Digital Risk Report 2024

Opportunities and Challenges of the AI Frontier

AUDITBOARD

Table of Contents

Introduction

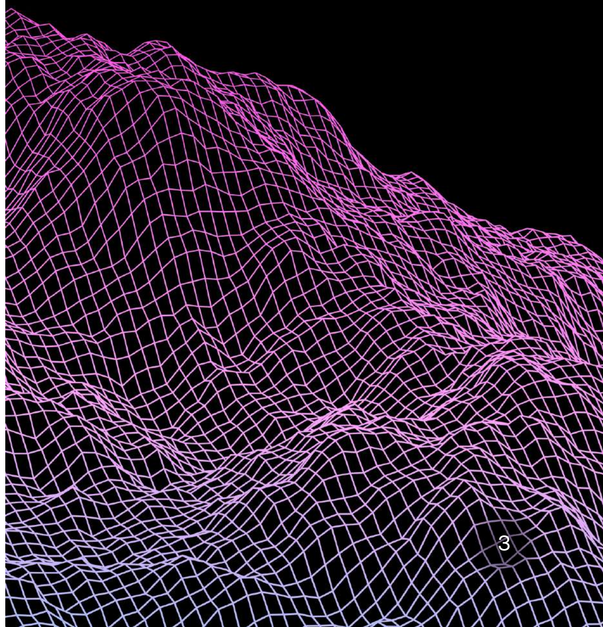
In an era where digital threats are increasingly complex and pervasive, the need for more sophisticated digital risk strategies is undeniable. The good news is that most companies are heeding the call to this need. Up significantly from last year, two-thirds (65%) of security professionals and department leaders surveyed report being in advanced stages of digital risk management maturity, actively mitigating or continuously monitoring digital risk.

This substantial uptick indicates a positive trend towards proactive and advanced risk management practices necessary for staying ahead of digital threats. But how are organizations handling the execution and management of digital risk initiatives, and what should enterprises prioritize now and in the years ahead?

To help answer these questions and others, AuditBoard, in partnership with Ascend2 Research, fielded the 2024 Digital Risk Survey to 404 professionals involved with their organization's cybersecurity and digital risk approach. The 2024 Digital Risk Survey reveals a transformative shift in how organizations manage and mitigate digital risks. This report provides a comprehensive analysis of current practices, highlighting significant advancements and offering actionable recommendations to further enhance digital risk management strategies. Emphasizing the need for an integrated risk management framework and technology, the report showcases how the interconnectivity of technology assets and business processes drives strategic goals.

Utilize the insights from this report to guide your efforts in promoting the advancement of your digital risk management initiatives, navigating the complexities of digital risk, and building more resilient risk management frameworks.

Throughout this report, you will see references to this integrated risk management framework and associated technology as ***connected risk***. Connected risk is the modern, technology-enabled, cross-functional approach to managing risk across the enterprise that is fundamental. Adopting a connected risk approach is fundamental to close the risk exposure gap that occurs when escalating risk demands outstrip risk management resources.



Key Findings & Trends

Rapid Maturation of Digital Risk Management

Nearly two-thirds (64%) of security professionals report that their companies are in the late stages of digital risk management maturity, a significant increase from the 26% reportedly in these more advanced stages in 2023.

Strong Collaboration Yields Better Results

Organizations with strong interdepartmental collaboration are significantly more likely to find their digital risk metrics effective and manage third-party risks comprehensively.

Enhanced Third-Party Risk Management

37% of organizations manage and monitor third-party digital risk using qualitative and quantitative assessments supported by various methodologies such as risk questionnaires, audits, and independent data analysis.

Extensive Use of Reportable Metrics

87% of companies utilize reportable metrics to manage digital risk, with 59% finding these metrics very effective, particularly during decision-making.

Increasing Role of AI

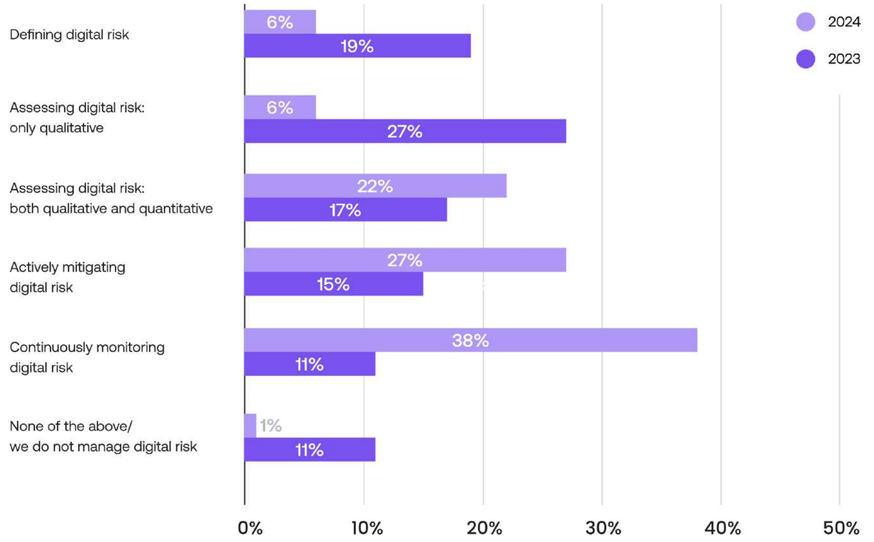
78% of organizations are tracking AI as an emerging technology risk, and many are leveraging AI to improve productivity, enhance threat detection, and automate responses.

