Anticipating Risks and Seizing Opportunities

PwC's Risk Roadmap for 2026
October 2025

Beyond the Horizon: Navigating the Risk Landscape in an Everchanging Environment

Trine Vestengen Hopkins
Territory Risk Lead
Denmark

Petri Näätänen
Territory Risk Lead
Finland

Lars Erik Fjørtoft
Territory Risk Lead
Norway

Christer Johnsson
Territory Risk Lead
Sweden

In today's rapidly evolving business landscape, organizations face an array of unprecedented risks and challenges. 2025 has already proven to be an unpredictable and disruptive year with geopolitical uncertainty, economic volatility and disruptive power of technology. Our 28th Global CEO Survey highlights the great optimism that CEOs have despite turbulent times. However, CEOs were not oblivious to risks with macroeconomic volatility cited as the threat most likely to precipitate a substantial financial loss in the year ahead.

Business leaders and assurance functions must take a proactive approach to risk: take risk intelligently to power your business and build resilience to protect it.

The nature of disruption is evolving - becoming more complex, more frequent, and more severe. In this environment, resilience is no longer optional and must be embedded into the very fabric of an organization's systems, processes, and infrastructure. Building this resilience enables organizations not only to withstand unexpected shocks and maintain stakeholder trust, but also to adapt swiftly to shifts in business models, emerging technologies, and regulatory demands.

Our **2026 Nordic report** considers the following:

- **Macroeconomic trends:** Short and medium term impact scenarios for overarching geopolitical risks.
- **Regulatory horizon:** Key regulations to be considered, including new legislation and changes to existing requirements
- **Reinventing compliance:** The impact of shifting regulations on organizations and strategies to stay ahead in the regulatory landscape.
- **Hot topics:** With the backdrop of the macroeconomic trend and the regulatory horizon, seven hot topics have been identified that organizations should be prepared for and bring to the forefront of boardroom discussions: (i) Cyber Security (ii) AI, (iii) Sustainability & Internal Controls, (iv) Third Party Risk Management, (v) Supply Chain, (vi) Tax, (vii) People & Organization.

Our selected topics are not intended to be exhaustive. By focusing on these areas which are top of mind for board and executive members, we aim to provide you with a useful reference to aid you in managing your organizational risks. Should you wish to discuss any aspect further, please do not hesitate to contact us.

For more information, please visit: pwc.dk - pwc.fi - pwc.no - pwc.se

Table of contents

Macrotrends

- Geopolitical uncertainty
- Regulatory timeline
- Reinventing compliance

Geopolitical Uncertainty

Summary

Geopolitical remains heightened as we continue to live in an era of geopolitical uncertainty. The systems and structures that have helped govern the global order in recent decades are weakening and changing. Global powers, responding to this evolving environment, are competing for influence and pursuing new diplomatic, economic and security relationships. The level and pace of geopolitical shifts and shocks are unlikely to lessen in the months ahead.

For businesses, changes in the geopolitical environment impact supply chains and production, regulatory and fiscal environments, global trade and tax norms, the movement of information, and the security of workforces, facilities and technology. In the coming year, organizations will face challenges emerging from three strategic themes:

Political Realignment

01

Globalism to Regionalism

02

The Decline of Multilateralism

03

What organizations should be doing

Against the backdrop of this continued volatility, business leaders remain focused on adaptability and resilience

Adaptability

As uncertainty increases, predicting the trajectory of international events will become increasingly difficult. Businesses need effective monitoring and scenario analysis capabilities to provide early warning of emerging risks and opportunities. Agility in response is required to effectively mitigate risks.

Resilience

Given the rate of change, businesses will be unable to prepare for every geopolitical risk scenario. Organizations will need to focus on building their resilience to prepare for increased uncertainty in the coming year.

Considerations for Control functions

Auditing the management of geopolitical risks helps organizations understand their capacity to identify, assess and effectively respond to geopolitical risks across overlapping strategic, financial and operational domains. As a risk area that is still nascent in many organizations, auditors can help the organization understand the status of, and options for, the ownership, governance and practical management of geopolitically driven risks.

Geopolitical Uncertainty

Strategic Themes

Businesses will face interconnected geopolitical risk drivers. Looking ahead to the coming year, several strategic trends are shaping the operating environment for firms.

Political Realignment:

Many of the world's democracies are in transition following the "year of elections." Accompanying this shift is the growing popularity of far-right politics, increased political polarization, and a resulting rise in societal tensions. Political realignments will be experienced differently across countries. This is especially significant for businesses with an international footprint, where the political cultures of Western democracies, in particular, may be increasingly diverse. Organizations managing global workforces will need to navigate issues ranging from diversity, equity, and inclusion to immigration and regulation.

Political Transitions

2025 will be defined by political transitions as the anti-incumbent wave from the 2024 elections reshapes governments worldwide. With opposition movements gaining influence and voter frustration fuelling polarization, geopolitical uncertainty is set to rise.

