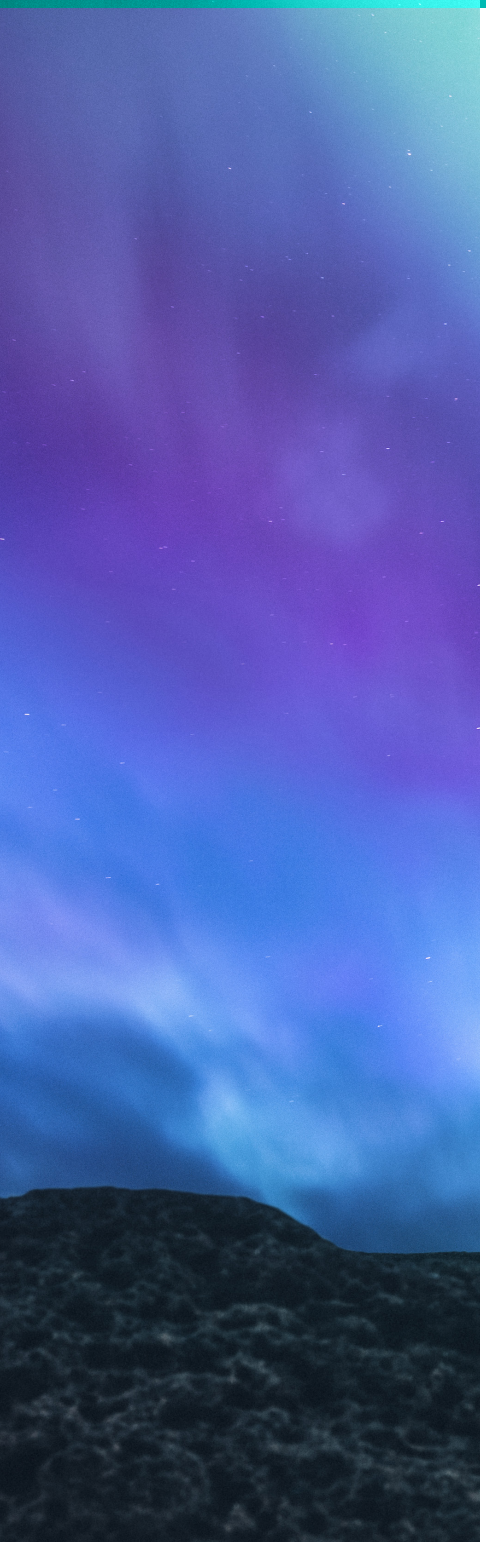
bakertilly | Internal Audit FOUNDATION

WHITEPAPER

Enhanced enterprise risk management

AND STRATEGIC DECISION-MAKING

Manage disruption, empower decisions, optimize performance



CONTENTS

Executive summary

The growth of enterprise risk management (ERM) has been impressive. The percentage of organizations claiming to have complete ERM processes in place jumped from 9% in 2010 to 34% in 2023.[1] Driven by growing risk complexity and interconnectivity, and increased regulation, the global risk management market is expected to grow from a $9 billion industry in 2025 to more than $32 billion in 2033.[2] Yet, even as more organizations embrace ERM's promise of enhanced risk management and strategic decision-making, relatively few reap its full benefits.

A survey[3] of professionals by Baker Tilly and the Internal Audit Foundation found 6 in 10 ERM programs connect with their organization's strategic planning, but many fail to connect information and insights provided by ERM with their strategic decision-making processes. Among the survey's other key findings:

- Organizations have opportunities to increase enterprise-wide risk awareness. Fewer than half (49%) of respondents agree or strongly agree that risk awareness resonates across the organization.
- ERM programs have room to better leverage emerging technologies. Nearly 6 in 10 survey respondents (59%) say their programs still rely on basic tools, such as word processing and spreadsheets. Governance, risk, and compliance (GRC) platforms are used by only 21% of respondents and in-house technology is used by 20%.
- There is great potential for artificial intelligence (AI) to play a larger role in risk management. Fewer than 1 in 10 respondents report AI is used frequently to assist in identifying risks (6%) or heavily used for data input into risk management activities (2%).

The report, ***Enhanced ERM and strategic decision-making***, offers strategies to address the most common shortcomings identified in the survey, helping organizations strengthen the connection between ERM and strategic decision-making. The discussion covers strategic recommendations in three key areas: **timely risk assessments**, **coordinated efforts and communication with internal audit**, and **leveraging technology**. Additionally, the report provides valuable benchmarking data on the current state of ERM, highlighting areas where programs fall short and why.

1. "2023 The State of Risk Oversight: An Overview of Enterprise Risk Management Practices – 14th Edition," AICPA and North Carolina State University's ERM Initiative, July 2023, https://erm.ncsu.edu/resource-center/2023-risk-oversight-report-erm-ncstate-lp/.
2. "Risk Management Market," Market Data Forecast, February 2025, https://www.marketdataforecast.com/market-reports/risk-management-market.
3. Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. *n* = 567.

Introduction

One goal of risk management is to identify, assess and manage risk that can hinder achievement of strategic objectives or lead to financial losses, operational disruptions or reputational damage. ERM elevates such efforts by putting in place processes and frameworks that allow for effective risk management across an entire organization, rather than just within specific departments, functions or activities. When operating at higher levels, ERM also offers information and insights that allow decision-makers to leverage opportunities offered by risk, such as gaining footholds in emerging markets ahead of competitors.

Proponents of ERM say it can lead to proactive risk identification, improved decision-making, enhanced regulatory compliance and financial performance, stronger corporate governance, improved operational resilience, better stakeholder relations, and a competitive advantage. It is no wonder that ERM adoption has grown significantly in the 21st century.

Ideally, effective ERM should equip boards and executive management with risk insights that support informed decision-making around strategic objectives. Indeed, as ERM programs mature, the information they generate should enhance short-, mid-, and long-term strategies that lead to sustained growth and success. But a recent survey of nearly 600 risk professionals by Baker Tilly and the Internal Audit Foundation finds organizations struggle to make that valuable connection.

To be sure, organizations face myriad challenges to implement and effectively mature ERM programs. Identifying and assessing risks, as well as developing controls to manage them, is as much an art as a science and varies between organizations and industries. Additionally, a variety of factors can influence ERM, including organizational culture, competition, industry regulations, technological advances and related disruptions. The authors of a June 2024 article in the Journal of Risk and Financial Management list seven common problems with ERM implementation, including, an over emphasis on reporting, insufficient influence into the decision-making process, too much adherence to static process, and the lack of role clarity.[4]

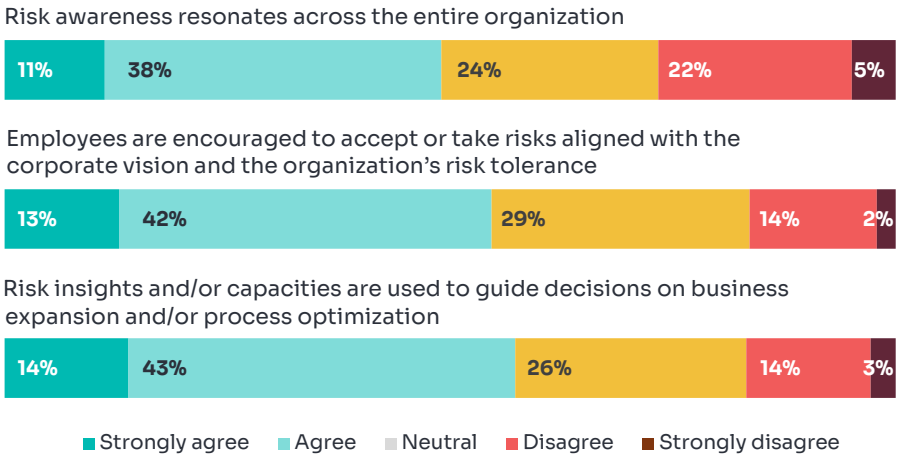
4. J. Fraser, R. Quail, B. Simkins, "What's Wrong with Enterprise Risk Management?" *Journal of Risk and Financial Management*, June 2024.

Connecting ERM and strategic goals

Leaders are more likely to develop and execute strategies that enhance operational performance and sustainable success when they understand how risks and risk management impact all aspects of the organization, know the efficacy of risk mitigation efforts and have insights into emerging risks. This is where ERM's value resides. ERM programs that do not connect with strategy ultimately fail to live up to their potential.

Companies vary widely in their maturity and connection between ERM and strategy. Some organizations struggle to establish a formalized risk strategy, and even those with formal processes sometimes experience disconnects between ERM activities and strategic goals. More fundamentally, organizations still struggle with achieving enterprise-wide risk awareness.