TREND

Digital Risk Maturity: 2024 vs 2023

Figure 1

How would you describe your organization's digital risk management maturity level?



Strategic Implications for Organizations

Integrating digital risk management into broader enterprise risk management frameworks can significantly enhance digital risk management strategies. This integration ensures alignment across the enterprise, resulting in a more comprehensive and cohesive risk strategy. Strong collaboration across different departments is crucial, as it breaks down silos and fosters a unified approach to managing digital risks.

> *52% of organizations have integrated digital risk management into enterprise risk management frameworks. This group reports more effective metrics, more advanced third-party monitoring, and stronger collaboration between functions that work together on digital risk.*

Using a combination of qualitative and quantitative assessments provides a well-rounded view of risks, improving the accuracy and effectiveness of risk management strategies. 37% of organizations use qualitative and quantitative assessments supported by comprehensive methodologies such as risk questionnaires, audits, and independent data analysis. These comprehensive methodologies ensure thorough risk evaluations, essential for managing third-party risks and other complex risk landscapes.

> *Organizations that base their qualitative and quantitative risk assessments on internal and external views are more likely to find their reportable metrics highly effective.*

Technology can be transformative. Cloud-based solutions enable organizations to manage risks more effectively in a dynamic environment. The shift towards cloud-based risk management software is critical for enhancing efficiency and scalability. Meanwhile, the use of AI is becoming more widespread and can enhance risk management capabilities significantly, particularly in automating responses and improving threat detection. Enterprises, however, must balance the risks and rewards of AI use.

> *81% of enterprises report using cloud-based risk-management software as their primary means of managing digital risk.*

Organizations must adopt a modern and collaborative approach to risk management to address the risk exposure gap. Connected risk platforms can significantly improve risk identification and decision-making, supporting an integrated and efficient approach. This strategy utilizes purpose-built technology to connect teams, unify data, and automate processes.

Best Practice #1:

Embrace Comprehensive Risk Assessments

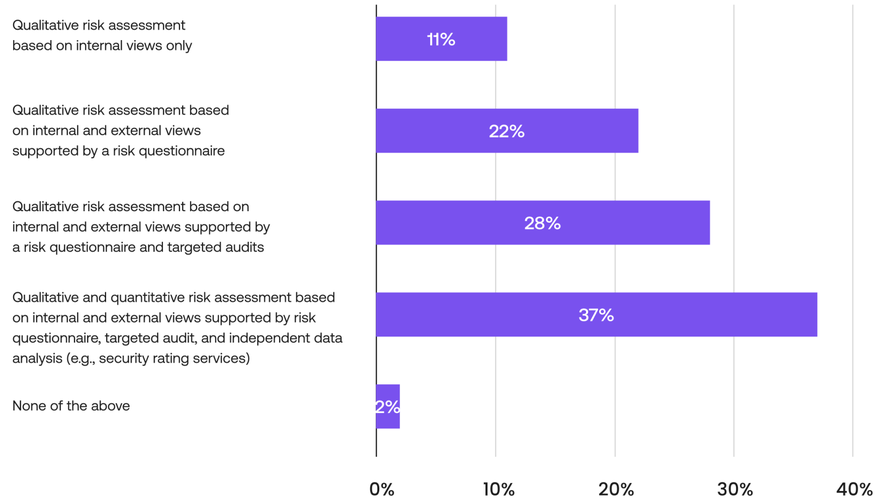
Combine Qualitative and Quantitative Analysis

Many organizations recognize the importance of a thorough and multifaceted approach to managing third-party digital risk. 37% of those surveyed used a combination of qualitative and quantitative risk assessments supported by risk questionnaires, targeted audits, and independent data analysis. Qualitative assessments provide context and detailed insights into the nature and potential impact of threats, while quantitative assessments offer measurable and objective data.

Enterprises combining qualitative and quantitative analysis based on internal and external views are arming themselves with more robust data, making them better positioned to identify, assess, and manage third-party risks effectively. In fact, according to our research, these organizations are significantly more likely to find their reportable metrics to be very effective.

Figure 2

How are you managing and monitoring third-party digital risk?



> *Those incorporating internal and external perspectives on qualitative and quantitative risk assessment are 1.5x more likely than all others to find their reportable metrics very effective (74% vs. 49%).*

NEXT-LEVEL APPROACH

The Benefits of Real-Time Data and Automation

Integrating real-time data feeds and automated risk-scoring systems into your reporting will make your data work harder, enhancing the timeliness and accuracy of third-party risk assessments.

- **Make more effective decisions.** Real-time insights enable more informed decision-making, prioritization of risk mitigation efforts, and allocation of resources.
- **Improve efficiency.** Automation can help streamline processes and workflows, allowing enterprises to scale risk management efforts more seamlessly.
- **Get ahead of risk.** With real-time data and automated scoring, organizations can proactively monitor third-party risks, identifying potential issues before they escalate.

Incorporate Internal and External Perspectives

Nearly two-thirds (65%) of organizations incorporate internal and external views in their qualitative risk assessments. These views are supported by techniques such as risk questionnaires and targeted audits. This approach helps organizations get a complete picture of third-party risks, ensuring that internal insights and external factors are considered, providing a thorough understanding of risks from multiple perspectives.

Internal data highlights company-specific issues, while external data reveals industry-wide challenges and external threats. Together, they enable the development of holistic risk mitigation strategies that address all potential risk areas.

