the organization's risk management practices. Without the necessary level of transparency and visibility, boards may find it difficult to maintain an inventory of the current risk structure, discuss risk scenarios, monitor the organization's appetite for risk, get reasonable assurance from management, and obtain independent reassurance from internal audit or outside consultants.
6. Charge executive management with the primary responsibility of designing, implementing and maintaining an effective risk program. The executive team is tasked with establishing the tone, direction, design and metrics for managing risk. Inherent in this role are setting expectations, pushing risk management through all layers of the organization, ensuring accountability, driving change, engaging the board and more.
7. Make business units responsible for both the performance of their business and the management of the risks they take. In simplest terms, if you own the business, you also own the risk. That means identifying, measuring, monitoring and controlling risks, as well as reporting on risks to

executive management. It also means reprioritizing activities as dictated by effective risk analyses and promoting risk awareness, all while operating within the framework established by executive management.

8. Verify that certain functions-namely, finance, legal, IT and HR-act as a risk-support system. While these functions bear primary responsibility for risks that originate within their own operations, they also have risk responsibilities beyond their functions. That is, they are responsible for developing and monitoring enterprisewide policies, procedures and controls that help mitigate risk. They also collect key information for management and perform risk mitigation analyses.

9. Ensure that internal audit, compliance and risk management provide objective assurance, monitor the organization's risk program and report on its effectiveness. While these functions have no responsibility for setting and directing the operations of the business, they should monitor and enhance the effectiveness of the organization's risk management style. By doing so, these functions provide reassurance that the internal control and risk structure operates effectively.

*Henry Ristuccia, a partner with Deloitte & Touche LLP, leads the governance and risk management practice in the United States. Donna Epps, a partner with Deloitte Financial Advisory Services LLP, is a member of the governance and risk management practice in the United States.*

**Reprinted from Risk Management Magazine.**

**Copyright Risk and Insurance Management Society, Inc. All rights reserved.**