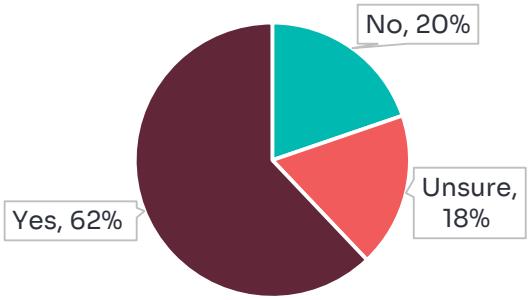
The current survey data show that fewer than half (49%) of respondents agree or strongly agree that risk awareness resonates throughout their organization. Additionally, just 57% agree or strongly agree with the statement, "Employees are encouraged to accept or take risks aligned with the corporate vision and the organization's risk tolerance." The same percentage (57%) agree or strongly agree that, "Risk insights and/or capacities are used to guide decisions on business and expansion and/or process optimization." A further breakdown of responses to this question reveals that public sector participants were even less likely to agree or strongly agree with the statements.



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q3. What is your level of agreement about the relationship between your organization's vision and its risk management? *n* = 567.

ERM programs should facilitate leveraging risk information for strategic planning and decision-making. However, the survey data reflects there is work to be done here, as well. Little more than 6 in 10 (62%) respondents agreed or strongly agreed that risk information is used for strategic planning at their organizations. Again, public sector respondents lagged in this area, with 46% agreeing or strongly agreeing.

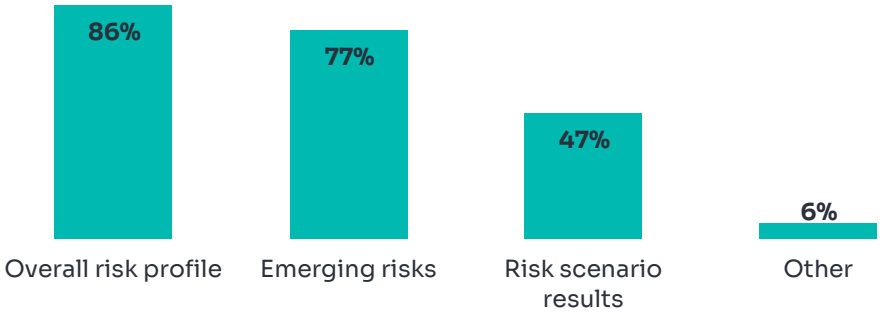
Risk information used for strategic planning



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q4. Is risk information used for strategic planning at your organization? *n* = 567.

The survey did reveal some positive findings. Among the 62% of respondents who indicated that their organizations use risk information for strategic planning, 86% reported using overall risk profiles, and 77% use information on emerging risks. However, fewer than half (47%) leverage risk scenario data.

Types of risk information used



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q5. What types of risk information are used for strategic planning at your organization? (Choose all that apply.) n = 352.

Leveraging ERM resources

There are abundant resources available to support ERM development. Frameworks developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the International Organization for Standardization (ISO) provide guidance for implementing, monitoring, and maturing ERM programs. The Risk & Insurance Management Society (RIMS) has developed a risk maturity model (RMM) for assessing and improving ERM operations. What's more, the rapidly evolving information technology (IT) industry has made Software as a Service (SaaS)-based ERM systems readily available from a variety of vendors.

FRAMEWORKS

COSO's ERM framework —*Enterprise Risk Management—Integrating with Strategy and Performance*— identifies five interrelated components at the heart of ERM:

- Governance and culture
- Strategy and objective-setting
- Performance
- Review and revision
- Information, communication and reporting

Each component is supported by a series of related principals.

Source: COSO Enterprise Risk Management—Integrating with Strategy and Performance

For example, the four principles supporting strategy and objective-setting are: analyzing the business context, defining risk appetite, evaluating alternative strategies and formulating business objectives.

Like the COSO ERM framework, ISO 31000 provides guidance on risk management that stresses an enterprise-wide approach. However, it emphasizes adaptability and flexibility, allowing organizations to tailor risk management practices to their needs. In contrast, COSO ERM offers a more structured framework for enterprise-level risk management, providing a comprehensive approach to identifying, assessing and responding to risks.

Whether putting in place processes and practices that support the five ERM components identified in the COSO framework or adopting ISO's more tailored risk management approach, both require a high level of coordination, collaboration and communication among risk managers, executive management and the board. Getting these basic components in place creates the foundation for a traditional ERM program. However, the greatest benefits come when ERM programs evolve and mature to an enhanced state where risk assessments, decision-making and development of short- and long-term strategies leverage the full gamut of information and insights ERM can provide.

External assessments of ERM programs, such as the risk maturity model available through RIMS, can provide valuable perspective and enhance ERM effectiveness. Outside consultants may also provide objective reviews and advice. However, few organizations leverage this resource. Just less than a third (32%) report using external resources. Even among those who do, the vast majority (83%) use them for specific, project-based needs.

Benchmarking

This section of the report provides a comprehensive overview of current practices within ERM programs based on the Baker Tilly and Internal Audit Foundation survey results. It focuses on key areas such as the frequency of risk assessments, risk response and reporting mechanisms, the use of external resources such as consultants, and the adoption of technology.

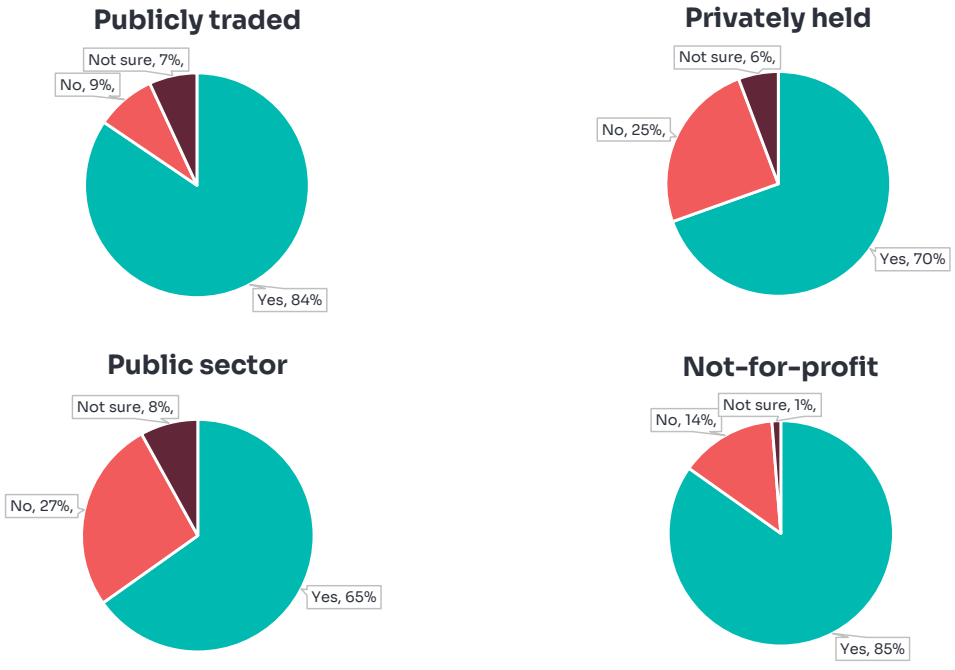
This benchmarking data provides valuable insights into the evolving landscape of ERM. It also serves as the foundation for **Strategies for improving ERM** (below), which highlights areas of improvement and strategies for organizations to enhance their risk management frameworks.

THE DATA

Risk assessments

When viewed in aggregate, 3 out of 4 respondents reported that their organization had conducted an enterprise-wide risk assessment within the past three years. However, when the data was cross-tabulated by organization type, respondents from privately held organizations and the public sector were more likely to indicate that no risk assessment had taken place within this time frame.

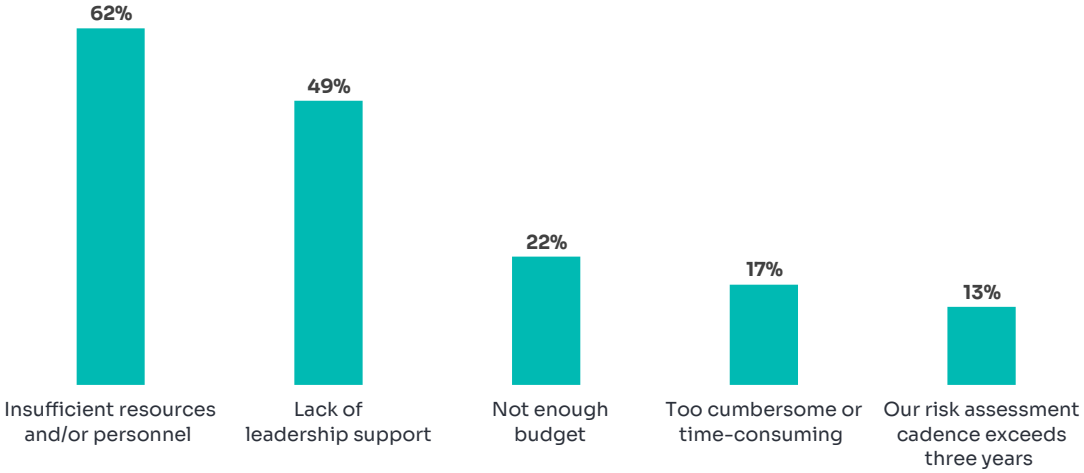
Has an enterprise-wide risk assessment been conducted in the past three years?



