



# Exploring third-party risk management for internal audit leaders

## KPMG Ask the Experts insights






With organizations increasingly dependent on external parties, robust third-party risk management (TPRM) programs are essential. As risk management and compliance evolves to increase coverage of third-parties, internal auditors are experiencing a significant shift to focus on TPRM. This shift requires auditors to be well-resourced and equipped to provide valuable recommendations, while balancing risk mitigation with efficiency, using a coordinated three lines of defense model for comprehensive oversight.

In the recent webcast, *Ask the Experts: Exploring third-party risk management in the age of automation and GenAI*, industry leaders shared valuable insights on the transformative role of TPRM and internal audit's (IA) opportunity to shine. The discussion emphasized adopting a risk-based approach, leveraging technology for due diligence, and fostering collaboration between IA and stakeholders.

### Key insights on TPRM programs

- ✓ TPRM is gaining importance and regulatory scrutiny across industries.
- ✓ TPRM programs are evolving from manual processes to more automated, technology-enabled solutions.
- ✓ TPRM ownership is often distributed, requiring a hub-and-spoke model with central governance and oversight.
- ✓ AI is transforming TPRM through efficient due diligence, smart questionnaires, and data integration.
- ✓ Proper TPRM resourcing isn't limited to staffing, and includes technology, data and the right third-party resources.

### Five things IA professionals need to do now

-  Adopt a risk-based approach to TPRM and tier third parties based on risk profile.
-  Align TPRM with the organization's ERM framework and integrate it with other risk management programs, such as information security, compliance, and privacy.
-  Work with legal to mitigate identified third-party risks through proper contract language (e.g. audit provisions), and leverage technology enablement for risk-based due diligence reviews. In addition, exercise audit rights in a risk-based fashion.
-  Trust instincts, challenge risks, and provide recommendations that identify efficiencies and support the bottom line.
-  Be a trusted adviser, help the business move at its speed while mitigating risks, and secure leadership buy-in for TPRM audit program.

### What's on the mind of IA professionals

**48%** of respondents stated that the percentage of their audit plan focused on TPRM was less than 10 percent. An additional 38 percent responded it was between 11 percent and 25 percent of the plan.

**80%** of respondents said their TPRM audit program was basic or nonexistent, indicating a significant need for improvement.

**41%** of professionals reported that their focus area in their TPRM audit program is cyber and information security. The second highest focus was regulatory compensation at 19 percent.

**71%** of professionals don't feel that they are properly resourced, with the minimum staff and proper tools/data to support their TPRM audit program.

Statistics are based on polling data from our September 2024 **Ask the Experts** webcast. [To see the full audience polling results, download our infographic here.](#) For more insights on Ask the Experts webcasts, visit us at [the Future of Internal Audit](#).

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:  [kpmg.com](https://www.kpmg.com)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.