

AUGUST 19, 2022

Are your risk-management practices keeping up with the times?

Risks abound in today's uncertain marketplace. Nearly two-thirds of senior finance leaders said that the volume and complexity of corporate risks have changed "mostly" or "extensively" in the past five years, according to a new report published by the American Institute of Certified Public Accountants (AICPA) and North Carolina State University.



Surprisingly, this report, *2022 State of Risk Oversight: An Overview of Enterprise Risk Management Practices*, found that only one-third of respondents

have complete enterprise risk management (ERM) processes in place. Unmitigated exposure to risk can disrupt your operations and even cause bankruptcy. That's why it's important for your organization to develop a comprehensive risk-management strategy — and for auditors to assess your ERM practices.

COSO framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in July 1985 to combat fraudulent financial reporting. The panel is a joint initiative of the AICPA, Financial Executives International, Institute of Internal Auditors, American Accounting Association and Institute of Management Accountants.

COSO first published its *Enterprise Risk Management — Integrated Framework* in 2004. Companies aren't generally required by law or regulations to apply an ERM framework. But they often choose to use COSO's ERM framework to enhance their ability to manage uncertainty, consider how much risk to accept and improve understanding of opportunities as they strive to increase and preserve stakeholder value.

Broad scope

Many people are unclear what the term "ERM" means. ERM encompasses more than taking an inventory of risks — it's an enterprise-wide process. Internal control is just one small part of ERM — it also may include, for example, strategy setting, governance, communicating with stakeholders and measuring performance.

These principles apply at all business levels, across all functions and to organizations of any size. They apply to not-for-profits, as well as for-profit entities.

Key components

Through periodic updates, COSO aims to capture today's best practices and help management attain better value from their ERM programs. The ERM framework addresses questions about how risk management should be incorporated with an organization's management of its strategy. It includes these five components:

1. Governance and culture,
2. Strategy and objective setting,

3. Performance,
4. Review and revisions, and
5. Information, communication and reporting.

In addition, COSO's *Guidance for Applying ERM to Environmental, Social and Governance (ESG)-related Risks* highlights ESG risks. This guide also identifies opportunities to enhance resiliency as organizations confront new and developing risks, such as extreme weather events or product safety recalls.

In 2019, COSO published another guide, *Managing Cyber Risk in a Digital Age*. It addresses how companies can apply COSO's framework to protect against cyberattacks. These attacks have been on the rise, in part, because people became increasingly reliant on the internet for working, learning and interacting during the pandemic. And home networks tend to be more vulnerable to cyberattacks than in-office networks.

Sign of the times

In 2022, market conditions — including the risks of cyberattacks, severe weather, rising inflation, supply chain disruptions and the shortage of qualified workers — continue to be volatile. And more uncertainty lies ahead. Our accounting professionals can help you identify and manage the risks. [Contact us](#) to discuss cost-effective ERM practices to make your organization more resilient and responsive in the future.