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q13. Has your organization conducted an enterprise-wide risk assessment in the past three years? Publicly traded, *n* = 174; Privately held, *n* = 174; Public sector, *n* = 112; Nonprofit or not-for-profit, *n* = 79.

Among those whose organizations had not conducted a risk assessment in the past three years, the majority cited insufficient resources and/or personnel (62%) and a lack of leadership support (49%) as the primary reasons.

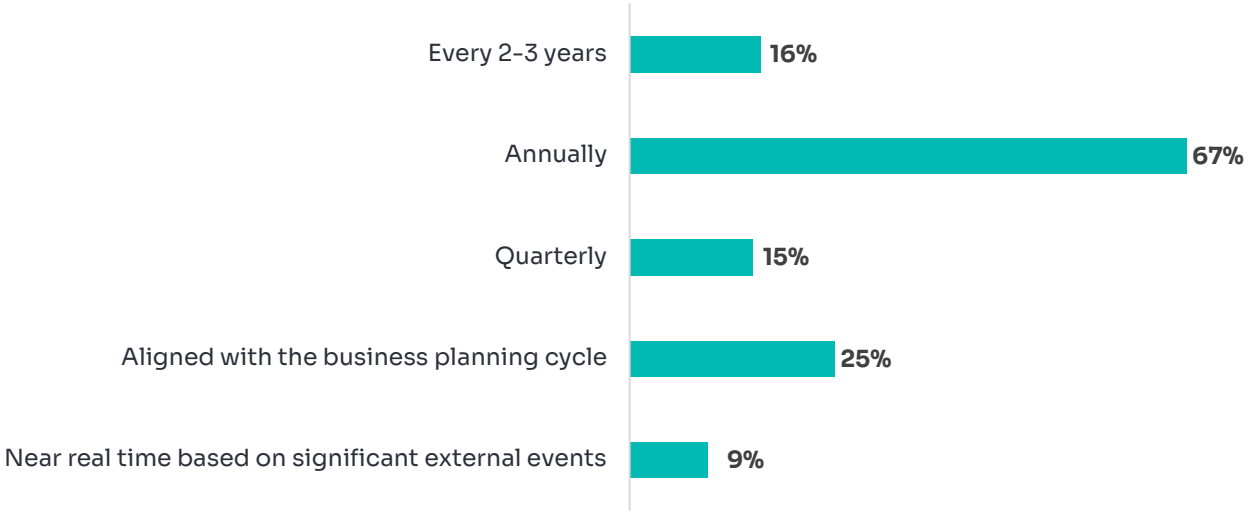
Reasons for not conducting a risk assessment in three years



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q14. Why has your organization not conducted a risk assessment in the past three years? (Choose all that apply.) *n* = 104.

Of those whose organizations conducted a risk assessment in the past three years, the majority (67%) stated that enterprise-wide risk assessments are conducted annually, while a quarter mentioned that risk assessments are aligned with the business planning cycle (e.g., strategic or long-range planning).

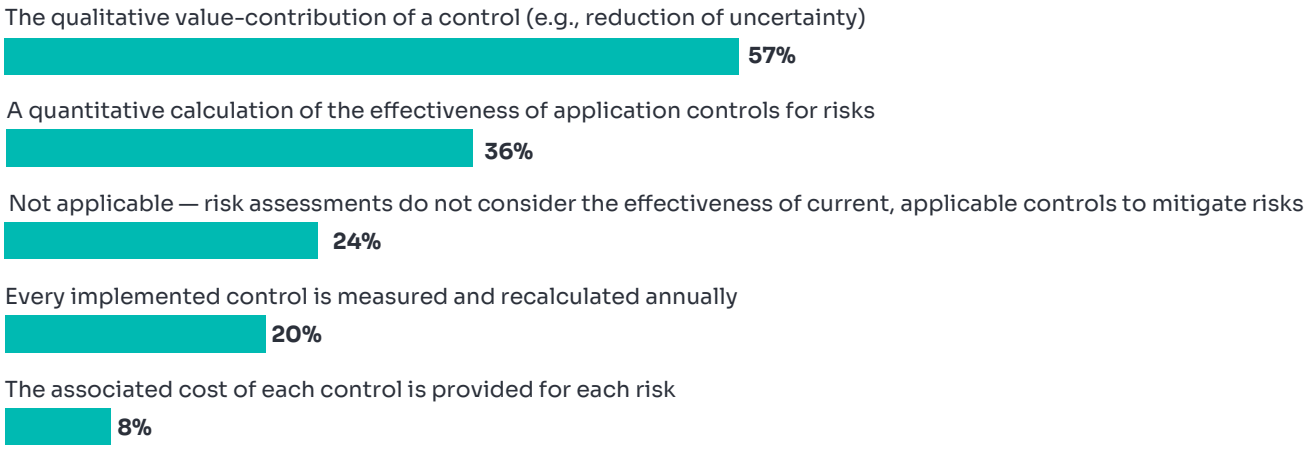
Frequency of enterprise-wide risk assessment



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q15. Which of the following describes the frequency of your organization's enterprise-wide risk assessment? (Choose all that apply.) *n* = 426.

Measuring mitigation and control effectiveness

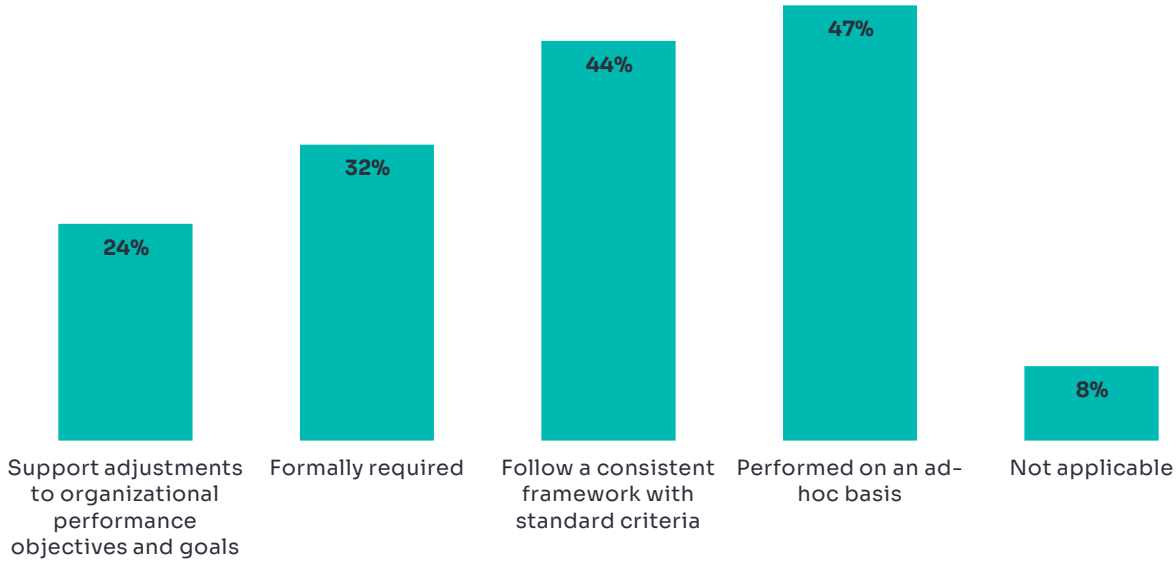
More than half (57%) of respondents reported that risk assessments evaluate the effectiveness of risk mitigations and controls based on the qualitative value contribution of a control. Another 36% indicated that risk assessments rely on a quantitative calculation of the effectiveness of application controls for managing risks. However, approximately a quarter (24%) believed that risk assessments do not consider the effectiveness of current, applicable controls in mitigating risks.



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q18. In what ways do risk assessments measure the effectiveness of risk mitigations and controls at your organization? (Choose all that apply.) *n* = 567.

