For Immediate Release
Contact:
Suzanne Dawson
S&C Public Relations Inc.
sdawson@scprgroup.com
(646) 941-9140

John Babinchak
The Institute of Internal Auditors
john.babinchak@TheIIA.org
(407) 937-1240

Nicole Hockin
Deloitte & Touche LLP
nhockin@deloitte.com
(303) 305-3074

Managing Cyber Risk in a Digital Age

New COSO Guidance Addresses How Companies Can Use ERM Framework to Assess Cyber Risks

Lake Mary, FL (Dec. 17, 2019) – Even as companies become more digital savvy, they continue to confront new and emerging data risks that pressure financial and reputational vulnerabilities. To help address these challenges, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), in collaboration with Deloitte Risk & Financial Advisory, is releasing new guidance, "Managing Cyber Risk in a Digital Age."

Written to boards of directors, audit committee members, executive management, and cyber practitioners, the new guidance addresses how companies can apply COSO's *Enterprise Risk Management–Integrating with Strategy and Performance* (*ERM Framework*), one of the most widely recognized and applied risk management frameworks in the world, to protect against cyberattacks. The guidance provides insight into how organizations can leverage the five components and 20 principles of the *ERM Framework* to identify and manage cyber risks.

As business and technology evolve, so has COSO's *ERM Framework*, which was updated in 2017 to highlight the importance of applying ERM throughout an organization, particularly in strategic planning. One of the foundational drivers behind the 2017 update was to address the need for organizations to improve their approach in managing cyber risks. This new guidance is designed to provide context related to the fundamental concepts of cyber risk management, making it easier for organizations to leverage existing technical cybersecurity frameworks.

"As cyber threats increase in number, complexity, and destructiveness, organizations face a greater risk in achieving their strategic objectives," said Paul Sobel, COSO Chair. "COSO's *ERM Framework* provides a foundation upon which a cybersecurity program can be built, integrating cyber risk management concepts with elements of strategy, business objectives, and performance, which can result in increased business value."

The guidance notes that the fast-evolving cyber threat landscape makes it imperative for boards of directors to increase their cyber competencies so that they may effectively evaluate how well these risks are being addressed. "For nearly half of responding organizations (49%), cybersecurity is on the board's

agenda, at least quarterly, according to Deloitte's 2019 Future of Cyber Survey."[i] It is crucial that boards develop cyber security expertise themselves or identify advisers with relevant skills.

"C-suite leaders and board members need to stay committed to a more active and involved role in guiding their company's cybersecurity strategy, and regulators are starting to require it. The pervasiveness of cyber will continue, as will the complexity and severity of the adversaries' threats," said Mary Galligan, managing director in cyber risk services at Deloitte & Touche LLP. "Boards will need the right skill sets for proactively addressing technology, data and privacy issues to help those organizations thrive in the future. But thinking behind major initiatives like the *ERM Framework* can help organizational leaders continually evolve their understanding of cyber risks, so that they can make strategic decisions with cyber risk always in mind."

Sobel added, "A business-as-usual approach to cyber risk management is bound to result in catastrophic damage. Those charged with governance, from the board to the C-suite, must drive a strong tone at the top, communicate a sense of severity and urgency, and challenge the status quo of their ERM programs and cyber security awareness throughout every level of the organization. There is little to no room for error."

"*Managing Cyber Risk in a Digital Age*" was authored by Deloitte & Touche LLP's Mary E. Galligan, managing director, Sandy Herrygers, partner and global assurance leader, and Kelly Rau, managing director.

For the full report, visit 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). For more information, visit www.COSO.org.

About Deloitte
Deloitte provides industry-leading audit, consulting, tax and advisory services to many of the world's most admired brands, including nearly 90% of the Fortune 500® and more than 5,000 private and middle market companies. Our people work across the industry sectors that drive and shape today's marketplace — delivering measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to see challenges as opportunities to transform and thrive, and help lead the way toward a stronger economy and a healthy society. Deloitte is proud to be part of the largest global professional services network serving our clients in the markets that are most important to them. Our network of member firms spans more than 150 countries and territories. Learn how Deloitte's more than 312,000 people worldwide make an impact that matters at www.deloitte.com.

###

[i] Deloitte's 2019 Future of Cyber Survey, in conjunction with Wakefield Research, polled 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019.