TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 133 | April 2026

What Boards Need to Know About ERM Oversight

In today's uncertain business environment, board members are finding themselves called upon to enhance their risk oversight. Stakeholders of all kinds increasingly expect boards to take a proactive role in overseeing an ever-changing risk landscape.

The risks facing organizations include geopolitical disruption, cybersecurity concerns, the impact of emerging technologies, supply chain issues, labor shortages, and severe weather, to name just a few. "Managing corporate risk is not just the business and operational responsibility of a company's management team — it is a governance and strategic issue that is squarely within the oversight responsibility of the board," according to the Harvard Law School Forum on Corporate Governance's "Risk Management and the Board of Directors."

The article adds that courts and regulators are focusing on board oversight and board responses when crises occur. While directors shouldn't be involved in day-to-day risk management, "every board's oversight role should include active engagement in monitoring key corporate risk factors, including through appropriate use of board committees," the article notes.

This issue examines board considerations in enterprise risk management (ERM) oversight and the role of internal audit in providing boards with valuable assurance and advice.

Determining ERM Maturity

A realistic assessment of the organization's ERM maturity level can provide boards with a greater understanding of where things stand and what changes may be needed. According to PwC's Director's Guide to ERM Fundamentals, at a high level, an organization's ERM maturity stages include:

- **Initial.** There are some informal practices but no formal policies or processes. The organization reacts to issues.
- **Developing.** There are systems and processes that are effective in some aspects of design or operation. The approaches are somewhat aligned to business operations.
- **Developed.** There are formal frameworks and systems embedded and operating to meet recognized standards.
- **Integrated.** The organization has integrated, collaborative, and enhanced systems and processes that enable a coordinated strategic and efficient response to current and emerging risks.
- **Optimized.** Systems, processes, and culture are well-integrated and aligned to strategic priorities. Technology is used to enhance governance, risk management, and monitoring/reporting.

"As the ERM program matures, the board can promote continuous improvement by challenging management on what is working and what is not," the guide states.

Digging Deeper

COSO's Executive Summary to *Enterprise Risk Management–Integrating With Strategy and Performance* suggests questions boards can ask management about ERM, including:

- Can all management — not just the chief risk officer — articulate how risk is considered in the selection of strategy or business decisions?
- Can management clearly articulate the entity's risk appetite and how it might influence a specific decision? COSO notes that the response may reveal insights into the organization's true mindset on risk taking.
- Can senior management discuss not only risk processes, but also how the organization's culture enables or inhibits risk taking?
- What lens does management use to monitor the risk culture, and how has that changed? Given inevitable change within and outside the organization, how can the board be confident of an appropriate and timely response from management?

COSO's Compendium of Examples includes specific observations on governance. One of the examples addresses how ERM can improve decision-making for better outcomes, enhance opportunities, and minimize negative surprises.

In the example, a company has moved to better understand existing and desired ERM capabilities. For instance, the CEO and internal auditor attend business performance reviews with the operating divisions to follow progress on performance goals and determine how an understanding of risks affects how they pursue those goals. Because of this effort, the CEO can better understand business performance, and the internal auditor has been better able to develop an audit plan.

Guidance on Best Practices

Organizations seeking to enhance their ERM approach can choose from several different ERM frameworks, including *COSO's Enterprise Risk Management–Integrated Framework,* the ISO 31000 Risk Management Standard, and the U.S. National Institute of Standards and Technology's Risk Management Framework. According to Optro's "Enterprise Risk Management Fundamentals," these frameworks typically share five key components:

- Company culture, governance, and values.
- Strategic planning, objectives, and goal setting.
- Risk management cycle.
- Monitoring and continuous improvement.
- Transparency, communication, and reporting.

The IIA's Three Lines Model is a best-practice model for board oversight of risk management, showing how key roles work together to support strong governance. The Enterprise and Business Process Risks Tool, aligned with the Model, helps organizations implement and manage a structured ERM program by providing a practical, customizable approach to identifying, assessing, managing, and monitoring risks at the enterprise and process levels.