The EU's (European Union) New Normal

Western Europe faces challenges from U.S. tariffs, slow economic growth, and insecurity. Finding lasting solutions to these issues will be extremely difficult.

Globalism to Regionalism:

Alongside changing approaches to multilateralism* come increasing shifts away from Western-led global diplomatic and trade relations. This is leading to greater focus on regional alliances, national security, protectionist trade barriers, and competition over control of emerging technologies. An increased emphasis on regionalism could impact global trade practices and encourage more localized business models. Securing resilient and cost-effective supply chains will become increasingly challenging as organizations navigate complex regulatory environments, rising trade barriers, and the weaponization of trade as a geopolitical tool.

Trade Reorientation: Politically motivated and national security-related trade barriers continue to reshape the global trade environment. Divergence between the West and other global regions could result in incompatible trade and market regulations across all sectors, affecting, for example, data sharing.

The Geopolitics of Technology: Competition to lead technological innovation will remain a key geopolitical driver. The focus on AI, quantum computing, and other advancements—including blockchain and digital assets—will fuel ongoing competition across all aspects of innovation, from critical minerals to data, intellectual property, and financial infrastructure. Control over tokenization, central bank digital currencies (CBDCs), and digital payment systems is increasingly linked to national security, digital sovereignty, and future economic influence.

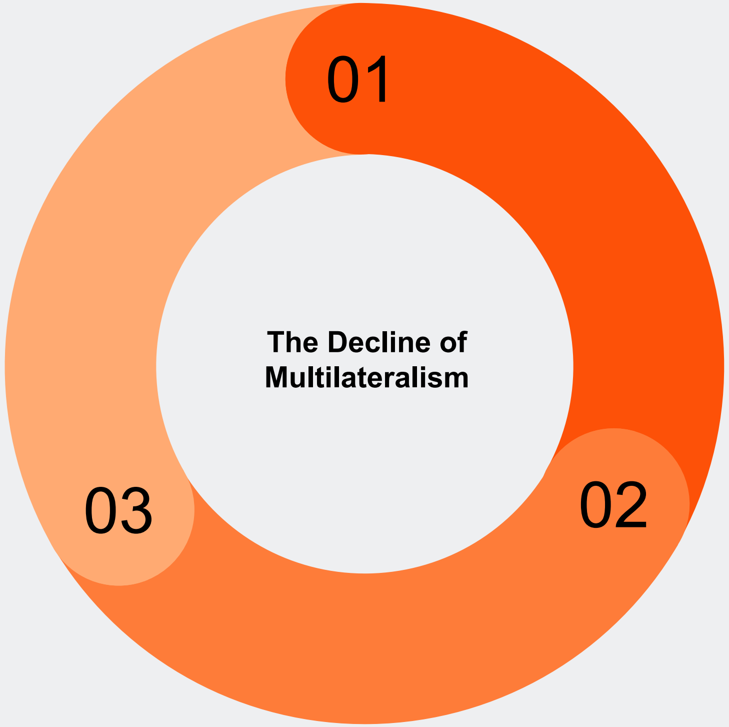
Changing International Alignments: Emerging coalitions are gaining momentum and offer small and medium powers alternatives to a Western-led order. This could have implications for global security and create new norms and opportunities in global trade.

*multilateralism - refers to an alliance of multiple countries pursuing a common goal

Geopolitical Uncertainty

International institutions and norms that have long governed state behavior are weakening, leading some states to take bolder unilateral actions with fewer consequences. As a result, conflicts as well as cyber and physical sabotage attacks continue to proliferate, and an increased sense of uncertainty and insecurity is driving defense spending globally.

The decline of multilateralism could lead to shifting global alliances, increased insecurity, and a disregard for international rules and conventions. Such changes can impact supply chains and production, regulatory and fiscal environments, global trade and tax norms, the free movement of information, and the security of workforces, facilities, and technology.



The Decline of Multilateralism

01 **Europe-Russia Relations**

Russian influence campaigns and "gray zone" attacks, such as cyberattacks, sabotage, assassination attempts on defense industry executives, and attacks on undersea infrastructure, are likely to continue. These actions could undermine EU and NATO unity, complicate the operating environment, and increase direct security threats.

02 **Shifting Approaches to Defence**

An uncertain security environment, combined with U.S. pressure on its allies to contribute more, will likely affect approaches to defense spending. This could lead to action-reaction cycles, creating opportunities for related industries but reducing government funding allocations.