External data can also help to validate and complement internal data, providing an objective viewpoint that can improve the accuracy of risk assessments. By incorporating external threat intelligence and industry trends, companies can anticipate and prepare for emerging risks. This proactive approach allows for timely adjustments to risk management strategies.

NEXT-LEVEL APPROACH

The Importance of Data Validation and Optimization

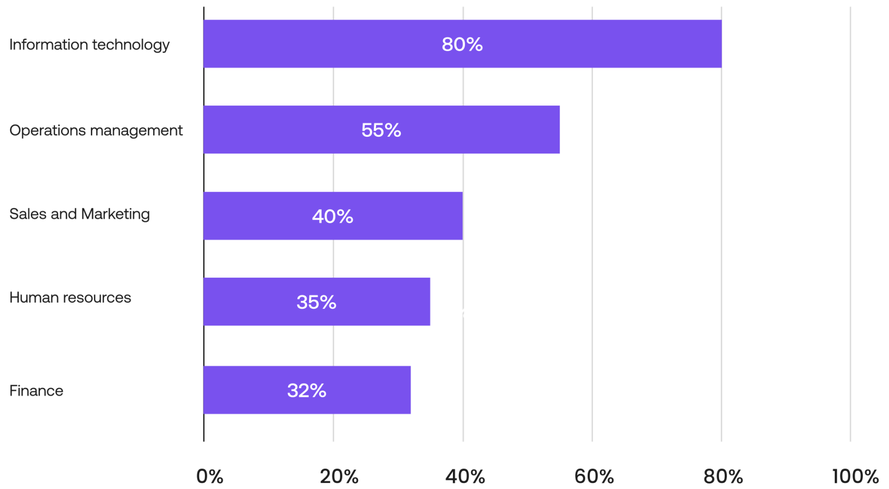
Digital threats constantly evolve, with new vulnerabilities and attack vectors emerging regularly. That is why continuous validation of the data you collect and a focus on continuous improvement of risk management are critical. This ensures that risk assessments remain relevant and effective in addressing current threats, allowing enterprise organizations to anticipate and respond to emerging threats proactively.

Advanced analytics, machine learning, and automation can further optimize risk assessment processes and will be key to managing and mitigating risk at scale. These technologies can identify potential threats and risk factors for more comprehensive insight, and learn and adapt to become even more accurate over time.

Four of five IT teams use AI to support their risk management objectives, but AI shouldn't be limited to IT. Cross-departmental use of these technologies can enhance threat detection and efficiency, scalability, collaboration, and resiliency across the organization. In fact, those with the strongest digital risk management collaboration report more use of AI in their finance, IT, and HR departments than others.

Figure 3

Which teams are using AI to support strategic objectives?



Best Practice #2:

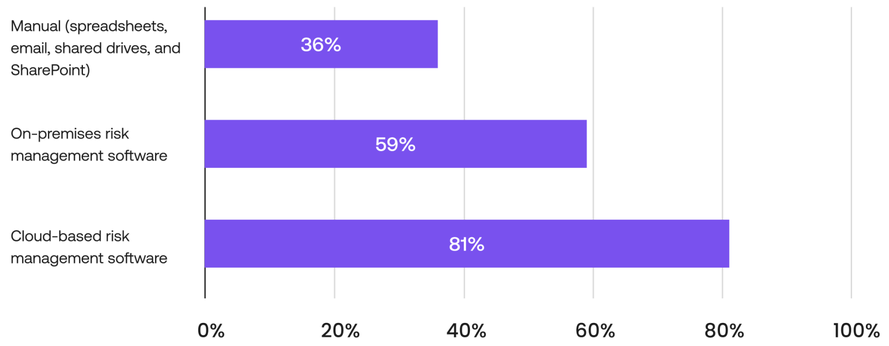
Leverage Advanced Technologies

Adopt Cloud-Based Risk Management Solutions

Our research indicates a **notable shift towards utilizing cloud-based risk management software as a primary solution for managing digital risk, with 81% of security professionals reporting use**. In 2023, only about 30% of enterprises reported using cloud-based solutions as their primary means of digital risk management. Replacing manual processes with cloud-based risk management solutions is crucial for improving efficiency and scalability in digital risk management.

Figure 4

What technology do you primarily use to manage digital risk?



NEXT-LEVEL APPROACH

Features to look for in cloud-based solutions

Select a cloud-based risk management technology that enhances your security posture, integrates smoothly with your operations, improves efficiency, and supports comprehensive risk management. Consider the following features as essential in your search:

