Digital Risk Maturity Report 2022

Turning Digital Risk Into Your Competitive Advantage

AUDITBOARD

Table of Contents

Introduction

Digital risk has become one of the fastest-growing, most pervasive risks in any organization. The 2022 World Economic Forum Global Risks Report estimates digital commerce will be worth $800 billion by 2024,[1] while a recent Gartner survey reveals that digital risk is the number one strategic business priority for corporate directors in 2022 and 2023.[2] Meanwhile, digital dependence is increasing at an accelerated pace due to technological investments made both during and after the pandemic's upheaval of the business world. As such, business leaders must be prepared for even larger investments in technology initiatives by their companies. According to a recent PwC survey of CIOs, 60% of companies are making significant investments in digital transformation technologies.[3] Deloitte also reports that the scope of digital initiatives has evolved from optimizing older processes to a complete reinvention of businesses as leaders jockey for position in a digital world.[4]

It's important to be clear about what digital risk is. Gartner defines "digital risk" as the set of risks inherent in digital products, services, and supporting processes.[5] This type of risk refers to unwanted — and often unexpected — outcomes stemming from digital transformation and the adoption of dependent or supporting technologies. Another term we will reference frequently in this report is digital transformation. Garter refers to digital transformation — or digitization —as "anything from IT modernization (for example, cloud computing), to digital optimization, to the invention of new digital business models." This process leverages next-generation technologies to gain efficiencies, align strategies or, in some cases, transform an entire business model.[6] While digital transformations are opportunities to create efficiencies, they also pose digital risks.

Gartner defines "digital risk" as the set of risks inherent in digital products, services, and supporting processes. This type of risk refers to unwanted — and often unexpected — outcomes stemming from digital transformation and the adoption of dependent or supporting technologies.

Crucially, digital risk is different from cyber risk, which Gartner defines as "the risk associated with cyber threats emanating from the external cyber environment."[7] Cybersecurity risk, third-party risk, business continuity risk, data privacy risk, and other forms of underlying risks add to the uncertainty of achieving business objectives during digital transformation.

[1] World Economic Forum, The Global Risks Report 2022.
[2] Gartner, 57% of Boards of Directors Are Increasing their Risk Appetite into 2022.
[3] PricewaterhouseCoopers, Technology Leaders Pulse Survey.
[4] Deloitte, Driving innovation and new business models through Industry 4.0.
[5] Gartner, Cyber Risk, Digital Risk, and The Digitalization of Risk Management.
[6] Gartner, Information Technology Glossary: Digital Transformation.
[7] Gartner, Cyber Risk, Digital Risk, and The Digitalization of Risk Management.

To get a sense of how digital risk is managed, AuditBoard conducted a Digital Risk Maturity survey in March 2022, which asked over 125 risk leaders how their organizations undertake risk management in this area. The survey revealed that while business leaders are aware of digital risks and are working toward comprehensive digital risk management, many organizations are still in the early stages from a maturity point of view. Key results from the survey included the following:

Digital Risk Maturity Level

- While over 90% of respondents have digital risk on their radar, only 30% of organizations are mature enough to actively mitigate those risks.
- 78% of respondents have placed ownership of digital risks with functions outside of business operations (such as IT or security), which can lead to inappropriate categorization of these risks as technical or compliance-only and create siloed risk management efforts.

Using Digital Risk Metrics

- 84% of respondents are not reporting measurable digital risk metrics to management.
- Many respondents claiming to use reportable metrics describe their activity as measuring only one component of digital risk, such as technology or fraud.

Third-Party Digital Risk

- 26% of respondents are not managing or monitoring third-party digital risk.
- Of those who are monitoring third-party digital risk, 24% are basing their assessment on internal views of third parties only.

