2026 EDITION

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

High-Value Data, High-Stakes Decisions: CFOs Drive Growth and Risk Strategies

By Christopher Wright
Managing Director, Global CFO Solutions and Business Performance Improvement Leader

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organizations balancing risk management with a strong focus on seeking growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity.

Our 14th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,540 board members and C-suite executives around the world regarding their views on:

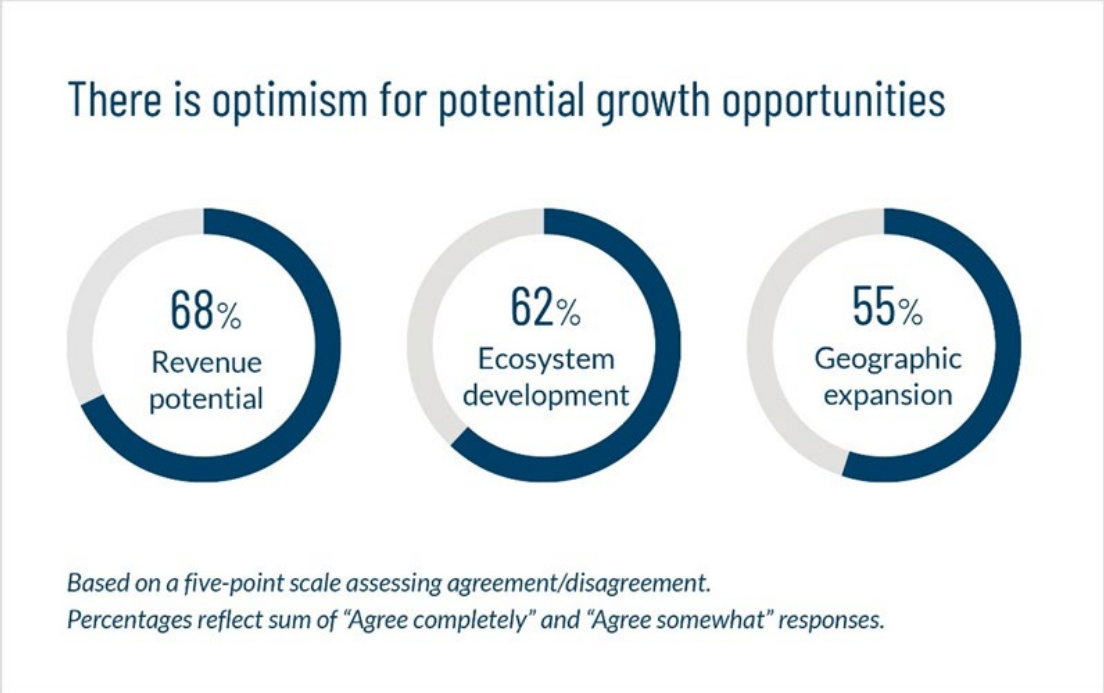
- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organizations;
- The top risks on the horizon for the near-term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long-term (a decade from now) related to 12 risk themes that consider the strategic and operational near-term risks; and
- A discussion of their organizations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. This paper offers specific insights into these issues from the perspective of the Chief Financial Officer (CFO).

Where do CFOs see the greatest opportunities for their organization over the next two to three years?

CFOs' interests in driving organizational growth have added substantially to their traditional "scorekeeping" duties. Finance leaders are increasingly regarded as the organization's purveyor of data – financial data *and* business data. These data-driven insights, which reflect both the "C" and the "FO" in the finance chief's title, enable the enterprise to pursue revenue growth, geographic expansion and ecosystem development. The latter activity involves strategic alliances and partnerships, including those designed to accelerate artificial intelligence (AI) deployments – both market-facing and internal use - and to enter new markets and geographies.

Strategic alliances and partnerships demand deep and nuanced CFO expertise. The complexity of the CFO's involvement in ecosystem development varies according to the nature of the alliance or partnership. Preferred supplier agreements can be relatively straightforward, while intricate joint ventures require sophisticated financial, accounting and economic considerations. CFOs must address the financial terms of an agreement while addressing creditworthiness, funding sufficiency, delivery capabilities, cash flow mechanics and timing, and accounting treatments. In certain countries and with certain partners, sanctions risks, intellectual property (IP) protections and technology integrations require deep consideration.



Relationships with all third parties must be subjected to an appropriate level of due diligence and ongoing monitoring across multiple dimensions – cyber security, data privacy, financial health and more – commensurate with the magnitude of risk each vendor or partner poses to the company.