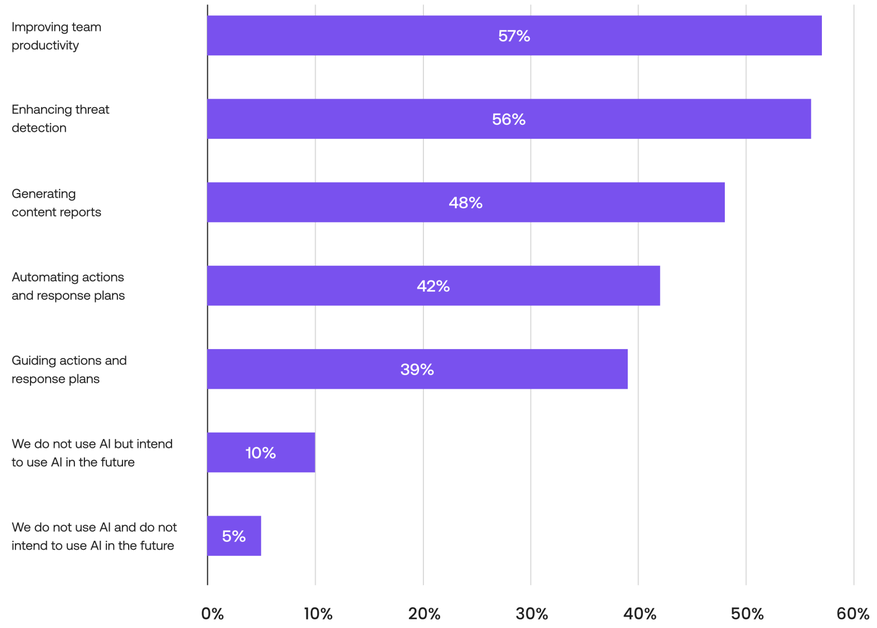
- **Robust security features:** Ensure data is protected from unauthorized access, breaches, and other cyber threats. Advanced security features often include real-time monitoring, threat detection, and automated response capabilities.
- **Compliance certifications:** Compliance certifications indicate that the cloud-based technology meets regulatory standards and adheres to best practices. This builds trust and provides assurance that data is being treated with safety and care.
- **Integration capabilities:** Integrating risk management technology with other enterprise systems enables a unified approach, ensuring smooth data flow and comprehensive risk management.

Implement AI

Over half of the enterprise organizations surveyed use AI to improve team productivity and enhance threat detection to better their digital risk posture. Nearly half say they use it in reporting and automating action and response plans.

Figure 5

Are you using AI in any of the following ways to enhance your digital risk posture?



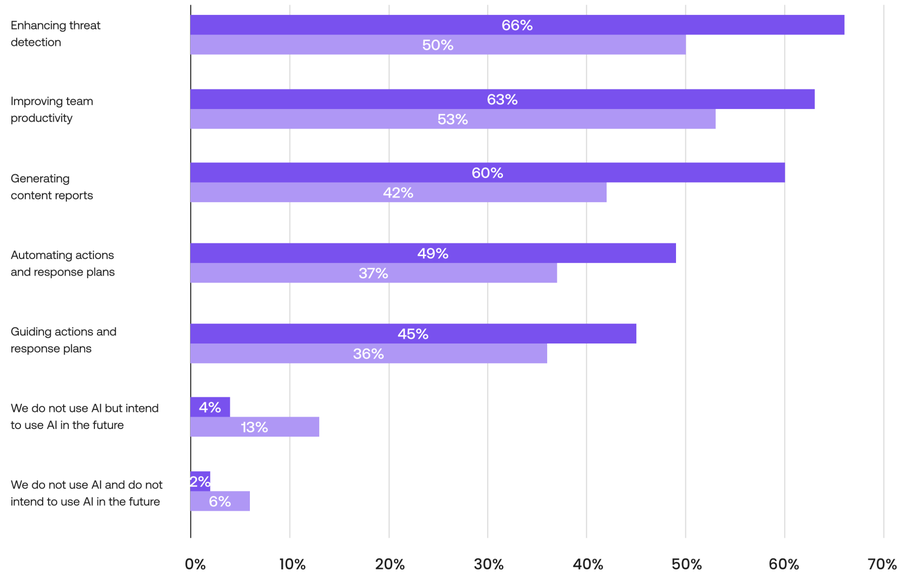
NEXT-LEVEL APPROACH

Invest in AI Training to Maximize Use

Those with the strongest team collaboration are significantly more likely to use AI to enhance their digital risk posture. As you implement technologies like AI and machine learning into your risk management strategy, investing in the proper training of team members can make a significant difference in maximizing their use.

Figure 6

Are you using AI in any of the following ways to enhance your digital risk posture?



Best Practice #3:

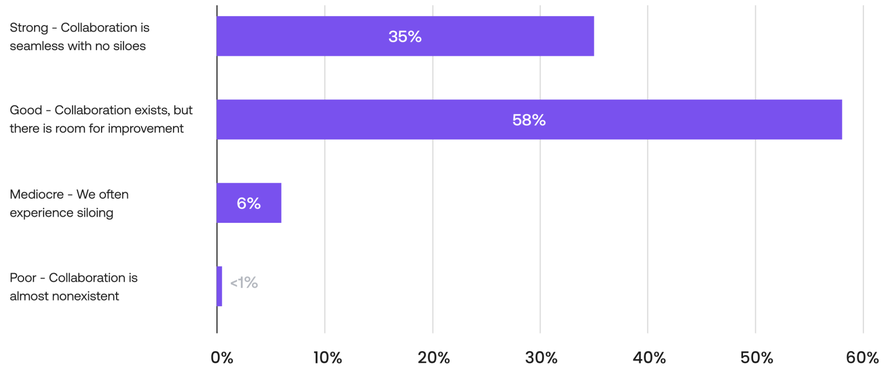
Foster Strong Interdepartmental Collaboration

Encourage Seamless Collaboration Between Departments

58% of professionals surveyed say they collaborate with functions working on digital risk, but there is room for improvement in how effectively they collaborate. Just over one-third (35%) say they have strong collaboration. Effective collaboration is essential for a comprehensive, integrated approach to digital risk management.

Figure 7

How would you describe the collaboration between functions that work together on digital risk (such as internal audit, compliance, risk, legal, IT, etc)?