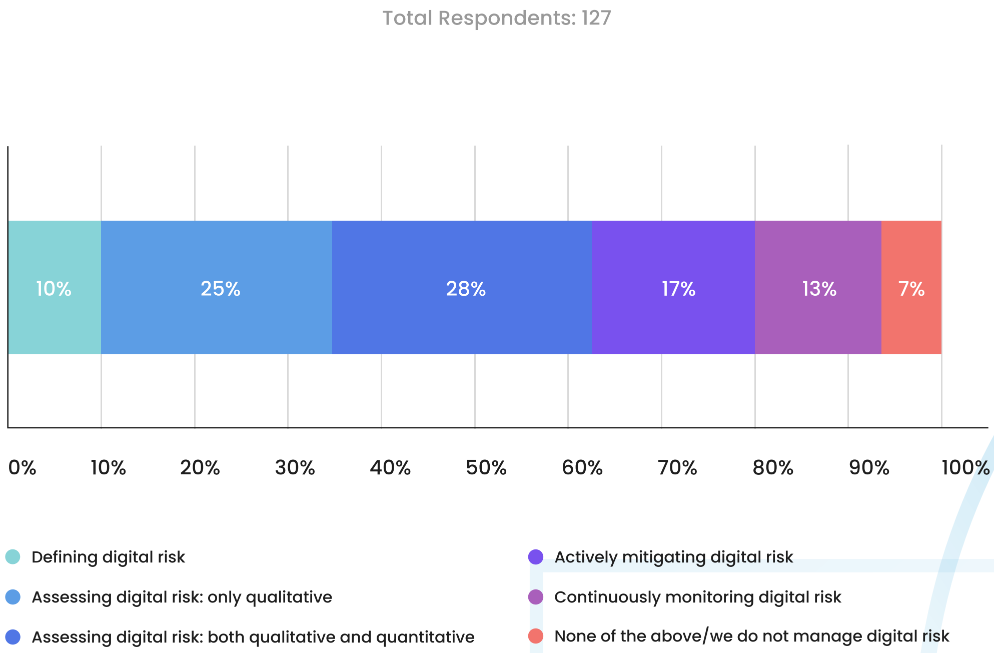
Our Digital Risk Maturity report examines the state of digital risk maturity in organizations across industries, and further explores why digital transformation itself is the key to effective integrated risk management.

Organizations Are Maturing — But Not Fast Enough

As organizations advance along the digital risk maturity spectrum, they progress from qualitative to quantitative metrics and from manual to automated approaches — allowing business leaders to measure risks more objectively rather than relying on subjective notions of control. In a mature state, leaders rely on technology to ingest data from an array of sources, including ones outside their organization, and utilize KRIs to alert them to areas requiring deeper investigation. Businesses with mature risk practices apply an integrated risk management (IRM) approach to assess, manage, and mitigate risk across the organization, third parties, and vendors. At the most advanced levels of risk maturity, an automated IRM approach supported by technology flags risks that require further investigation, and triggers a to-do action for assurance teams. This is the state of continuous risk monitoring.

AuditBoard's Digital Risk Maturity Survey asked participants to rate their organization's level of digital risk management maturity. While over 90% of respondents report digital risk on their radar at some level, only 30% are at a stage where they are actively mitigating digital risks. The majority of respondents (63%) indicated they were still in the early stages of defining and assessing their risks, and had not yet reached the point of mitigation or continuous monitoring. Considering the importance placed on getting ahead of digital risks, risk teams should aim to advance their organization's risk maturity level to keep pace with management and board expectations.

Figure 1. How would you describe your organization's digital risk mangement maturity level?

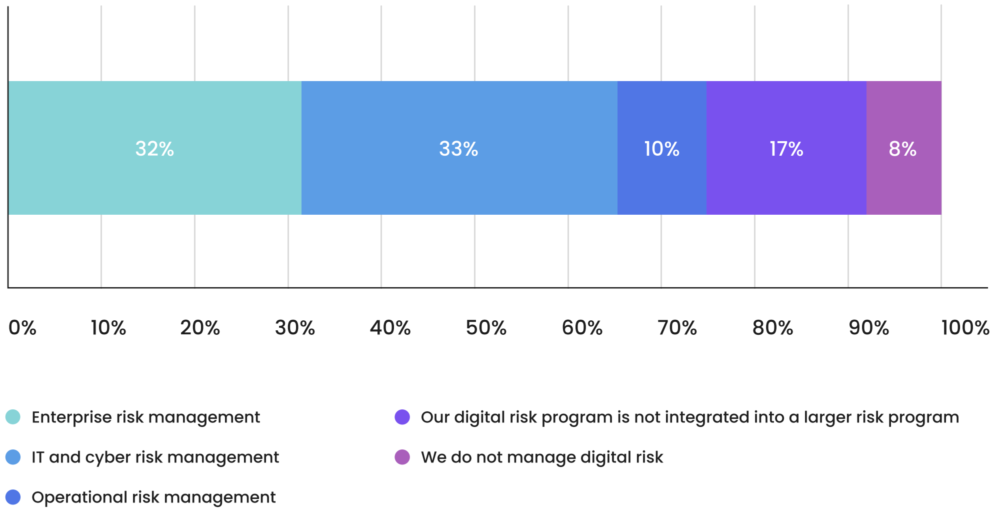


An important element of digital risk maturity is ensuring digital risk is a part of an enterprise-wide, integrated risk approach closely aligned with business operations. Gartner defines integrated risk management as “a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.” An integrated approach to risk management combats siloed risk management activities by encouraging awareness of organization-wide risks across all departments and levels. According to Gartner: “To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers, and outsourced entities.”[8]

