COSO
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION
NEWS RELEASE

For Immediate Release

Contact:
Robert Perez
The Institute of Internal Auditors
robert.perez@theiia.org
(407) 937-1247

COSO in the Cyber Age

Research report offers guidance on using Frameworks to assess cyber risks

NEW YORK (Jan. 14, 2015) — Rapid innovations in technology are creating a complex and interconnected world with the number of Internet users soaring from a few million to nearly 3 billion in less than a generation. This cyber revolution boosts productivity and expands markets, while making customer transactions nearly effortless.

But it also is fueling a new class of digital crime in which hackers plunder and sell crucial data to the highest bidder. Businesses and governments are struggling against the onslaught of breaches by cyber criminals, many backed by nation-states, organized crime, terrorists and even so-called "hacktivists" with social or political agendas.

Most acknowledge that cyber attacks are virtually impossible to stop. They must, therefore, be managed.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) today released a new research report that provides direction on how the *Internal Control-Integrated Framework* (2013) and the *Enterprise Risk Management-Integrated Framework* (2004) can help organizations effectively and efficiently evaluate and manage cyber risks.

Using the 2013 *Internal Control-Integrated Framework* as an example, *COSO in the Cyber Age* provides direction on identifying and implementing internal control components and principles, from demonstrating commitment to integrity and ethical values, to risk analysis, and evaluating and communicating deficiencies.

"There is growing concern at all levels of industry about the challenges posed by cyber crime," said Robert B. Hirth Jr., COSO chairman. "This new guidance helps put organizations on the right path toward confronting and managing the frightening number of cyber attacks."

The report, authored by Mary E. Galligan, director, Cyber Risk Services, Deloitte & Touche LLP, and Kelly Rau, senior manager, Deloitte & Touche LLP, urges organizations to make cyber risk management a top priority. The report suggests some key questions an organization should ask:

- Are we focused on the right things?
- Are we proactive or reactive?

- Are we adapting to change?
- Do we have the right talent?
- Are we incentivizing openness and collaboration?
- Can executive management articulate its cyber risks and explain its approach and response to such risks?

"Cyber risk will only continue to be more difficult to manage as time passes, technology evolves, and hackers become more sophisticated," the report's authors conclude. ". . . The 2013 *Framework* can be used to guide a transformation that supports an organization's efforts to design, evaluate, and maintain an environment of being secure, vigilant, and resilient in a cyber-driven world."

To read the full report, go to www.COSO.org.

###

About COSO
Originally formed in 1985, COSO is a voluntary private sector organization dedicated to improving organizational performance and governance through effective internal control, enterprise risk management and fraud deterrence. COSO is jointly sponsored by the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).