> *Strong collaboration across teams managing digital risk matters. Those with strong collaboration are more than two times more likely than all others to describe their reportable metrics as very effective (87% vs 41%).*

NEXT-LEVEL APPROACH

Ongoing Communication is Critical

Continuous cross-departmental communication and access to data are crucial to building strong collaboration on digital risk initiatives. Establish cross-functional risk committees and regular inter-departmental meetings to ensure ongoing communication and coordination. Use collaboration tools and platforms to facilitate seamless information sharing.

Break Down Silos

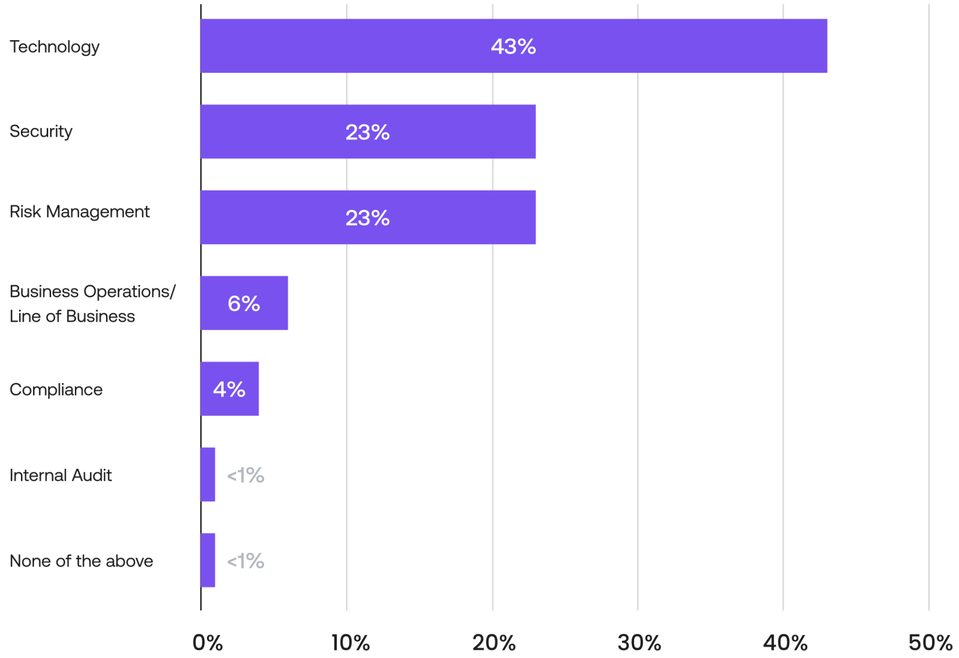
Aligning teams and removing silos is essential in establishing and maintaining strong communication and collaboration to increase digital risk management effectiveness. **Silos can lead to fragmented views of risk**, where each department only focuses on its specific threats without understanding the broader risk landscape. Removing siloes ensures that risk management efforts are integrated, providing a holistic view across the organization.

Who Is Responsible for Digital Risk Management?

For 43% of companies surveyed, technology departments are primarily responsible for managing digital risk, while nearly one quarter (23%) say that security or risk management departments are primarily responsible.

Figure 8

Who is primarily responsible for managing digital risk in your organization?



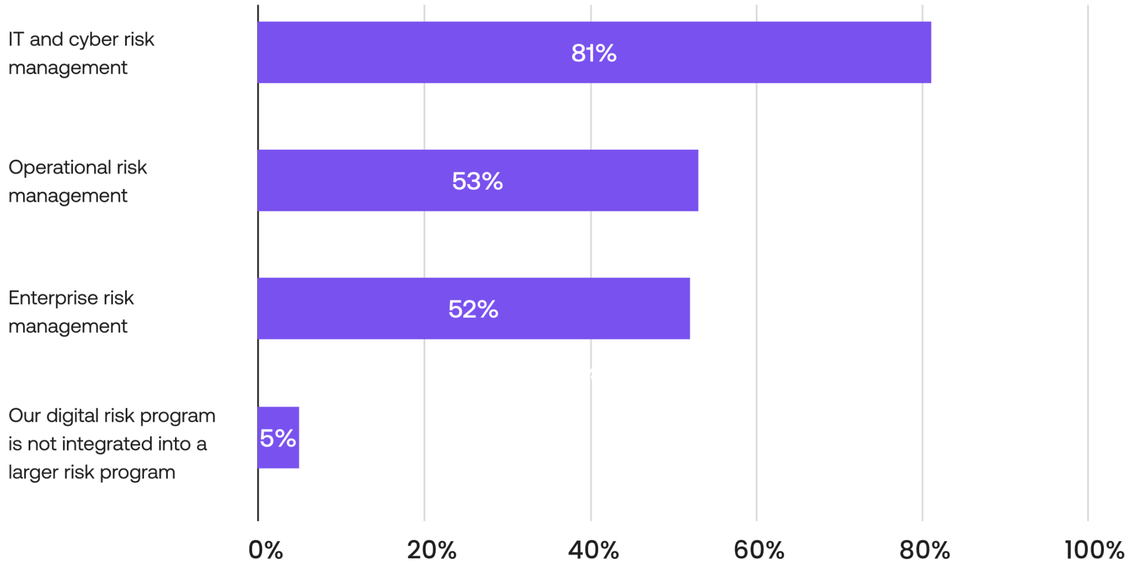
Integrate Digital Risk Management Across the Enterprise

While 81% of enterprise organizations have their digital risk management program integrated into IT and cyber risk management, **just over half say their digital risk program is integrated across the enterprise**. Enterprise-level integration is vital for improving collaboration, enhancing risk assessment, and creating a holistic view of risk that addresses all potential risk areas.