In our survey, we asked whether digital risk was integrated within a larger risk management program. 32% of respondents reported that digital risk was integrated with their risk management program, and 10% said digital risk aligned with operational risk. In both cases, the results are positive as they show digital risks are linked to the business.

Figure 2. Is your organization’s digital risk management program integrated into a larger risk program?

Total Respondents: 127



However, Figure 2 shows that one-third (33%) of respondents stated digital risk management is integrated into their IT and cyber risk management program. These results tell us that while many organizations are aware of digital risk, they may misinterpret digital risk purely as a technical or security risk. Such an approach could lead to a siloed view of digital risk that focuses on technology risk over other business risks, when, in practice, digital risk is more closely aligned with business risks and strategic initiatives. These results illustrate why an integrated approach to risk management — versus relegating digital risk ownership to a specific corporate function — can benefit the business by affording it a more holistic and accurate view of risks to the organization.

[8] Gartner, Information Technology Glossary: Integrated Risk Management (IRM).

Digital Transformation Can Help Organizations Reach Greater Risk Maturity

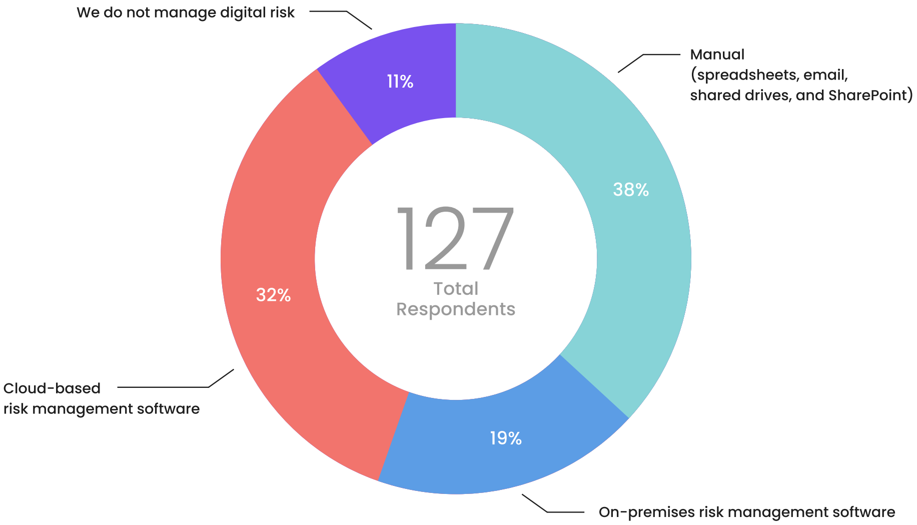
Our survey results reveal that there is hope for organizations that are seeking to improve their digital risk maturity. Digital transformation can help organizations automate and improve their digital risk management programs. Per Gartner's definition of IRM, a key element of an integrated approach to risk management is that it is supported by enabling technologies. Automating a risk management program using technology — e.g., software-as-a-service solutions, robotics process automation (RPA), and advanced analytics solutions — can create efficiencies and lead to more effective risk management practices and assurance activities.

An excellent example of a process that can be automated using technology is the risk assessment. Managing digital risk is by nature a collaborative effort that requires inputs from different teams and from multiple systems. One of the most time-consuming activities for risk teams is collecting these inputs through conducting risk assessments. Manually performing risk assessments using email, surveys, and spreadsheets requires a significant amount of time. Thankfully, this process can be automated through the use of a risk management technology solution that can gather feedback from multiple stakeholders and consume data from different systems.

As Figure 1 showed, the majority (73%) of respondents were engaged in some form of risk assessment. However, when asked if they used technology to manage their digital risk assessment activities, only half (51%) stated they did.

Ultimately, these results reveal that while some teams are leveraging enabling technology to advance risk management, a nearly equal number of risk teams today are not yet harnessing the full capabilities of the risk management technology solutions available in the marketplace.