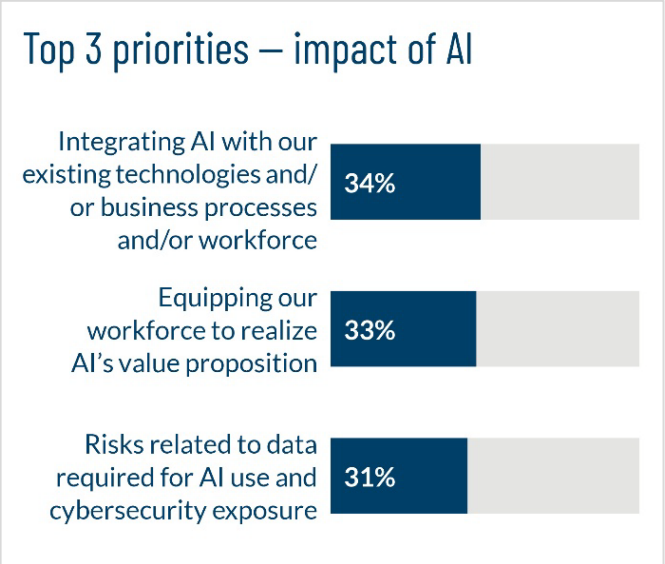
While finance groups cannot afford to get the *accounting* for ecosystem development and geographic expansion activities wrong, CFOs must also ensure that their senior colleagues and boards understand the *economics* and *financing* of these arrangements. Fulfilling this mandate requires real-time data systems that prevent the organization from falling behind the curve on emerging threats and opportunities.

What will be the organization's most significant challenges regarding the impact of AI over the next two to three years?

AI is reshaping competitive dynamics and operational risk, as the Center for Audit Quality's analysis of recent SEC Form 10-Ks for S&P 500 companies illustrates: 448 S&P 500 companies – 90% – mentioned AI-related information in their 2024 10-K. This represents an increase of almost 25% from the 359 companies that report AI-related information the previous year, according to the CAQ. Additionally, 424 companies – 72% – mention AI-related information in their Risk Factor disclosures, compared to 312 mentioning AI Risk Factors in 2023.[1]

The AI-related challenges finance leaders expect to contend with in the next two-three years are by turns strategic in nature (keeping pace with competitors), value oriented (maximizing the returns on AI investments – which CFOs rate as a higher priority compared to other C-suite members), and risk focused (AI-related data privacy and cybersecurity risks) – much like the nature of the CFO's role itself.

In the past 18 months, many organizations moved quickly to deploy AI, raising difficult decisions regarding technology investments that may not deliver proven short-term returns. While AI's long-term payoffs remain a wise bet, CFOs need to help the organization strike a more immediate balance between a legitimate fear of missing out (FOMO) and getting a return on investment (ROI) from AI.



CFOs are also focusing on how AI enablement affects third-party risk management, another risk concern that CFOs rate as more pressing compared to other C-suite members. Given that the organization's AI capabilities increasingly depend on vendor ecosystems, CFOs must ensure that procurement groups, third-party risk management teams and legal teams have mechanisms in place to evaluate whether partners can perform reliably and responsibly in an AI-enabled environment.

Maximizing AI ROI also requires attention to technology modernization and talent. Human expertise is a crucial driver of AI investment returns, and CFOs should ensure their organizations prioritize and dedicate resources to training, hiring and enabling teams to use AI solutions and to collaborate with AI agents.

What are the most significant short-term (two to three years) concerns and risks on the minds for CFOs?

A scan of CFOs' short-term risk priorities shows that the magnitude of concerns about cyber threats, third-party risks, legacy IT infrastructure, emerging AI risk and technology upskilling have increased in the past 12 months. A closer look suggests that concerns about access to talent and skills figures prominently in many other risk areas, including at least half of CFOs' top short-term risks.

[1] https://www.thecaq.org/sp-500-and-ai-reporting.

Skills gaps can impede AI integration efforts and prevent cybersecurity capabilities from adapting to ever-changing attack modes. The clock is ticking on the technology modernization work many organizations must perform to pave the way for the deployment of AI and other advanced tools. Time pressure stems in large part from the dwindling supply of legacy-technology experts. IT professionals fluent in FORTRAN, COBOL and Assembly languages are leaving the workforce. Mainframe architects and experts familiar with aging Java stacks are difficult to find and hire. There also is a pressing need to train and upskill growing swaths of the workforce as AI-enablement takes root throughout most of the enterprise.