Assessing major programs and initiatives

The data show a promising understanding of risk principles for key initiatives. Nearly half (47%) of respondents indicated that risk assessments are conducted on an ad-hoc basis for major programs and initiatives, while 44% stated that these programs follow consistent frameworks and standardized criteria. A third (32%) also said risk assessments are formally required for such programs. Of note, the level of ad-hoc reviews was consistent across publicly traded, private and public sector respondents, which reflects an encouraging rigor of risk discipline on major programs and initiatives.



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q16. Specifically for major programs and initiatives at your organization, how are risk assessments conducted? (Choose all that apply.) *n* = 567.

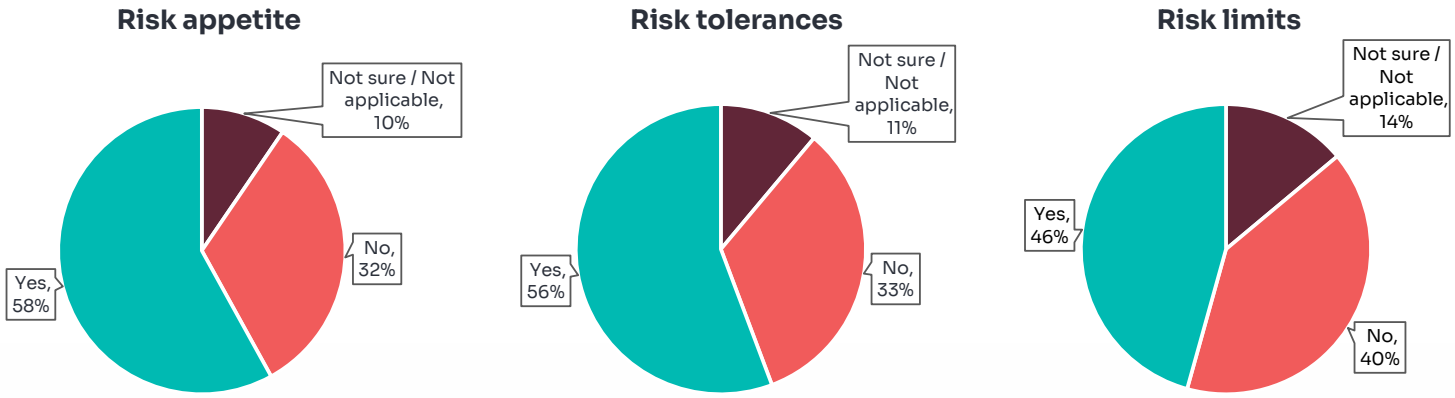
Measures of risk boundaries

Measures of risk boundaries refer to metrics or methods used to define an organization's approach to managing risk within acceptable limits. In the survey, participants were asked to report how the following COSO measures are utilized in their risk management programs:

- **Risk appetite:** The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
- **Risk tolerances**: The acceptable level of variation an organization is willing to accept regarding a specific risk.
- **Risk limits:** The specific thresholds set to monitor and ensure that actual risk exposure stays within the defined risk tolerance level.

At first glance, responses to this question paint a favorable picture of organizations applying more advanced ERM practices within their programs. Nearly 6 in 10 say they apply risk appetite (58%) and risk tolerance (56%) in managing risk. Nearly half (46%) of respondents apply risk limits concepts.

Are these measures used in your risk management program?

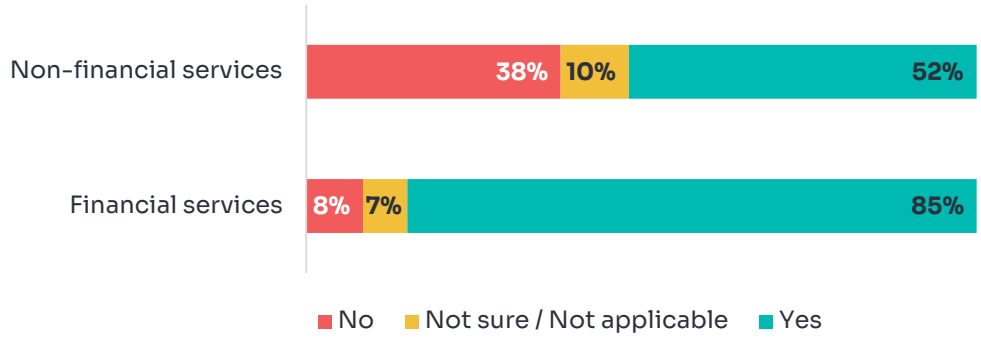


Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q17. Do you utilize the following measures in your risk management program (as defined by COSO)? *n* = 567.

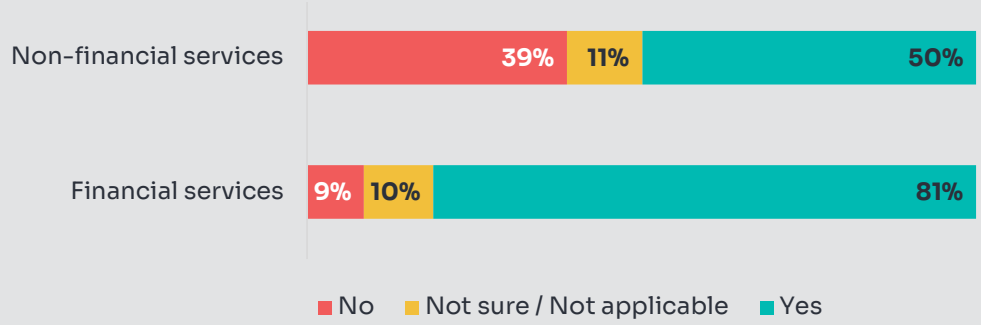
However, a closer analysis of the data reveals that these percentages are skewed positively due to the number of financial services respondents, who accounted for nearly 19% of all participants. When financial services respondents are extracted from the data, the number of favorable responses declines to more modest adoptions, with risk assessments dropping from 58% to 52%, risk tolerance decreasing from 56% to 50%, and risk limits dipping from 46% to 40%.

This is likely due to strict oversight on the establishment of Risk Appetite Frameworks (RAFs) imposed on financial services by regulators such as the Financial Stability Board, Office of the Comptroller of the Currency and others.

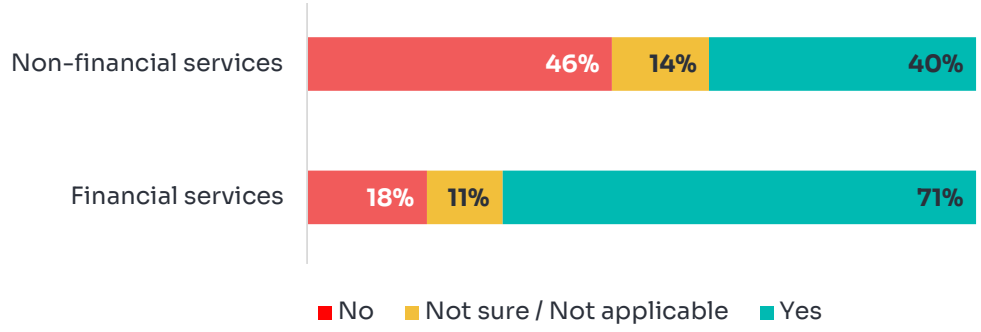
Measures used across financial vs. non-financial services: Risk appetite



Measures used across financial vs. non-financial services: Risk tolerances



Measures used across financial vs. non-financial services: Risk limits

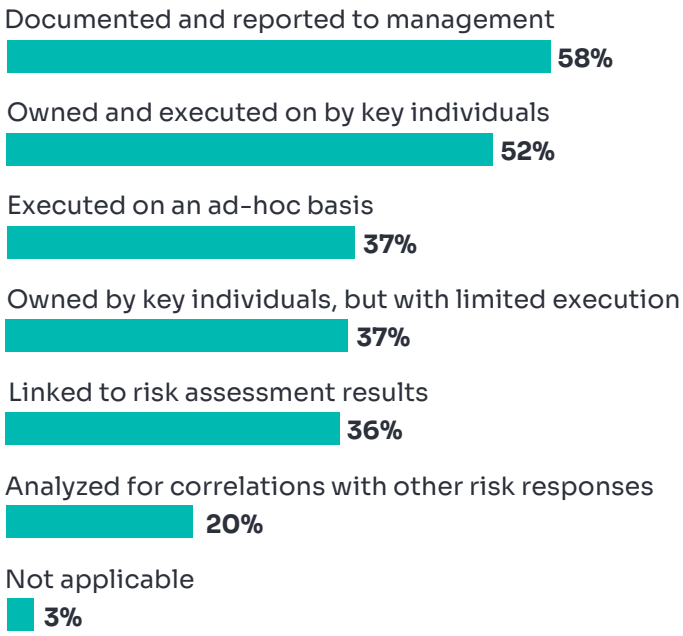


Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q17. Do you utilize the following measures in your risk management program (as defined by COSO)? Financial services, *n* = 106; Non-financial services, *n* = 461.