Figure 3. What technologies are you using to manage digital risk?

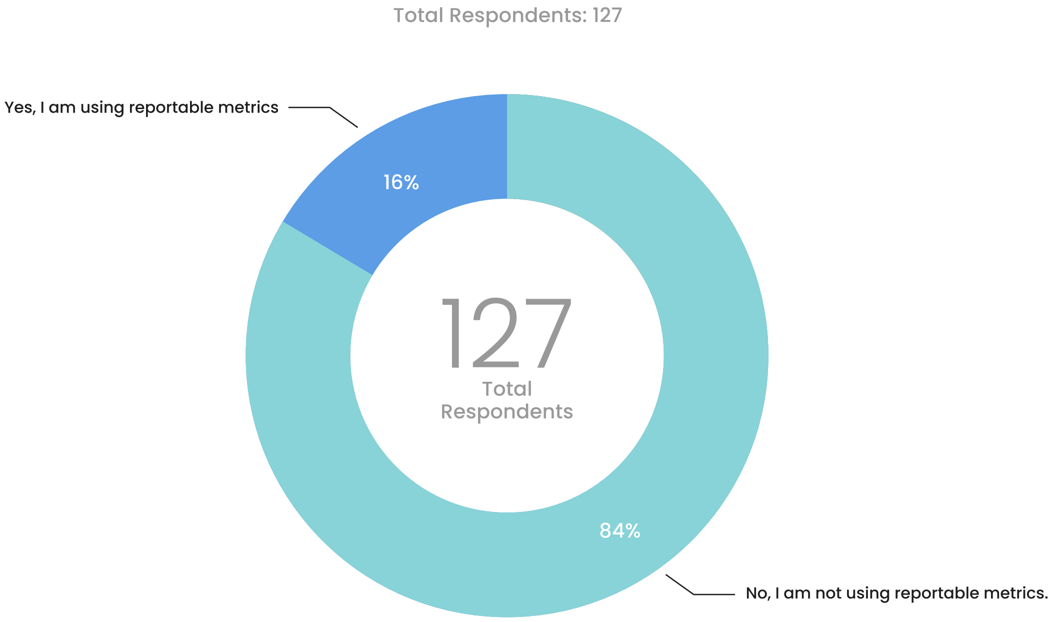


Getting Digital Risk Metrics Right: Understanding Management's Objectives

A best practice when managing digital risk is to align with management's desired outcomes for a digital transformation initiative. Is the expectation to automate a single manual process using a technology solution, or is this a much larger project involving multiple automation initiatives? Many digital transformation projects attempt to unify disparate processes within a single technology platform with the goal of integrating data for extracting business intelligence and data mining. This is why understanding management's objectives is the most critical starting point for any digital transformation. Until we know management's objectives, we cannot define the risks, measure progress, or determine success.

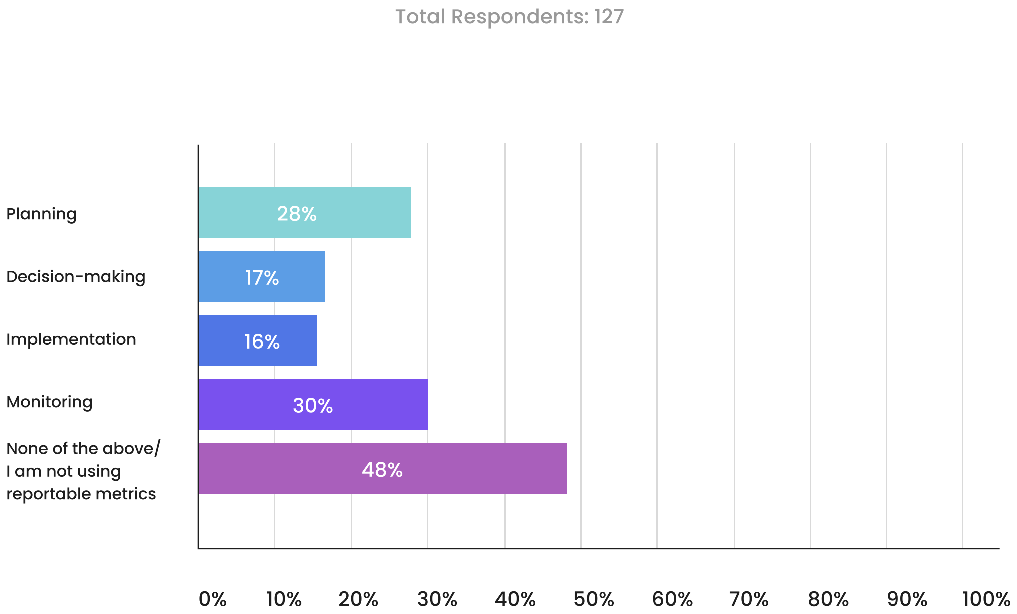
Once you understand the objectives driving the initiative, proper metrics can be developed for monitoring digital risk. In AuditBoard's Digital Risk Maturity Survey, we asked participants if they were using reportable metrics to effectively manage digital risk. The answer was overwhelmingly (84%) "No." Most organizations have not reached this level of maturity yet, a finding that is in line with our earlier observation that only 13% of respondents had attained continuous digital risk monitoring. Continuous, metric-based monitoring keeps the focus on success and maintains an open dialogue with stakeholders, a much better alternative than relying on a periodic risk assessment.