> *Organizations with digital risk management programs integrated into broader enterprise risk management frameworks report stronger collaboration, more effective reportable metrics, and more advanced third-party monitoring than others.*

Figure 9

How is your organization's digital risk management program integrated into a larger risk program?



NEXT-LEVEL APPROACH

Create Dashboards That Provide a Unified View of Risk

Enterprise organizations should have integrated risk management dashboards that provide a unified view of all risk areas. This will enable more informed decision-making and more effective risk management.

When creating these dashboards, it is crucial to define and align objectives across departments and use these objectives to build a comprehensive view of all risk areas. Regular testing, validation, reviews, and updates are all necessary to maintain effectiveness and alignment with organizational goals.

Best Practice #4:

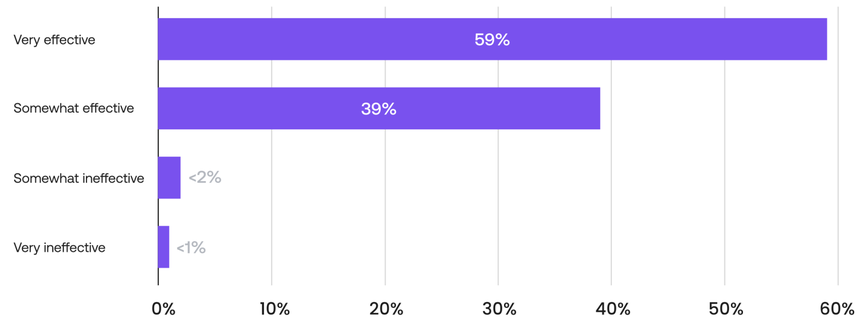
Utilize Effective Reportable Metrics

Develop and Use Actionable Metrics

Our research reveals extensive use of reportable metrics, with nine out of ten (87%) enterprise organizations reporting use to manage digital risk. Moreover, nearly all companies using reportable metrics find them effective, with a majority (59%) considering them very effective. Again, this underscores the importance of data-driven decision-making in digital risk management strategies.

Figure 10

Rate the effectiveness of your reportable metrics in managing digital risk.



> *97% of security professionals using reportable metrics find them effective in managing digital risk.*

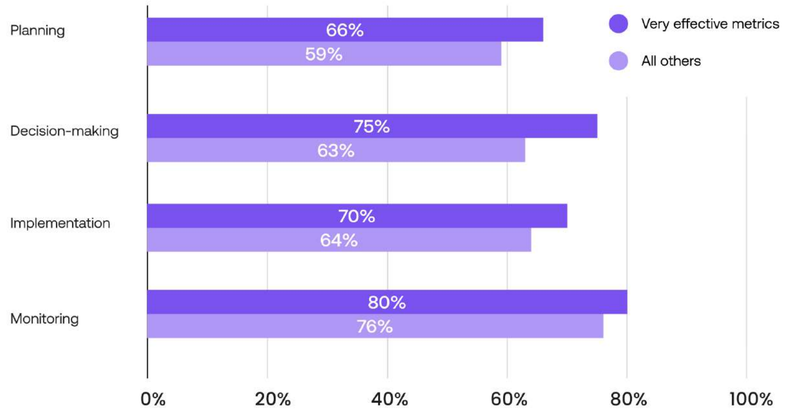
NEXT-LEVEL APPROACH

Use Reportable Metrics in All Stages of Product Development

Overall, 78% of companies use metrics in the monitoring stage of the digital product/service development process, and another 70% use metrics in the decision-making phase. About two-thirds of those surveyed use metrics in the implementation (68%) and planning (63%) stages. Interestingly, those who consider the metrics they use to be very effective are significantly more likely to use reportable metrics in all stages of the digital product/service development process, most notably in the decision-making stage (75% of those with very effective metrics strategies use reportable metrics in their decision-making phase of product development vs just 63% of all others).

Figure 11

In which stages of the digital product/service development process are you utilizing reportable metrics?



Continuously Monitor and Refine Metrics

By continuously monitoring and refining reportable metrics, organizations can maintain a digital risk management program responsive to changes in the ever-evolving threat landscape and regulatory environment while adapting to their specific organizational needs. Regularly updating and optimizing these metrics can help organizations:

- **Adapt to evolving digital threats:** Continuous monitoring allows for timely adjustments to risk management strategies.
- **Ensure accuracy and relevance:** Metrics can become outdated or irrelevant over time. Regular refinement ensures metrics provide a true picture of an organization's risk posture.
- **Remain compliant:** Continuously monitoring and optimizing metrics helps organizations adhere to regulatory frameworks and demonstrates a strong commitment to compliance.
- **Optimize resource use:** By regularly updating metrics, organizations can use data to determine which risks need immediate attention and where to focus efforts.

