

A man with short brown hair and glasses, wearing a white button-down shirt and a blue lanyard, is looking down at a laptop. He is standing in a server room with rows of server racks in the background. The room is dimly lit with blue ambient lighting. A large red diagonal shape is overlaid on the left side of the image.

TECHNOLOGY INDUSTRY SPOTLIGHT

Enterprise Risk Management

An Engine for Achieving Performance

IBDO[®]

Five Questions Technology Leaders Should Ask About Enterprise Risks

Technology providers today operate in a volatile risk environment that varies across an industry that includes software, hardware, media, and telecom sectors. AI adoption, cyberattacks, and geopolitical economic uncertainty are just a few of the risks that, if left unchecked, can derail operations before leaders have time to react to the initial problem. As a result, enterprise risk management (ERM) has become less about compliance and more about operational survival.

Some organizations may manage these risks in isolation — a compliance report here, a heat map there — treating risk management as a periodic exercise rather than an operating discipline. That approach is no longer sufficient. A strong ERM strategy connects risk directly to performance, giving leaders the coordinated visibility and accountability needed to protect production and make faster decisions under pressure.

The following questions and answers shed new light on ERM and how an ERM assessment can help technology organizations reduce risk and operational disruption.

What Are the Most Significant Enterprise Risks Facing Tech Organizations Today?



Artificial intelligence (AI)

AI adoption has ramped up the past few years. Technology organizations find it necessary to adapt to innovation while managing disruption to their business models.



Compliance

Regulations related to AI, cybersecurity, privacy, digital markets, and cross-border operations are complex.



Data protection

Personal data and proprietary data, including intellectual property, is vulnerable to cyber threats and data breaches.



Supply chain

No matter the cause, disruptions in the supply chain significantly affect business operations for tech organizations, particularly those focused on hardware or software.

How Have Top Risks Changed in Recent Years, and What New Risks Are Emerging?

- ▶ **AI adoption:** Traditional technology risks have become more AI-focused. AI usage has expanded to include services typically provided by some tech organizations, including software development and customer services.
- ▶ **AI governance:** Technology organizations may lack policies and protocols that govern the use of AI platforms. This potentially increases the possibility of data breaches, data leakage, and stolen intellectual property. When left without official guidance, employees may engage in shadow AI use, further increasing risk to the organization.
- ▶ **Regulations:** Tech leaders may be feeling uncertain about strategic planning due to the growing number of laws and regulations related to AI, cybersecurity, privacy, digital markets, and cross-border operations.
- ▶ **Data protection:** AI has provided new capabilities to tech organizations — and bad actors intent on accessing proprietary and personal data. A strong defense is needed, backed up by clear protocols on how to handle critical issues.
- ▶ **Third-party risk and digital ecosystems:** Whether providing SaaS and cloud services to customers or using them within their own organization, new risks will be emerging for tech leaders to manage.
- ▶ **Talent and workforce:** The rapid growth of AI and other digital innovations may have outpaced the ability to train and hire skilled workers. The corresponding risk of human error could affect the organization's ability to achieve its business goals.



Where Do Technology Organizations Most Commonly Struggle With ERM?



It's crucial to develop **formal risk management procedures** that connect ERM to business strategy.



Some organizations prepare **extensive documentation** about general risks, including disruptive innovation, but do not convert that documentation into actionable planning.



Tech leaders may find it difficult to **identify how AI could pose a risk** to their operations and business planning before problems arise.



As technology rapidly evolves, it can be difficult for tech leaders to **realize the full scope of cybersecurity risks** and then act to protect their organization from cyberattacks and data breaches.



Risk management often occurs in **silos** with the coordination and accountability that could strengthen a technology organization's response to threats.



Keeping pace with the **risks that innovation creates** is often a challenge for tech leaders.



Enterprise risk can increase when **key positions are left unfilled**, and the workforce lacks the skillset and training to handle new technologies.



How Can Tech Organizations Better Connect Risk Management to Operational Performance and Strategy?



Conduct a thorough ERM assessment to identify and prioritize risks across the organization.



Develop strong ERM then embed it into strategic business plans. Evaluate all initiatives through a risk lens and define risk appetite for innovation and AI adoption.



Stress test identified risks through simulated events, such as a malware incident, to confirm response processes and procedures hold up under real conditions.



Focus on decision making instead of reporting. Rather than defaulting to static risk inventories, use ERM to clarify strategies and assign clear accountability and decision rights.



Give key stakeholders access to both quantitative and qualitative data to help them understand how risks could affect business performance.

How Can an ERM Assessment Build Resilience and Agility?



An ERM assessment creates visibility into interconnected risks, helping enable more coordination between functions in the organization.

By gaining a thorough understanding of potential changes or events, organizations can align ERM processes with shifting business conditions and strategic objectives.

The results from an ERM assessment can help a tech organization establish controls, create clear escalation triggers, and clarify both ownership and accountability.

Embedding risk considerations into broader business processes instead of treating ERM as a standalone function can position the organization to withstand shocks to business performance and adapt to technological innovation.

Turning Risk into a Performance Opportunity

For many organizations, the challenge is not identifying enterprise risks by translating risk documentation into integrated strategic planning. An enterprise risk assessment can shift risk management from a reactive, compliance-focused exercise to a strategic tool that supports long-term planning and performance. Organizations that make this transition are better positioned to sustain operations during disruptions and remain focused on strategic priorities rather than continuously responding to the latest crisis.

BDO's eBook, **Enterprise Risk Management: An Engine for Achieving Performance**, explores how technology organizations are replacing static heat maps and siloed risk efforts with an integrated ERM strategy that strengthens resilience, improves accountability, and supports better decision-making across the enterprise. BDO's [ERM services](#) offer tailored risk management strategies designed to help technology leaders protect their organizations and achieve their performance goals, with a cross-functional approach spanning protection, innovation, and operations.

Explore the **Enterprise Risk Management: An Engine for Achieving Performance** ebook ►





Contact BDO today to learn more about
our **Enterprise Risk Management services**
and how we can help your organization
build resilience for the future.

Have questions or want to learn more? Contact us!

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