Figure 4. Are you using reportable metrics to effectively manage digital risk?



Metrics designed for continuous risk monitoring throughout all stages of digital transformation initiatives are important for successful digital risk management. Survey participants were asked at what points in the digital risk management process they used reportable metrics. The highest percentage of respondents use reportable metrics during planning (28%) and monitoring (30%). Respondents also reported using metrics during decision-making (17%) and implementation (16%), but to a lesser extent.

Figure 5. In which stages of the digital product/service development process are you utilizing reportable metrics?



As organizations move up the maturity curve, metrics should be used at every stage of digital risk management. Planning metrics measure what leaders are trying to get out of a product, service, or digital transformation effort. Metrics at the decision-making stage can flag product or service viability issues. Implementation metrics provide valuable information to leaders looking to manage competing priorities. Monitoring provides a measure of success in reaching the target set by key stakeholders. Ultimately, all of these metrics provide insight into different aspects of digital risk.

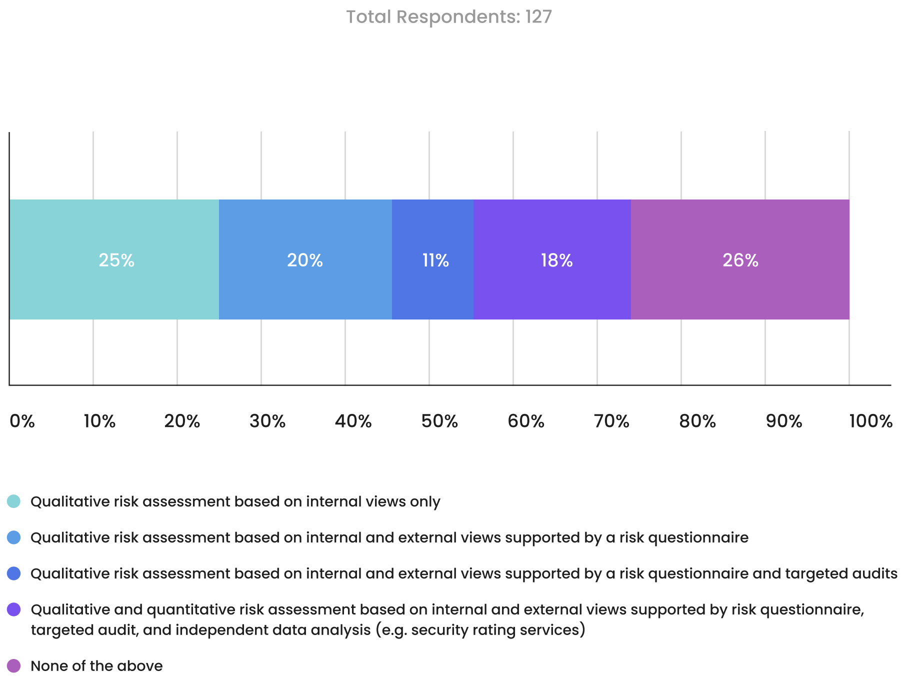
Though metrics may be important at every stage, it's also important not to lose sight of the big picture. Not every digital risk is a "key risk," and not every metric is critical. Choose risks that speak directly to the objectives that were defined at the start of the digital risk assessment process. Management will need information on these risks more than any others, and in most cases, they will need this information in real time.