Partnering With Internal Audit

Internal audit can be a valuable partner to boards in their efforts to enhance ERM. In fact, The IIA reports internal audit roles related to ERM are evolving, and a growing number of CAEs have responsibility for ERM. According to The IIA North American Pulse of Internal Audit study, the percentage of CAEs reporting they were responsible for ERM programs alongside their role as head of internal audit rose to 34% in 2025.

One key element supporting an effective risk management function is collaboration across the three lines. Under The IIA's Three Lines Model:

- **First line:** Management and operation leaders who manage risks.
- **Second line:** Risk management and compliance functions that monitor and oversee risks.
- **Third line:** Internal audit, which offers independent assurance and advice on achieving the organization's goals.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit theiia.org/Tone to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to **Tone@theiia.org.**

Expectations for Boards

Core risk-related responsibilities for the board include:

- Setting the organization's risk appetite and tolerance.
- Approving and monitoring the ERM framework.
- Aligning strategy and risk exposure.
- Overseeing risk culture and internal controls.
- Monitoring emerging risks and critical areas.
- Ensuring clear roles and responsibilities.

– Diligent, "Understanding Board Oversight of Risk Management Now and for the Future"

The Model "makes clear that, while internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the execution of its work, independence does not imply complete isolation," according to Collaboration Without Compromise: Practitioner Perspectives on Internal Audit, Risk Management, and Governance Practices, a report from Baker Tilly, the Internal Audit Foundation, and Wolters Kluwer TeamMate. Internal audit's expanding responsibilities in a number of areas, including ERM, provide opportunities to elevate this function's role as an independent evaluator of governance and risk management effectiveness.

The report notes that 90% of respondents see benefits in coordination between the second and third lines, including:

- Improved risk coverage.
- Reduced duplication of effort.
- Strengthened organizational alignment.
- Enhanced communication to the board and more efficient reporting.

Thirty-nine percent of report respondents say they have seen greater integration of the internal audit and risk functions over the past five years, and 60% say this number will rise over the next five years. "When thoughtfully designed through information sharing, coordinated activities, and aligned priorities, such approaches help ensure boards receive reliable information for informed decision-making," the report says.

A Clear View

As much as anything, ERM is about recognizing or anticipating change and deciding what it means for the organization. COSO notes that a clear view of change enables organizations to make sound decisions on tough questions, such as whether it's best to make new investments or pull back. As COSO states, "Enterprise risk management provides the right framework for boards to assess risk and embrace a mindset of resilience."

Technology and ERM

There is great potential for artificial intelligence (AI) to play a larger role in ERM. Fewer than one in 10 respondents report using AI frequently to assist in identifying risks (6%) or say that they are using it heavily for data input into risk management activities (3%), according to Enhanced Enterprise Risk Management and Strategic Decision-Making, from Baker Tilly and the Internal Audit Foundation.

Integrated governance, risk, and compliance (GRC) platforms can support ERM processes. An ERM Maturity Survey from Baker Tilly and the Internal Audit Foundation reveals only 21% of responding professionals use them. Many organizations' ERM programs are based on simple tools, such as word processing and spreadsheets (59%) or in-house technology tools (20%).

"In an age when digital transformation has accelerated reliance on technology across all aspects of operations and redefined strategies, it is dangerous to not have ERM keep pace," the Enhanced Enterprise Risk Management report cautions.

With that in mind:

- Software as a service and GRC tools can enhance basic ERM programs and can promote a deeper enterprisewide grasp of risks. They can centralize data, automate workflows, and make it easier to identify risks, which can enable better decision-making and minimize risk exposure.

- The report advises organizations to support, facilitate, and monitor exploration of safe AI use within the organization and identify ways to put AI to work in ERM processes.

"Graduating from traditional ERM approaches with the help of collaborative tools, external risk scanning, cross-functional integration, and cutting-edge technologies should be the goal of all ERM programs," the report states.

Among global experts surveyed, 50% expect either a turbulent or stormy global risk outlook over the next two years, growing to 57% over the next 10 years." Only 1% predict a calm outlook.

– World Economic Forum Global Risks Report 2026.