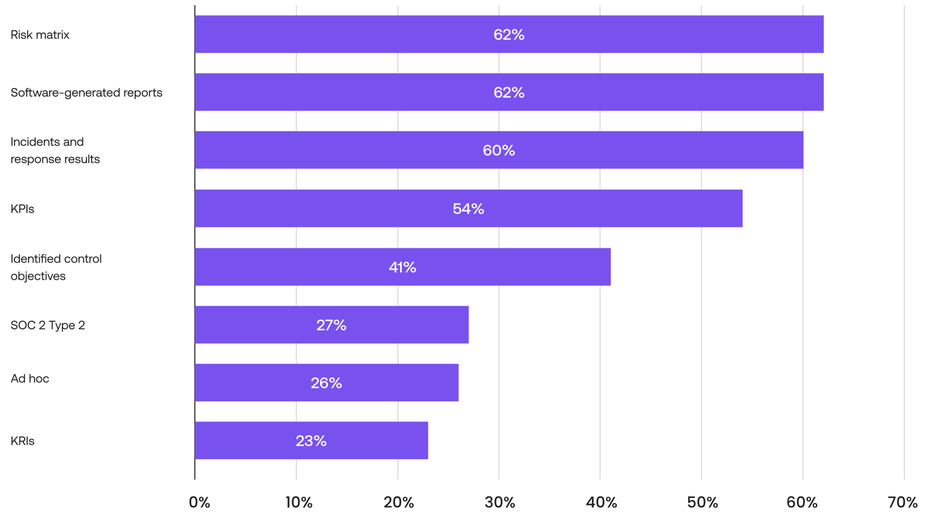
NEXT-LEVEL APPROACH

Which Metrics Are Most Frequently Used by the Enterprise?

Among all organizations surveyed, the most commonly used metrics in digital risk management are risk matrices, software-generated reports, and incidents and response results.

Figure 12

Which of the following metrics are you using?



Those who report the most success from their metrics are significantly more likely than those with less effective metrics to be using software-generated reports (68% vs 54%), KPIs (61% vs 43%), identified control objectives (46% vs 34%) and KRIs (27% vs 16%).

Best Practice #5:

Prepare for Emerging AI Risks

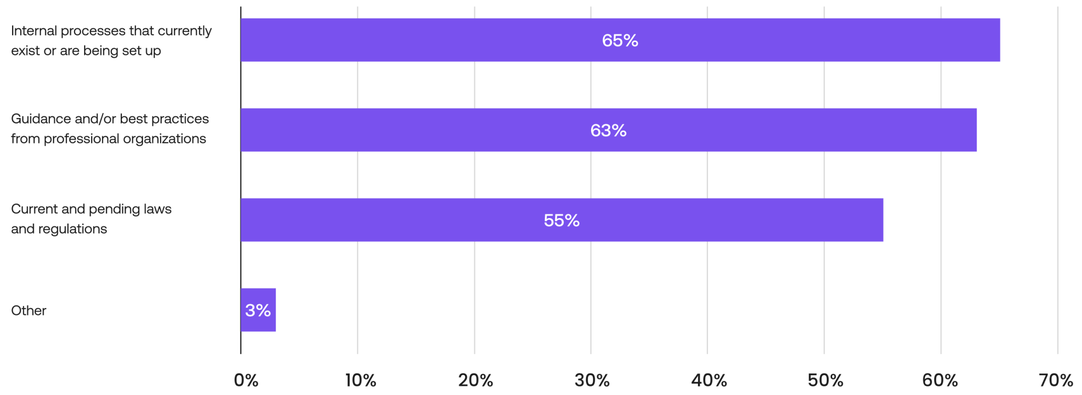
Track and Assess AI-Related Risks

While AI can be pivotal in improving efficiency and efficacy in managing digital threats, enterprise organizations must consider the potential risks associated with using AI. **The most effective use of AI requires active awareness and management of the risk exposure it carries.** The vast majority (78%) of organizations surveyed have identified and are tracking AI as an emerging technology risk.

Two-thirds of organizations prioritize AI risk assessment using existing internal processes and/or guidance and best practices from professional organizations. Another 55% say they use current and pending laws/regulations to prioritize AI risk.

Figure 13

How does your organization prioritize the evaluation and assessment of AI risk?



NEXT-LEVEL APPROACH

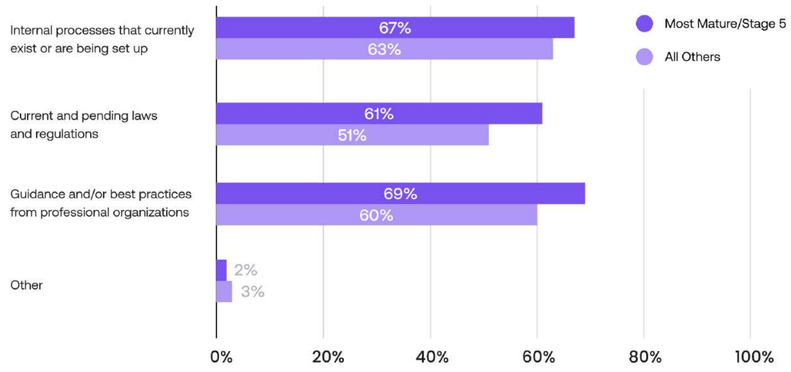
Use Established Internal Processes and External Guidelines to Manage AI Risk

Those with the most sophisticated digital risk management strategies are significantly more likely to evaluate and assess AI-related risk using current and pending laws and regulations, guidance from outside organizations, and existing internal processes.

By relying on a combination of these areas, organizations gain a more comprehensive understanding of the emerging risks associated with AI and can formulate a more holistic approach to managing those risks.

Figure 14

How does your organization prioritize the evaluation and assessment of AI risk?



Ensure the Proper Use of AI

Ethical and responsible use of AI to support digital risk management objectives is essential in maintaining high AI-related risk tolerance. By implementing a framework for responsible AI use, enterprise organizations can ensure that AI supports their digital risk management objectives while maintaining trust and integrity in their AI initiatives.