Investing in Risk Management Technology Is Critical to Keep Pace With Digital Risk

Technology is a key enabler for successful digital risk assessment and ongoing monitoring. In Figure 3, we noted that over half (51%) of our Digital Risk Maturity Survey respondents said they were using some form of risk management software, yet only 32% reported using cloud-based risk management software. This is cause for concern, as over the past decade, cloud-based tools have become the preferred software for risk management due to their ability to consume data using APIs and other types of system integrations. To keep pace with the evolving risk landscape, further investment is crucial.

The role of cloud-based technology that can integrate with other systems is especially relevant when discussing third-party digital risk. When asked about this growing risk area, 26% of respondents reported that they are not managing and monitoring third-party risk. Of those who are monitoring third-party digital risk, 25% are basing their assessment on internal views of third parties only. A major factor in the ability to monitor, or even consider, third-party information is the technical capability to consume partner data with technology.

Figure 6. How are you managing and monitoring third-party digital risk?



Managing third-party digital risk can include data beyond the internal information the company has on business partnerships. The information can be gathered through external data sources (e.g., security rating services, regulatory disclosures, and news reports), interviews, questionnaires, independent reports (e.g., SOC reports), and targeted audits. Qualitative data may also include direct data feeds from third-party internal systems to your risk management software. To capture external data in your risk management software, you will likely need to work with your partners to exchange data through an API or other type of integration — demonstrating the importance of cloud-based technology, whose integration capabilities ensure the transfer of large amounts of data between systems.

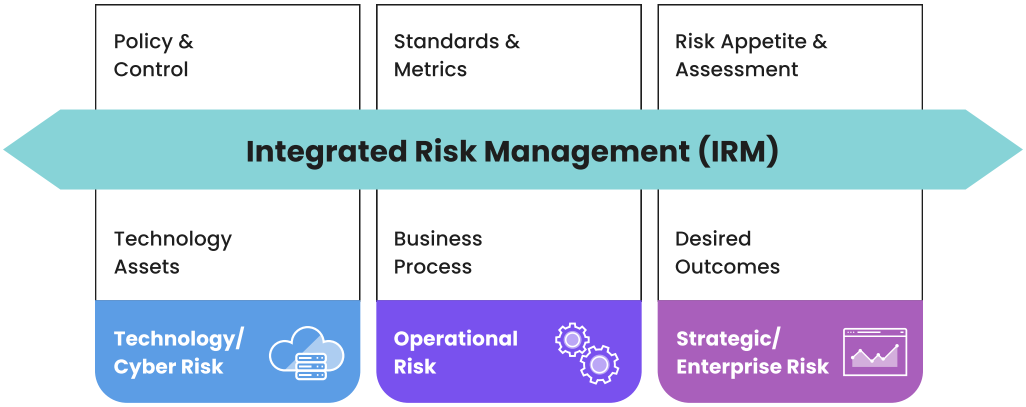
How Can Organizations Turn Digital Risk Into Their Competitive Advantage?

Technology has the power to help organizations transform digital risk into a competitive business advantage. An organization that successfully sources and implements best-in-breed technology solutions to support its integrated risk practices will wind up with strong digital risk management programs. In turn, a strong digital risk program can enable an organization to safely scale its automation initiatives — helping to create more efficiency, cost savings, and value-producing capability across business functions. This will also result in more effective and efficient technology implementations, more reliable performance, and better and timelier metrics for making decisions in a fast-changing world.

Digital transformation is an open-ended topic that spans the domains of strategy, operations, and technology. When business leaders have confidence in their digital risk management program, they are more confident in the organization's ability to address not only common digital risks such as cybersecurity, business continuity, data privacy, and third-party risk, but also emerging digital risks such as integrating RPA, machine learning, natural language processing, and smart devices connected to the network.

With so much at stake, business leaders are prioritizing digital transformation. To add value, assurance professionals should understand management's digital objectives, identify relevant digital risks, assess these risks, and provide meaningful insights to management. One challenge assurance professionals may face is misaligned priorities. In the 2022 ECIIA Risk in Focus report, the top priorities for auditors were cybersecurity and regulatory change but digital risk was not considered.[9] While cybersecurity and regulatory change represent risks that may lead to losses, they do not directly impact an organization's need to generate revenue. Yet, digital risk is linked directly to revenue generation and future growth — major priorities for any business today.

Figure 7. How can an integrated risk approach help?