Risk response and reporting

Some organizations are beginning to adopt more structured approaches, with 58% reporting that risk response actions are documented and communicated to management. This indicates a formal process for managing risk, where mitigation actions are both recorded and shared with key stakeholders for oversight and decision-making.

While more than half (52%) of key individuals (e.g., risk owners or champions) are responsible for overseeing risk response actions, less than 4 in 10 (37%) own and execute these actions.

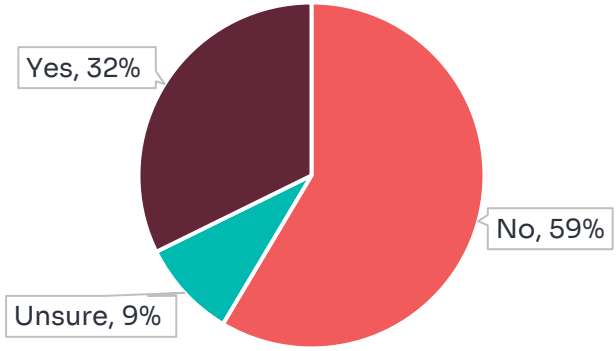


Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q19. In what ways are risk response actions handled at your organization? (Choose all that apply.) *n* = 567.

External resources

Most organizations, regardless of type, size or ERM function size, do not use external consultants within their risk function. An evaluation of how this could affect overall ERM effectiveness is explored in the section on **Strategies for improving ERM** (below).

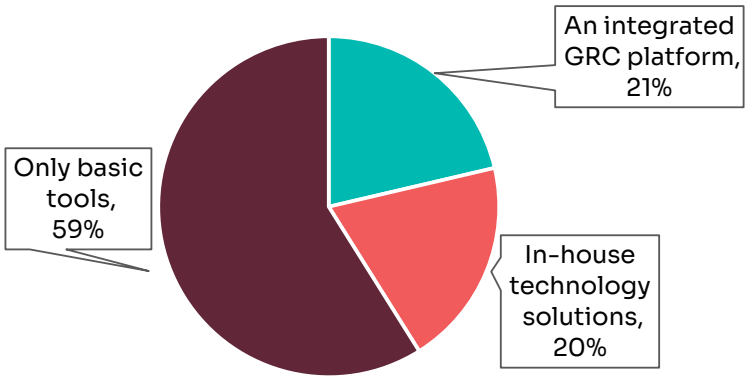
Are external resources used in your risk function?



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q11. Does your organization's risk function use external resources? *n* = 567.

Technology use

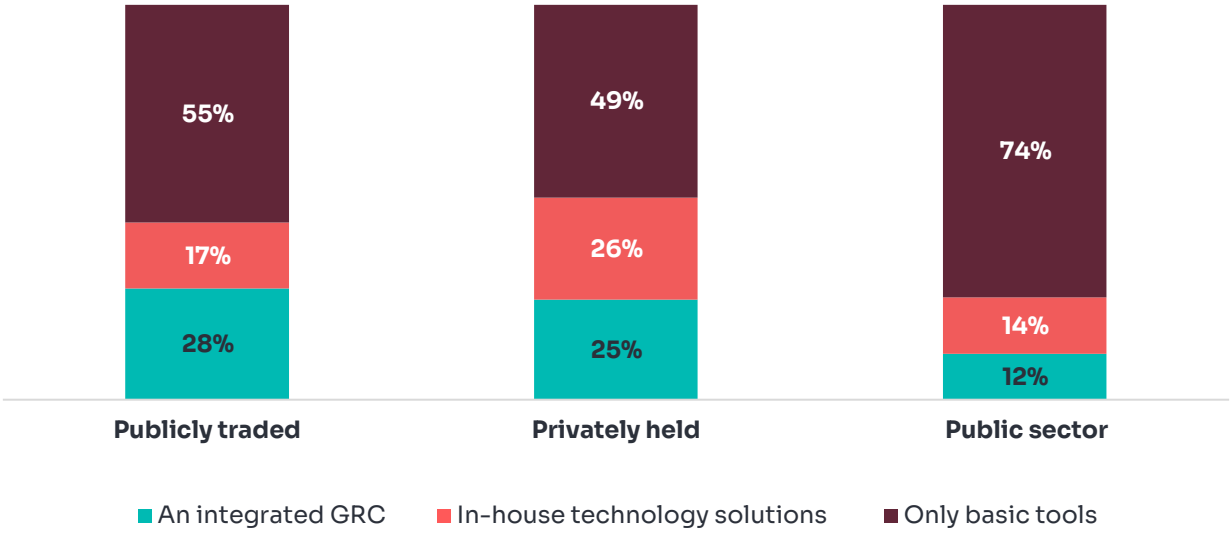
Technology, such as integrated GRC platforms, is playing an increasingly vital role in supporting ERM processes, with a growing number of organizations affirming the use of advanced tools for data analysis, reporting and decision-making. However, most have not incorporated AI, robotic process automation (RPA), machine learning (ML) or other advanced technologies to a great extent.



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q23. Which statement best describes your risk function's use of technology? *n* = 567.

About 6 in 10 respondents (59%) say they still rely on basic tools (e.g., word processing, spreadsheets), with only 2 in 10 reporting using integrated GRC platforms (21%) or in-house technology solutions (20%). Public sector respondents lagged in technology use with nearly 3 in 4 (74%) relying on basic tools, 12% leveraging GRC platforms, and 14% using in-house technology.

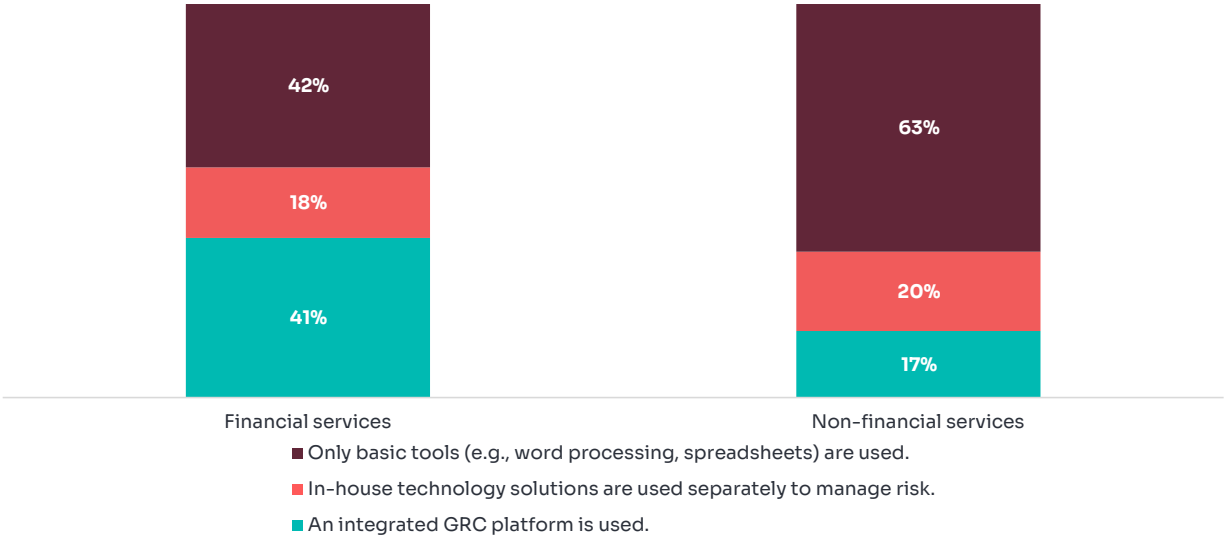
Risk function's use of technology by organization type



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q23. Which statement best describes your risk function's use of technology? Publicly traded, n = 174; Privately held, n = 174; Public sector, n = 112.

When comparing financial services respondents to those in non-financial sectors, a clear divide emerges. A larger proportion of financial services respondents (41%) report using an integrated GRC platform, whereas 63% of non-financial services respondents indicate they use only basic tools.