- **Establish a set of AI principles and policies:** Adopt ethical principles to guide the use of AI within the organization, as well as a set of policies and procedures that outline AI-related development, deployment, and monitoring.
- **Form a cross-departmental AI ethics committee:** Form a committee across multiple departments to oversee AI initiatives to ensure consideration of various perspectives.
- **Conduct regular AI assessments:** Audit AI systems to ensure they comply with established ethical guidelines and governance policies.
- **Provide training**: Educate employees with training sessions that cover ethical principles, regulatory requirements, and best practices for the responsible use of AI.

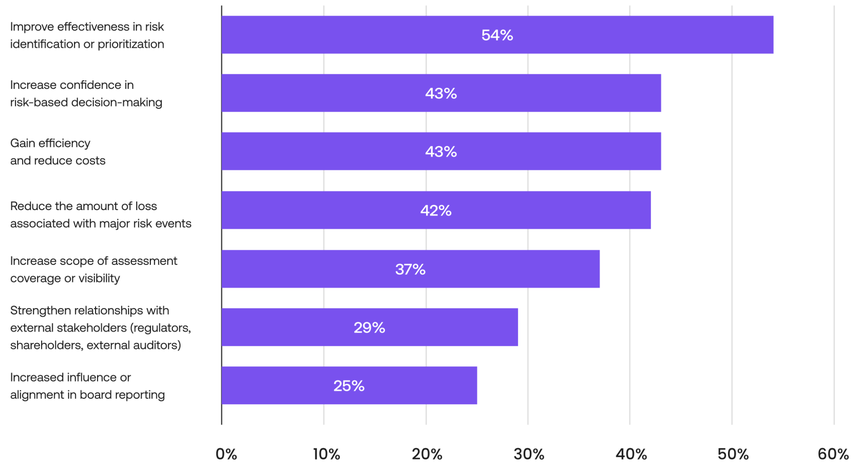
> *Nearly half (46%) of enterprise organizations surveyed feel they have high levels of risk tolerance toward AI. Another 42% report a moderate AI risk tolerance.*

Navigating the Complexities of the Digital Risk Frontier

The findings from this survey underscore the critical importance of evolving digital risk management practices. As organizations mature in their approaches, integrating advanced technologies and fostering strong collaboration will be vital to staying ahead of emerging threats. Organizations can better protect their digital assets and ensure long-term resilience by adopting the best practices outlined in this report.

Figure 15

What are the primary benefits of adopting a connected risk platform?



- **Adopt comprehensive third-party risk assessments.** Organizations using both qualitative and quantitative assessments from both internal and external perspectives have more effective reportable metrics.
- **Upgrade technologies to support digital risk management.** Cloud-based risk management solutions and AI can enhance threat detection and improve decision-making capabilities.
- **Include risk-adjacent departments in risk management initiatives.** Encouraging cross-departmental alignment can provide a holistic view of risk and improve risk management effectiveness.
- **Optimize reportable metrics.** Determine and regularly assess the most effective reportable metrics to be applied across all stages of digital product development.
- **Balance risk vs. reward when using AI.** Determine how the use of AI might expand risk exposure and create guidelines and systems to prevent AI-related threats.
- **Adopt a connected risk platform.** Close the risk exposure gap by adopting a modern and collaborative approach to risk management that utilizes purpose-built technology to connect teams, unify data, and automate processes. Learn more about connected risk here.

By following these steps and leveraging the 2024 Digital Risk Survey insights, organizations can better navigate the complexities of digital risk and build more resilient risk management frameworks.

Participants and Methodology

Participants

N = 404 security professionals and organizational leaders

Methodology

Auditboard, in partnership with Ascend2 Research, developed a custom online questionnaire to survey 404 security professionals and organizational leaders working for enterprise organizations with over $25M in revenue across varying industries in the United States. All survey participants were in managerial roles or above and confirmed involvement in their organization's cybersecurity and digital risk approach. The survey was fielded in May 2024.

Job Role	
Senior Executive	36%
Internal Audit, Risk Management, or Compliance	8%
Security or Technology	40%
Business Operations	11%
Finance	4%
Legal	1%

Industry	
Industrial	23%
Technology	39%
Finance and insurance	10%
Services	22%
Government and education	5%
Non-profit	1%

Company Size	
1 to 99 employees	3%
100 to 999 employees	30%
1,000 to 9,999 employees	49%
10,000 or more employees	18%

Company Revenue	
Less than $500M	25%
$500M - $1B	34%
$1.1B - $10B	28%
More than $10B	12%
I don't know / Cannot disclose	1%

About the Author

Richard Marcus, CISA, CRISC, CISM, TPECS, is Chief Information Security Officer at AuditBoard, where he is focused on product, infrastructure, and corporate IT security, as well as leading the charge on AuditBoard's own internal compliance initiatives. In this capacity, he has become an AuditBoard product power user, leveraging the platform's robust feature set to satisfy compliance, risk assessment, and audit use cases.

About the Research Partners

AUDITBOARD

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. Nearly 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.

Ascend2™
RESEARCH-BASED MARKETING

Companies partner with Ascend2 to create original research from survey conceptualization through report and content creation to media outreach. Ascend2 helps companies fuel marketing content, generate leads, and engage prospects to drive demand through the middle of the funnel. For more about Ascend, visit ascend2.com.