Top global near-term risks

2026 rank	Risk issue	Average*	2025 rank
1	Changes in global markets and trade policies	3.36	5
2	Cyber threats	3.30	7
3	Increases in labor costs	3.29	4
4	Third-party risks	3.12	15
5	Economic conditions, including inflationary pressures	3.11	1

* Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."

Third-party risks demand the CFO's attention for several reasons. First, third, fourth and nth parties represent a top cybersecurity risk. Recent high-profile attacks show that bad actors are targeting larger suppliers whose outages inflict maximum financial damage across their extensive customer base. Second, assessments of vendors' AI use, and the risks that usage poses to their customers, must be integrated into vendor due diligence, sourcing, onboarding and monitoring activities. The same holds for assessments of vendors' post-quantum cryptography readiness.[2] Sanctions-related risks and other geopolitical and global trade issues also must be identified and mitigated throughout the company's supply chain and vendor ecosystem. Finally, CFOs must ensure that the financial performance and cash flow- discipline of strategic suppliers are rigorously monitored.

Economic volatility, driven by inflationary pressures and evolving trade policies, compounds these concerns. Separate data from Protiviti's Global Finance Trends survey indicates that nearly three-fifths of finance leaders report material impacts from trade policy uncertainty on forecasting accuracy, reporting requirements, and profitability.

Based on these near-term risk issues, in what areas is the organization likely to invest the most over the next two to three years, and why?

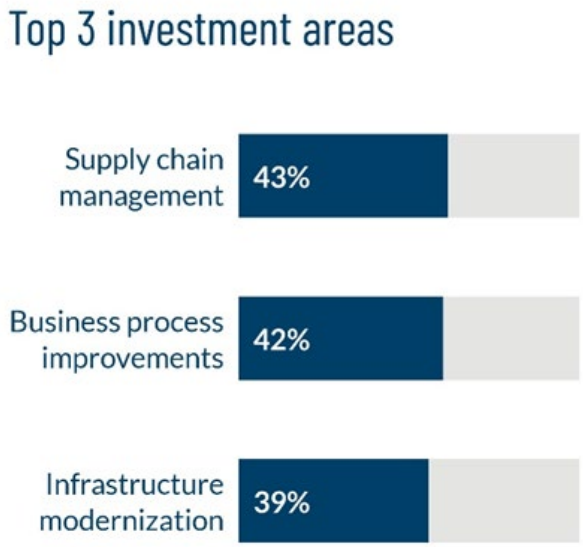
Not surprisingly, CFOs' short-term organizational investment priorities closely align with their two-to-three-year risk concerns.

Data privacy and cybersecurity investments loom large. CFOs must make sure that these allocations reflect the organization's cybersecurity priorities, cyberattack likelihoods (along with the magnitude of

[2] https://www.protiviti.com/us-en/post-quantum-world-podcast-series.

potential damage), and organizational risk appetite. No board member wants to hear that the company is spending $1 million to guard against a $50,000 risk. By translating cyber risks into financial terms, financial leaders can more effectively prioritize investments. Leveraging risk quantification methodologies supports organizational efforts to reduce cybersecurity insurance premiums.

CFOs are also strengthening the alignment between their finance group and information security teams to help reduce budget inefficiencies. The finance group's evaluation of cybersecurity ROI – measured via reductions in incidents, compliance improvements and operational resilience indicators – can help eliminate duplicate spending on redundant tools while leading to stronger, more straightforward security architecture.



Similar quantification expertise and ROI discipline helps right-size investments in third-party risk management and supply-chain risk management, where tariffs and other global trade challenges are difficult to navigate. Sanctions affect sourcing activities and can pose cash flow and credit collection risks from a supply chain management perspective while increasing the cost of goods sold (COGS) – knock-on effects requiring the CFO's involvement.

This explains the CFO's emphasis on investments in regulatory compliance infrastructure. Sweeping regulatory requirements such as the General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) demand comprehensive, people, process and technology responses.[3] Compliance infrastructure also needs to support tariff rules, payments and related trading restrictions, which are legal obligations. Non-adherence to this complex and rapidly evolving tangle of trade policy rules can result in potentially severe penalties and give rise to supply chain disruptions, along with financial and reputational risks.