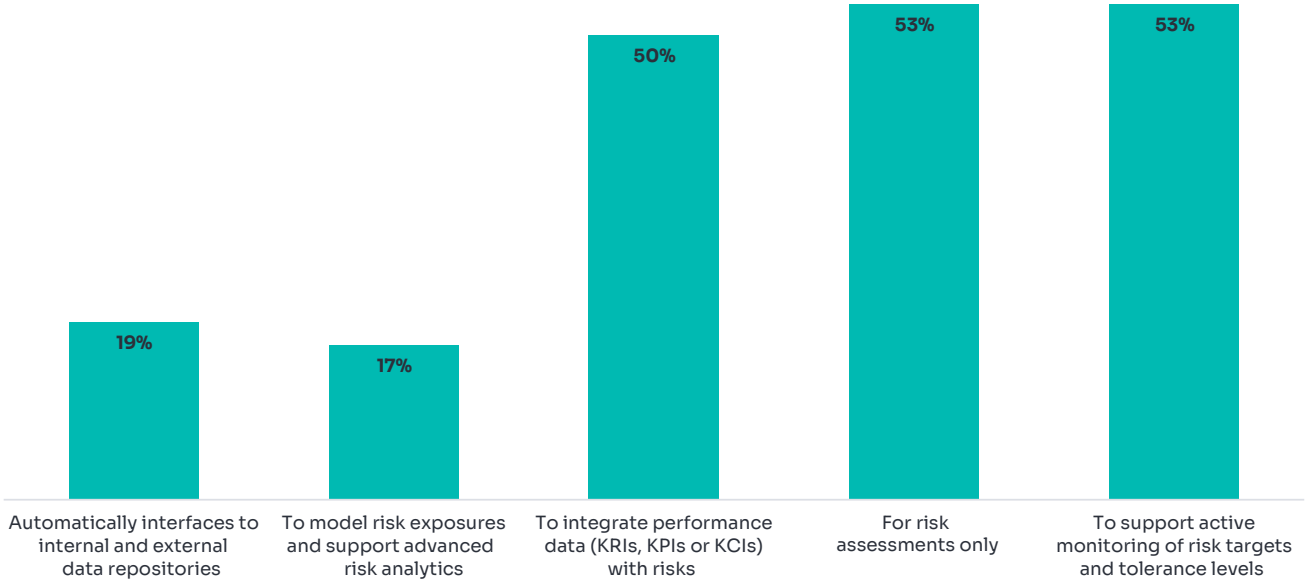
Risk function's use of technology by sector



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q23. Which statement best describes your risk function's use of technology? Financial services, *n* = 106; Non-financial services, *n* = 461.

For those who report using GRC technology platforms, most use it strictly for risk assessments or for monitoring risk targets and tolerance levels (53%), while half leverage platforms to integrate performance data (e.g., KRIs, KPIs or KCIs). Fewer than 2 in 10 leverage GRC tools to automatically interface with internal or external data repositories (19%) or to model risk exposures and support advanced risk analytics (17%).

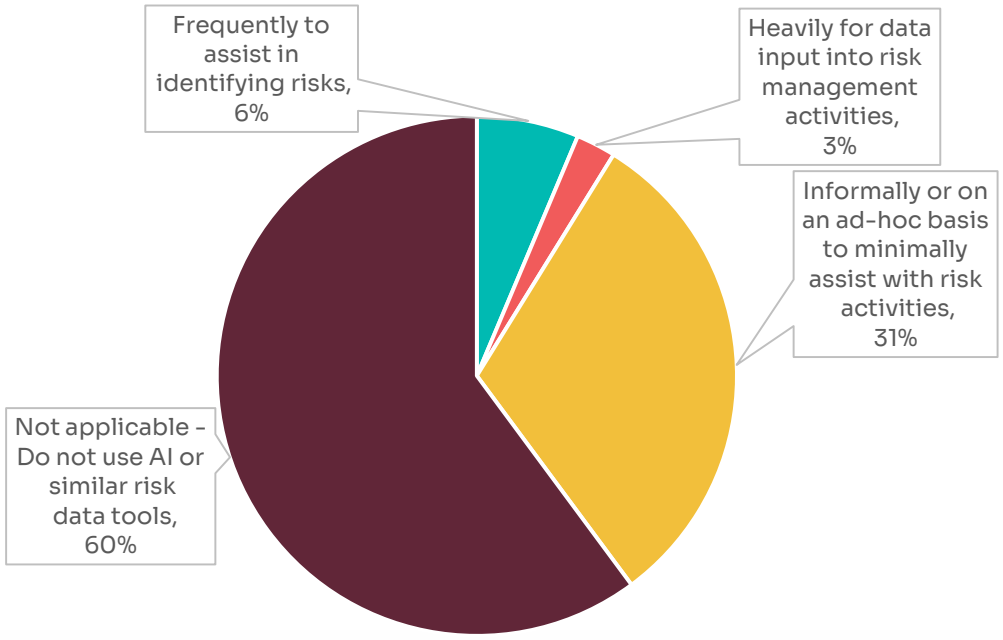
GRC technology platform integration



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q24. In what ways is the integrated GRC technology platform used at your organization? (Choose all that apply.) *n* = 121.

While AI has taken the business world by storm since the introduction of ChatGPT and other large-language models in 2022, it has yet to be significantly incorporated within ERM. Six in 10 (60%) respondents report no use of AI or similar risk data tools, and about 3 in 10 (31%) report informal or ad-hoc use to minimally assist with risk activities. Fewer than 1 in 10 (6%) report AI is used frequently to assist in identifying risks, and a scant 2% report AI is used heavily for data input into risk management activities.

Risk function's use of artificial intelligence



Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q25. How would you describe your risk function's use of artificial intelligence (AI)? *n* = 567.

Internal audit independence

Risk management assurance and advice provided by internal audit is vital to effective ERM, but questions about potential conflicts or threats to independence can sometimes limit internal audit's participation and influence.

Internal audit independence is addressed in The Institute of Internal Auditors (The IIA) Global Internal Audit Standards™, as well as The IIA's Three Lines Model.[5] The model, which is built around six principles that focus on the roles and responsibilities of the governing body (board), executive management (first and second line), and internal audit (third line), addresses the independence question directly.

ERM value is enhanced when all risk players, including internal audit, play active roles. Collaboration and information sharing foster improved communication, transparency, and accountability. Additionally, this approach helps reduce service duplication and audit fatigue, while also discouraging the formation of risk silos.

> **Internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the carrying out of its work, enjoying unfettered access to the people, resources, and information it requires. It is accountable to the governing body. However, independence does not imply isolation. There must be regular interaction between the internal audit function and management to ensure internal audit work is relevant and aligned with the strategic and operational needs of the organization.[5]**

Survey respondents were given the option to respond to the following open-ended question: **If the responsibility of managing risk management processes is shared across functions within your organization, briefly describe the specific measures in place to preserve the independence of the internal audit function.**

A thematic analysis of the responses identified two primary efforts aimed at preserving the independence of the internal audit function: clearly defined reporting structures and independently delineated functions. This brief overview highlights examples of actions organizations are taking, as reported by respondents, to ensure the independence of internal auditors.

- **Clearly defined reporting structures** refer to who reports to whom and how authority flows within the organization.
- **Independently delineated functions** refer to the distinct roles and responsibilities within an organization that are clearly defined, often focusing on what each department or individual is responsible for.

5."The IIA's Three Lines Model: An Update of the Three Lines of Defense," The Institute of Internal Auditors, Lake Mary, FL, 2025. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

THEME I: REPORTING STRUCTURE

The majority of respondents described various ways in which reporting structures are leveraged to preserve internal auditors' independence; these include the establishment and use of committees or working groups, separating lines of reporting by executives or board members, separating lines of reporting by other means, and the use of a third-party service provider.

Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q10. (Optional.) If the responsibility for managing risk management processes is shared across functions within your organization, please briefly describe the specific measures in place to preserve the independence of the internal audit function (n = 98). Codes are non-exclusive. Percentages are calculated against the total number of code applications (n = 115), so they reflect the distribution of all coding references rather than the proportion of unique comments).

Selected supporting quotes for **reporting structure**:

Committee/working group

- "I report directly to the audit committee."
- "The CAE is [an] ex-officio, non-voting member of the ERM governance committee."
- "Internal audit has a direct reporting line to the audit and risk committee."

Separation (C-level/board)

- "At board committee level, there are different committees to oversee the work of ERM (governance & management resources) and internal audit (audit)."
- "ERM is under the responsibility of [the] chief audit officer. Audit builds its plan with inputs from ERM."

Separation (outside C-level/board)

- "There are clear roles and responsibilities for each function (internal audit and risk manager) established in policies and procedures; internal audit only collaborates [on] risk assessment, but avoids the design or implementation of controls..."
- "Risk management and compliance is separate from [the] internal audit function."

Use of third-party provider

- "We use [an] internal audit service provider that is not involved in ERM, which helps keep some level of independence from ERM."

