Risk & Compliance | August 29, 2012 | CFO.com | US

Why U.S. Risk Managers Should Take a Hint from the Rest of the World

Let's face it: the ISO enterprise risk management framework used by most companies outside the United States is edging out the U.S.-favored COSO framework. Is there any point in clinging to the latter?

John Bugalla, Kristina Narvaez

For better or worse, ISO 31000 is on a path to becoming the global standard framework for enterprise risk management (ERM). Any organization that does business internationally should be using it for ERM guidance.

In fact, most ERM programs around the world, except in the United States, use the ISO framework, even though it was introduced just three years ago by the International Organization for Standardization. Most U.S. companies still use COSO, put forth in 2004 by the Committee of Sponsoring Organizations following the high-profile scandals at Enron, WorldCom, and others. (The United States did not participate in the initial ISO working group and played no part in crafting the framework.)

An unintended consequence of the two frameworks' coexistence is that some multinational companies are using both – COSO in the United States and ISO in the rest of the world. On its face, that is out of line with a core principle of ERM: a consistent approach to and treatment of all risks.

ISO is fundamentally different from COSO. The latter defines risk as "the possibility that an event will occur and adversely affect the achievement of objectives." It focuses on the downside. ISO, on the other hand, views risk as "the effect of uncertainty on objectives," thereby allowing for positive outcomes. Think of the ISO approach as akin to managing the risk involved in buying a stock, where a spectrum of outcomes is in play.

Another important difference is that if internal audit initiates and implements an ERM program following the COSO framework, how can it then credibly audit the program? The ISO framework, however, says that *management* should embed ERM into the strategic planning process, which allows the internal audit and compliance control functions to do their job of evaluating whether the program is performing as intended.

A key strength of ISO 31000 is its focus on the identification of risk owners and the need for widespread education, both internally and externally, about organizational risks. This approach increases

accountability and strengthens communication. ISO also links to business objectives at all levels, making risk management more relevant and important.

While both the COSO and ISO frameworks are guides designed to bring organization and structure to the ERM process, many risk-management practitioners treat them as hard-and-fast rules. But adopting either one offers no form of assurance that risk-management failures will not occur.

ERM success depends on a collaboration of various groups, including board-level risk and audit committees performing their oversight responsibilities, executive management setting risk-management policy, middle management carrying out risk-management policy, and internal audit monitoring the risk-management process.

John Bugalla is a principal with ermINSIGHTS and Kristina Narvaez is president and CEO of ERM Strategies LLC. James Kallman, Ph.D., also contributed to this article.