How do CFOs view the 10-year risk outlook for their organization?

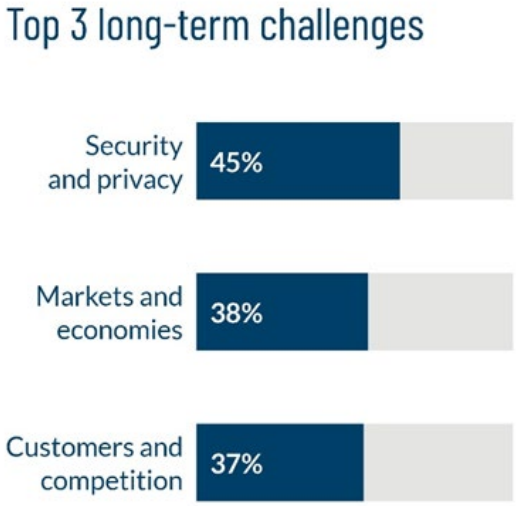
When CFOs assess their long-term concerns, the risks they emphasize relate to strategic matters. While security and privacy will remain urgent 10 years from now, CFOs also expect to invest more time and expertise on markets and economies, customers and competition, AI deployments, and sustainability in 2036.

This focus suggests that finance leaders will cement their role as the organization's purveyor of high-value data. Where this data may have been solely financially focused and backward-looking a decade ago, it has become increasingly more business-focused and forward-looking in recent years, especially since the global pandemic.

[3] https://www.protiviti.com/us-en/whitepaper/dora-compliance-untangling-key-hurdles-implementation.

The “FO” portion of the CFO’s role will also be increasingly important and valuable. In tandem with the CEO, finance leaders have a mandate to keep the organizational laser-focused on ROI. *What’s the return on our cybersecurity spend? If we invest $1 million in an agentic AI solution, will it yield a 20% productivity improvement or closer to 10%? How can AI generate new revenue streams, accelerate time-to-insight, sharpen forecasting accuracy, increase value-added work, enhance the customer experience, reduce our cost of risk, or strengthen our talent management capability?*

CFOs also rate talent challenges as a top long-term concern, upping the ante on current workforce rightsizing and upskilling decisions and their future ripple effects.



As finance leaders expand their focus on operational and strategic issues, they must source, analyze and share high-quality, judiciously curated and increasingly real-time business data that places the finance group in the thick of moving the company forward.

Guidance/call to action for next two to three years

As CFOs extend their operational reach, CFOs can perform the following actions to simultaneously address their risk concerns and the organization's strategic growth objectives:

- Focus on ROI and financial accountability- for tech modernization, AI investments, M&A and other growth drivers
- Quantify, convey and address the high costs of legacy IT environments and systems, including higher operational costs, process inefficiencies, forecasting degradation, talent attraction and retention challenges, falling behind in AI deployment, and loss of competitive advantages and shareholder value.
- Advocate for treating data governance and management as a mission-critical component of technology enablement and modernization.
- Develop a clear board-reporting framework that translates cyber risks into financial- and business-impact metrics.
- Implement a risk-quantification methodology that ties cybersecurity investments to reduced risk (translated into dollars) while seeking opportunities to consolidate security tools for cost efficiency, simplified support and improved usability
- Align AI goals with business strategy and invest in scalable AI infrastructure and technologies. A strong technical foundation includes resilient data pipelines, cloud platforms and integration tools that enable AI agents to operate efficiently.
- Treat human expertise as an indispensable driver of higher returns on AI investments.
- Prioritize and dedicate resources to training, hiring and enabling teams to effectively use and collaborate with AI solutions.
- Invest in regulatory compliance infrastructure improvements given an increasingly fragmented, complex and volatile global regulatory landscape and its impacts on financial cybersecurity, sustainability and human capital reporting requirements.
- Map exposures to tariffs, sanctions and related trade restrictions across the product and service portfolio, and across supply chains, to pinpoint and address areas prone to margin pressures.
- Establish realistic timelines and investment requirements for supply chain overhauls while identifying raw material access, capital requirements, labor availability and other constraints.
- Ensure that third-party risk management capabilities address risks related to cybersecurity and data privacy, vendors' AI use, post-quantum cryptography and financial stability.

About the author

Chris Wright is a Managing Director in New York. He leads Protiviti's global CFO Solutions and Business Performance practice and serves on our global ESG steering committee.