THEME II: INDEPENDENTLY DELINEATED FUNCTIONS

Many respondents recounted actions their organization is taking to ensure independence, often employed outside of the use of formalized reporting structures. Specifically, clearly delineating the ownership of risks, positioning internal audit as a non-decisional advisory/consulting role, engaging in separate risk assessments, or engaging in other processes to separate work, responsibilities and duties.

Note: Baker Tilly & Internal Audit Foundation ERM Maturity Survey, Jan. 07 to Feb. 07, 2025. Q10. (Optional.) If the responsibility for managing risk management processes is shared across functions within your organization, please briefly describe the specific measures in place to preserve the independence of the internal audit function (*n* = 98). Codes are non-exclusive. Percentages are calculated against the total number of code applications (*n* = 115), so they reflect the distribution of all coding references rather than the proportion of unique comments).

Selected supporting quotes for **application of independently delineated functions**:

Delineated ownership of risks

- "Internal audit is not responsible for assessing risks."
- "Internal audit does not set the procedures with controls in place to mitigate risks..."
- "Internal audit's role is restricted to either observer/participant within risk management processes."

Internal audit in advisory/consultant role

- "Internal audit works in an administrative and advisory role."
- "Internal audit plays an advisory role and a non-voting role in all ERM..."
- "The internal audit function facilitates the ERM process, but makes it very clear that the risks are owned by the business and executive management."

Separated risk assessments

- "ERM works with risk owners to ensure appropriate oversight and management of risk mitigating activities that are different in many cases from the formal controls used for audit testing and compliance."
- "While IA drives the risk assessment, management is clear that they own the assessment, are required to provide significant input, and own the results. IA uses the assessment as a primary input to its annual audit plan."

Other (varied)

- "The two functions have distinct charters with very little overlap."
- "Internal audit's charter specifies the roles and responsibilities of the internal audit function. Internal audit also understands the function is not responsible for business decisions."
- "The functions and responsibilities are defined in the company's bylaws and internal regulations."

Strategies for improving ERM programs

The results from the Baker Tilly and Internal Audit Foundation survey paint a clear picture: most ERM programs are not yet at a level of maturity where they deliver maximum value to their organizations. However, understanding where these programs fall short can help identify a pathway to greater success.

Weak technology adoption; inconsistent application and understanding of risk assessments, appetite, and strategy; middling collaboration and communication among key players; lack of executive support; and limited outreach to outside expertise each contribute to ERM's unfulfilled potential.

The following section provides analysis, discussion and strategic recommendations in three key areas:

- Timely risk assessments
- Communication, collaboration and roles
- Leveraging technology

TIMELY RISK ASSESSMENTS

Data reflecting that 3 out of 4 organizations have performed enterprise-wide risk assessments within the past three years, can be viewed positively. However, considering the extraordinary level of disruption and risk volatility since 2020 (COVID pandemic, geopolitical instability, AI integration, tariff wars) a single risk assessment in three years would be insufficient for most organizations.

The majority (67%) of those whose organizations have conducted risk assessments since 2022 report conducting them annually. But even this frequency may not be sufficient in disruptive times.

It is likely that assessments within divisions or functions occur more frequently, but this only paints a partial picture of risk. Relying on piecemeal approaches to risk assessment defeats the purpose of true enterprise-wide risk management.

Also missing are efforts to coordinate the timing of risk assessments to the timing of strategic planning. Of the organizations that report conducting risk assessments annually, just a quarter (25%) report they align with the business cycle. What's more, just over 6 in 10 (62%) report ERM offers information about risk and risk management for decision-making, but less than 4 in 10 (39%) say it aligns with risk management efforts.

It is troubling that a quarter of all respondents have not conducted a risk assessment in the past three years. Of this group, 62% cited insufficient resources and 49% cited a lack of leadership support as top reasons. Both point to failures in showcasing the value and usability of timely risk information. The challenge for ERM managers is to educate leadership about the greater value that timely risk assessments provide, which include improving risk mitigation, identifying emerging risks, and generating useful information for decision-making.

An additional component of timely risk assessment is understanding how effectively the organization mitigates its risks. Responses to a survey question on metrics for monitoring risk mitigation effectiveness reflect work is needed in this area.

A near majority of respondents (46%) said risk mitigation effectiveness is reported periodically as part of the established risk management program. This reflects such reporting is ad-hoc and not part of a formal process. About 4 in 10 (38%) said such reporting is required, but only for top risks. About a quarter of respondents (24%) said such reporting is required for critical or highly visible programs and initiatives. Another 18% said metrics are used occasionally for critical or highly visible programs and initiatives. Finally, 13% reported that no metrics for monitoring risk mitigation exist.

STRATEGIC TIPS: TIMELY RISK ASSESSMENTS

Communicate these key messages to the board and executive management on the benefits of timely enterprise-wide risk assessments.

- Up-to-date understanding of risk is fundamental to effective risk management to inform strategies and to set, monitor and evaluate risk appetites.
- Conducting a risk assessment annually is recommended for most organizations, although this may not mean a full assessment is needed every year.
- In disruptive times, assessing risk quarterly can help identify emerging trends and allow the organization to be more nimble in its response to risk.
- Risk assessments should include measuring risk mitigation efforts. If you don't know what's working and what's not, you won't know where to add resources to improve risk management.
- Risk assessment can be integrated into existing planning processes and budgets.
- The cost of frequent risk assessments is easily outweighed by the information they provide.
- Coordinate messaging to executive management and board on risk mitigation efforts, collaboration, and combined assurance.
- Coordinate preparation of risk assessments and relevant data and insights from ERM with strategic decision-making cycles.

COORDINATED EFFORT AND COMMUNICATION WITH INTERNAL AUDIT

Survey participants were asked to describe how risk, compliance, and internal audit functions coordinate their efforts. Six in 10 (60%) indicated that risk information is shared among these functions. However, coordination among them happens only annually – in activities such as risk assessments – for half (50%) of respondents.

What's more, agreement on common taxonomies to describe risks, which can improve clarity and reduce confusion and duplication, were reported by just over a third (36%) of respondents. Nearly as many (31%) said meetings occur to communicate on activities, but there is no coordination.

While acknowledging the value of coordination, these data points reflect that ERM is driven more by process than purpose. Developing common risk assessments is more than an annual task to be ticked off a checklist. Ideally, coordinated risk assessments are part of a corporate culture that appreciates an enterprise-wide understanding of risk and its power to generate information and insights beyond the siloed views of individual functions, departments, or activities.

Greater coordination and collaboration can lead to enhanced risk assessments that leverage technology, improve measures for success, consider risks beyond likelihood and impact to include preparedness and velocity, and consider scenario planning.

Roles

The survey asked respondents to describe how their organizations ensure understanding of risk roles, responsibilities and scope of coverage.

Understanding of risk roles and responsibilities appears to focus primarily on documentation, with half (50%) of respondents reporting formal documentation of roles, and 53% reporting role documentation, review, and periodic updates. Just over six in 10 (61%) report roles are communicated to appropriate personnel.

However, more mature approaches to understanding and embracing roles, such as risk training and documentation to both risk and non-risk teams, were reported by fewer than 4 in 10 (37%). Nearly 2 in 10 (18%) reported roles and responsibilities across risk functions are informal.

STRATEGIC TIPS: COMMUNICATION, COLLABORATION AND ROLES

- Greater meeting cadence is key. Seek opportunities for more formal and informal meetings on a quarterly basis among key risk players.
- Creating specialized committees focused on key risk areas, such as cybersecurity or IT, can improve communication and collaboration. Make sure risk, compliance, and internal audit leaders are included.
- Seek out technology tools, such as SaaS and GRC software, that make information sharing easy, transparent, and productive.
- Create more opportunities to share knowledge, such as job swaps, guest auditor or reciprocal training programs.
- Embracing roles means more than simply adding a line to a risk manager's job description.
- Conduct annual risk training to key stakeholders on the risk program. This might include risk owners or all employees to promote a wide understanding of risk and to drive risk culture..

LEVERAGING TECHNOLOGY

Organizations that use technology for more mature ERM activities, such as automating interface with data repositories, advanced risk analytics, or modeling risk exposures are rare. Indeed, the majority of ERM programs (59%) still rely on basic tools, such as word processing and spreadsheets.

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.

Readily available SaaS and GRC tools can help to elevate basic ERM programs and realize greater value from enterprise-wide understanding of risks. Such platforms can centralize data, automate workflows, and provide visibility into risks, leading to more informed choices and reduced risk exposure.

Similarly, AI has the potential to kickstart ERM programs that have yet to reach their potential. But the vast majority of ERM programs have yet to leverage this technology, with fewer than 1 in 10 (6%) reporting AI is used frequently to assist in identifying risks, and just 3% reporting AI is used heavily for data input into risk management activities.