Source: Wheelhouse Advisors IRM Navigator, March 2022

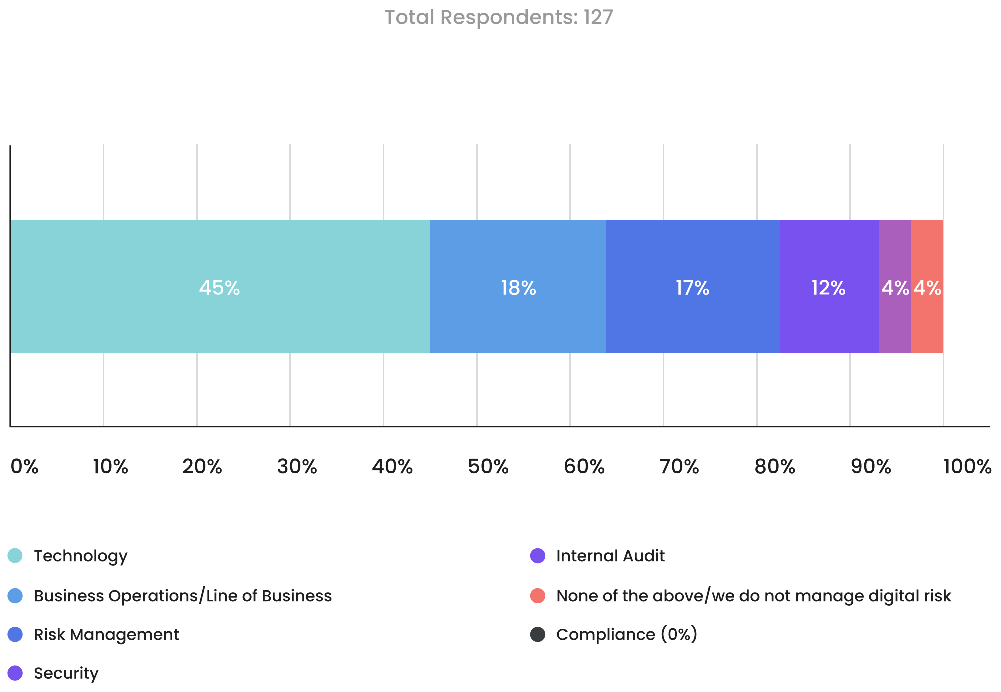
[9] ECIIA, 2022 Risk in Focus Report.

Applying an integrated risk management approach can reduce silos to provide a view across strategic, operational, and technological risks. Business leaders need better visibility and understanding of digital risk across the business landscape, including the growing ecosystem of third-party providers and vendors. Only so much information can be gleaned from SOC reports and interviews. Having real-time information from your critical partners is a major advantage in a highly integrated digital world. With increased visibility into digital risk, business leaders will have the ability to make data-driven decisions that are less reliant on subjective measures. Taken even further, the information can be used to set future plans by taking advantage of scenario analysis and predictive modeling. Attaining this level of IRM is a true competitive advantage since even risk quantification and analytics are still in a nascent state of development for many IRM solution providers.

Taking an Integrated Risk Approach Supported by Technology

A differentiator in successfully managing digital risk is involvement from key business stakeholders at all stages of progress. When asked who within the organization is responsible for managing digital risk, survey results showed 78% of respondents associated digital risk management with groups other than business operations. This can lead to siloed digital risk insights across an organization, limiting business stakeholders' ability to plan, develop, implement, and monitor digital products in service of the business's best interests.

Figure 8. Who is responsible for managing digital risk in your organization?