STRATEGIC TIPS: LEVERAGING TECHNOLOGY

- Leverage internal resources with data analytic skills to build home-grown digital tools.
- Start with basic automation tools, such as Power BI, the Microsoft Suite and large language models (LLMs), such as ChatGPT.
- Internal auditors can become advisors and technology advocates. Educate the board and executive management on the benefits of GRC platforms, including automated workflows, reduced risk exposures and increased transparency.
- Review existing technologies used throughout your organization for ways in which risk data could be incorporated into current systems.
- Support, facilitate and monitor exploration of safe AI use within the organization and look to incorporate AI into ERM processes.
- Look for opportunities to apply GRC and other software across multiple functions and activities to promote collaboration, demonstrate transparency and improve tech ROI and create a plan to build tools out over time. Transforming to a digital model may take months or years.

Conclusion

In today's dynamic risk landscape, having a clear, well-informed and enterprise-wide view of risk is fundamental to navigating uncertainties, protecting assets and building strategies that enhance performance and ensure sustainable success. A mature and aligned ERM program provides the structure to deliver that view. However, survey data reflect that most ERM programs are just scratching the surface.

Aligning risk information and insights with strategic decision-making is the ultimate benefit ERM can provide. Ensuring effective and astute risk assessment and measurement, identifying and understanding emerging risks, leveraging technology to support efficient and agile data collection and metrics, and enhancing resilience through effective scenario planning are all attributes of mature ERM.

Such maturity translates to risk assessments that go beyond likelihood and impact to consider management preparedness and velocity that help ensure resilience. 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.

Like all risk management, ERM is unique to each organization and is only as strong as the information it collects and insights it can provide. The ERM shortfalls identified in this report center on the effectiveness of enterprise-wide risk assessments; communication, collaboration and roles; lack of executive support; and technology use. ERM leaders are urged to use the benchmarking data and suggested strategies provided to improve their programs.

Appendix

Survey demographics

REGION

Q35. In what region is your organization based? *n* = 567.

Africa	5.1%
Asia Pacific (Including Central Asia)	9.2%
Europe	7.2%
Latin America (South America, Central America, Mexico, and the Caribbean)	18.3%
Middle East	0.4%
North America	59.8%
	100%

PROFESSIONAL FOCUS

Q26. Which of the following best describes your current professional focus? (Choose one.) *n* = 567.

Accounting or finance	3.7%
Audit committee/board member	3.7%
CEO	1.2%
Compliance	4.8%
C-suite/executive management	4.6%
Educator	0.5%
External audit	0.2%
Fraud	0.4%
Information technology (IT) or related	0.5%
Internal audit	61.4%
Internal controls over financial reporting (ICFR)	1.1%
Legal/general counsel	0.2%
Other	1.8%
Risk management	16.0%
	100%

PROFESSIONAL ROLE

Q27. Which of the following best describes the level of your professional role? *n* = 567.

Executive management	29.6%
Director or equivalent	37.9%
Senior manager/manager	23.8%
Staff	7.8%
Other	0.9%
	100%

ORGANIZATION SIZE

Q30. For your organization as a whole, choose the range that best describes the current total number of full-time equivalent employees (FTEs). *n* = 567.

More than 50,000	7.1%
10,001 to 50,000	14.6%
5,001 to 10,000	13.9%
1,501 to 5,000	21.7%
501 to 1,500	18.3%
500 or fewer	22.2%
Not sure/not applicable	2.1%
	100%

INTERNAL AUDIT FUNCTION

Q33. How many full-time-equivalent employees are in your internal audit function (including the chief audit executive and sourced staff)? *n* = 567.

Over 50	6.9%
21 to 50	10.9%
11 to 20	14.1%
6 to 10	19.0%
2 to 5	33.0%
1	8.3%
No separate internal audit function	6.2%
Not sure	1.6%
	100%

ENTERPRISE RISK MANAGEMENT FUNCTION

Q34. How many full-time-equivalent employees are in your ERM function? *n* = 567.

Over 50	3.9%
21 to 50	2.5%
11 to 20	4.2%
6 to 10	8.5%
2 to 5	34.7%
1	21.9%
Not applicable – We do not have a separate ERM function	21.9%
Not sure	3.2%
	100%

ORGANIZATION TYPE

Q28. What type of organization do you currently work for? (If you are a service provider, please answer based on your primary client.) *n* = 567.

Nonprofit or not-for-profit organization	13.9%
Not sure/not applicable	0.4%
Other	1.1%
Privately held organization	30.7%
Public sector	19.8%
Publicly traded organization	30.7%
Service provider/consultant	3.5%
	100%

INDUSTRY CLASSIFICATION

Q29. What is the primary industry classification of the organization for which you work (or your primary client if you are a service provider)? *n* = 567.

Energy, industrial and consumer products	27.00%
Government and public services	20.60%
Financial services	20.30%
Healthcare	12.00%
Technology	6.90%
Professional services (including legal)	4.90%
Other	4.90%
Construction and real estate	2.80%
Restaurants	0.40%
Private equity	0.20%
	100%

About The Institute of Internal Auditors and the Internal Audit Foundation

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 260,000 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 Internal Audit Foundation is an essential global resource for advancing the internal audit profession. Foundation-funded research provides internal audit practitioners and their stakeholders with insight on emerging topics and promotes and advances the value of the internal audit profession globally. In addition, through its Academic Fund, the Foundation supports the profession's future by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership program. For more information, visit theiia.org/Foundation.

About Baker Tilly

Baker Tilly, operating under an alternative practice structure, is a leading assurance, tax and advisory firm that provides a comprehensive range of professional services to businesses, organizations, entities and individuals. Beyond those borders, we are reshaping the industry by protecting and enhancing our clients' value through forward-thinking strategies, cutting-edge innovation and a bold willingness to blaze new trails. The result is a customized pathway to success for each of our clients, as we deliver tailored solutions that help them achieve financial stability, regulatory compliance and sustainable long-term growth.

Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, are independent members of Baker Tilly International, a worldwide network of independent accounting and business advisory firms in 143 territories, with 43,500 professionals and a combined worldwide revenue of $5.62 billion. Visit bakertilly.com.

IIA Internal Audit Foundation

2024–25 BOARD OF TRUSTEES

President
Warren W. Stippich Jr., CIA, CRMA

Officers
Glenn Ho, CIA, CRMA

Nora Kelani, CIA

Shirley Livhuwani Machaba, CCSA, CRMA

Trustees
Subramanian Bhaskar

Jose Gabriel Calderon, CIA, CRMA

Susan Haseley, CIA

Dawn Jones, CIA, CRMA

Reyes Fuentes Ortea, CIA, CCSA, CRMA

Anthony J. Pugliese, CIA

Hossam El Shaffei, CCSA, CRMA

Michael A. Smith, CIA

Staff Liaison
Laura LeBlanc,
Senior Director, Internal Audit Foundation

2024–25 COMMITTEE OF RESEARCH AND EDUCATION ADVISORS

Chair
Nora Kelani, CIA, CRMA

Members
Tonya Arnold-Tornquist, CIA, CRMA

Christopher Calvin, PhD, CIA

Joseph Ian Canlas, CIA, CRMA

Andre Domingos

Christina Duquette, CRMA

Marc Eulerich, PhD, CIA

Dagmar Flores, CIA, CCSA, CRMA

Anargul Kairulla, CIA

Ayaka Mitsunari

Ahmed Shawky Mohammed, DBA, CIA

Grace Mubako, PhD, CIA

Ruth Doreen Mutebe, CIA

Emmanuel Pascal, CIA, CRMA

Brian Tremblay, CIA

Koji Watanabe

Stacy Wright, CIA

Staff Liaison
Nicole Narkiewicz, PhD
Director, Academic and Research Strategy,
The IIA

Baker Tilly is a leading advisory, tax and assurance firm, providing clients with a genuine coast-to-coast and global advantage in major regions of the U.S. and in many of the world's leading financial centers – New York, London, San Francisco, Seattle, Los Angeles, Chicago and Boston. Baker Tilly Advisory Group, LP and Baker Tilly US, LLP (Baker Tilly) provide professional services through an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable laws, regulations and professional standards. Baker Tilly US, LLP is a licensed independent CPA firm that provides attest services to its clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and business advisory services to their clients. Baker Tilly Advisory Group, LP and its subsidiary entities are not licensed CPA firms.

Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, are independent members of Baker Tilly International, a worldwide network of independent accounting and business advisory firms in 143 territories, with more than 47,000 professionals and a combined worldwide revenue of more than $6 billion. Visit bakertilly.com or join the conversation on LinkedIn, Facebook and Instagram.

Let's connect Baker Tilly US @bakertillyus bakertilly.com