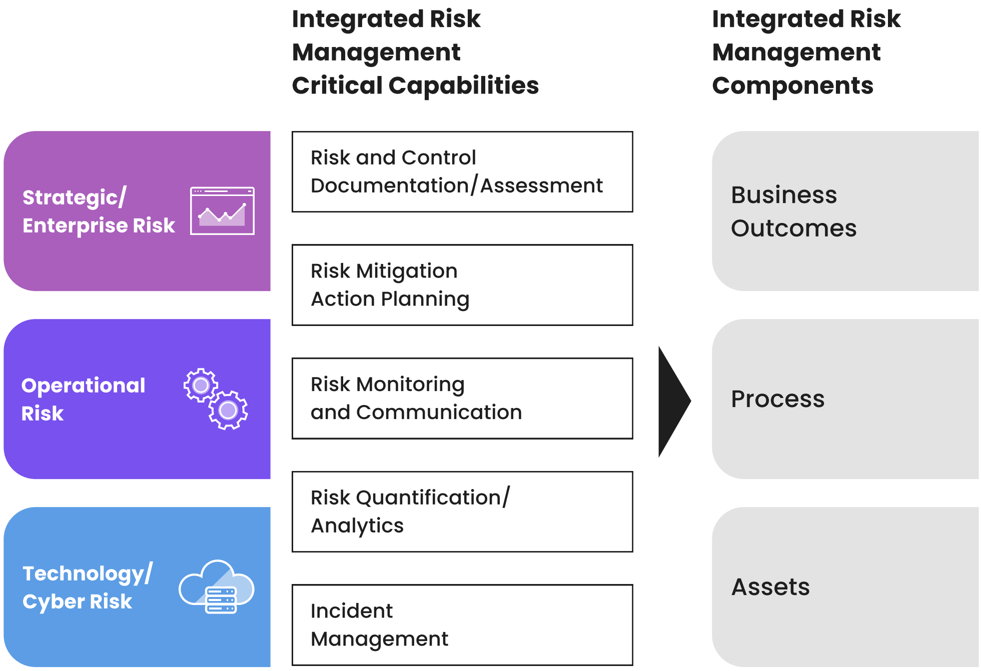


Instead, applying an approach that captures five critical IRM capabilities can provide a full view of strategic, operational, and technological risks. Those capabilities, illustrated in Figure 9, include:

- Risk assessment and control design.
- Risk mitigation through control activities.
- Risk metric monitoring and communication.
- Risk quantification and analysis.
- Issue identification and management.

By utilizing these capabilities to gain better visibility and understanding of digital risks, business leaders gain the integrated risk perspective necessary to ensure successful business outcomes. To reach this level of IRM, technology that supports all five capabilities listed above is essential.

Figure 9. IRM supports a real-time view of digital risk


Integrated Risk Management Critical Capabilities
Integrated Risk Management Components
Strategic/ Enterprise Risk
Operational Risk
Technology/ Cyber Risk
Risk and Control Documentation/Assessment
Risk Mitigation Action Planning
Risk Monitoring and Communication
Risk Quantification/ Analytics
Incident Management
Business Outcomes
Process
Assets

Source: Gartner

When digital risk is part of a comprehensive IRM program, the risks are aligned with four main objectives: achieving better performance, stronger resilience, greater assurance, and cost-effective compliance. This framework helps the company balance digital risks against other high priority emerging risks such as environmental, social, and governance (ESG) risks, talent risks, and cybersecurity. This balance comes from an enterprise-wide culture of risk awareness and a culture that understands the role of a strong control environment. Ultimately, a successful IRM program permeates the organization by connecting policies, standards, and business objectives to the associated risk assessments, metrics, and controls — all within a technology solution that enables business leaders to make the best use of data for decision-making.

Conclusion

The Digital Risk Maturity Survey results reveal that business leaders are mostly in the early stages of digital risk management, and that increasing maturity is crucial to ensure business success in a volatile risk environment. If you are in the early maturity stages, it may be beneficial to assess your current status by following these steps:

1. Define digital risk for your own organization.

2. Evaluate risk management program maturity and determine gaps.

3. Identify executive sponsors at the highest level (ideally the CEO) to drive risk management improvements.

4. Identify risk owners/business leaders and involve them in creating a framework, defining metrics, and selecting technology.

Investment in technology can pay back substantial dividends by fueling your organization's competitive advantage. The integrated risk data gathered both from within the organization and from critical business partners/suppliers drives better results. Further maturity in areas like scenario analysis and predictive modeling requires integrated risk data as well. This is where the future competitive advantages in areas beyond digital risk can be found.

About the Author

John Wheeler

Senior Advisor, Risk and Technology
AuditBoard

John A. Wheeler is the Senior Advisor, Risk and Technology, for AuditBoard, and the founder and CEO of Wheelhouse Advisors, a global risk management strategy and technology advisory firm. A former Gartner analyst, John is a recognized expert, frequent speaker, and author on the effective use of risk management practices and technology in large and midsize businesses. His major areas of specialty include enterprise/operational risk management, integrated risk management (IRM) technology, executive leadership, and corporate governance. He has 30+ years of professional experience in a variety of roles spanning executive management, finance, risk management, audit, and IT

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 30% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2 and Gartner Peer Insights, and was recently ranked for the third year in a row as one of the fastest-growing technology companies in North America by Deloitte.

To learn more, visit: AuditBoard.com.