03 **Conflict Proliferation**

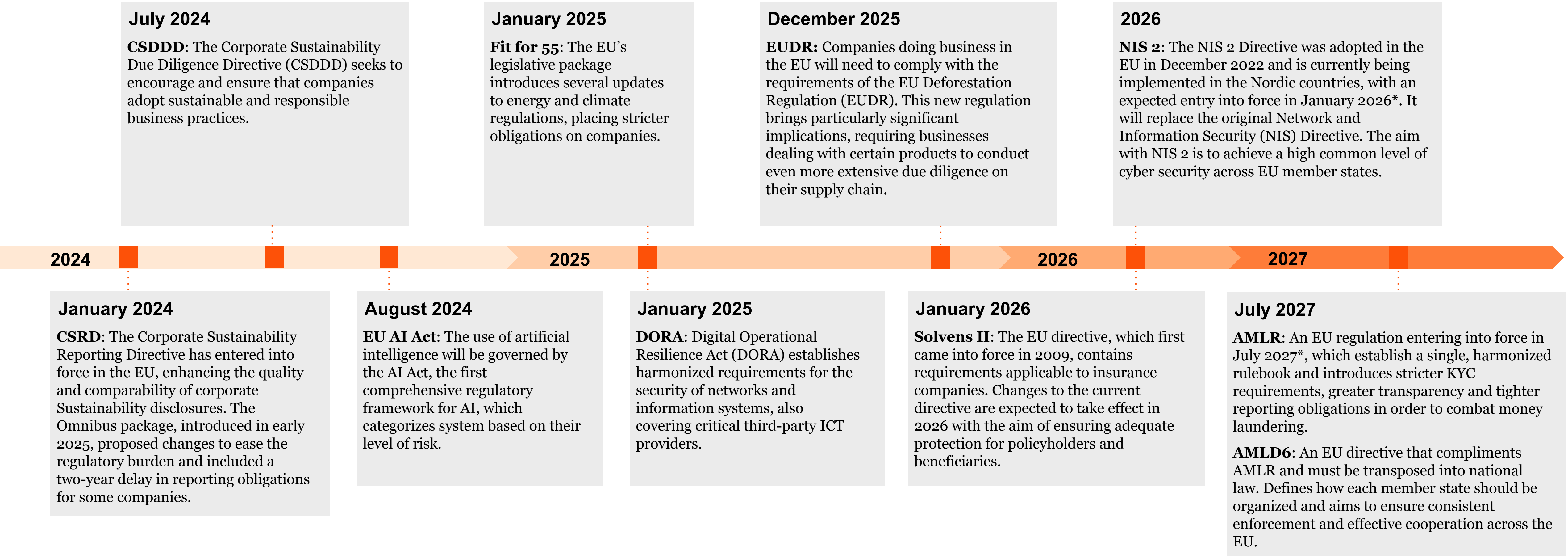
As international norms break down and the strength of international institutions weakens, the risk of interstate conflict grows. Even limited conflict events can impact security, operations, markets, and supply chains, especially if organizations face multiple crises simultaneously.

*multilateralism - refers to an alliance of multiple countries pursuing a common goal

CC
C
C

Regulatory timeline

Below is a visual timeline of key existing and upcoming regulatory changes for 2024 - 2027, to be considered as business leaders and assurance functions navigate risks, seize opportunities and deliver stakeholder value by 2026.



January 2024

CSRD: The Corporate Sustainability Reporting Directive has entered into force in the EU, enhancing the quality and comparability of corporate Sustainability disclosures. The Omnibus package, introduced in early 2025, proposed changes to ease the regulatory burden and included a two-year delay in reporting obligations for some companies.

July 2024

CSDDD: The Corporate Sustainability Due Diligence Directive (CSDDD) seeks to encourage and ensure that companies adopt sustainable and responsible business practices.

August 2024

EU AI Act: The use of artificial intelligence will be governed by the AI Act, the first comprehensive regulatory framework for AI, which categorizes system based on their level of risk.

January 2025

Fit for 55: The EU's legislative package introduces several updates to energy and climate regulations, placing stricter obligations on companies.

January 2025

DORA: Digital Operational Resilience Act (DORA) establishes harmonized requirements for the security of networks and information systems, also covering critical third-party ICT providers.

December 2025

EUDR: Companies doing business in the EU will need to comply with the requirements of the EU Deforestation Regulation (EUDR). This new regulation brings particularly significant implications, requiring businesses dealing with certain products to conduct even more extensive due diligence on their supply chain.

January 2026

Solvens II: The EU directive, which first came into force in 2009, contains requirements applicable to insurance companies. Changes to the current directive are expected to take effect in 2026 with the aim of ensuring adequate protection for policyholders and beneficiaries.

2026

NIS 2: The NIS 2 Directive was adopted in the EU in December 2022 and is currently being implemented in the Nordic countries, with an expected entry into force in January 2026*. It will replace the original Network and Information Security (NIS) Directive. The aim with NIS 2 is to achieve a high common level of cyber security across EU member states.

July 2027

AMLR: An EU regulation entering into force in July 2027*, which establish a single, harmonized rulebook and introduces stricter KYC requirements, greater transparency and tighter reporting obligations in order to combat money laundering.

AMLD6: An EU directive that compliments AMLR and must be transposed into national law. Defines how each member state should be organized and aims to ensure consistent enforcement and effective cooperation across the EU.

* at the time of publication of this report

Reinventing compliance

Navigating Compliance in an Era of Transformation

Compliance today is more complex than ever. Rapid transformation, new business models, and shifting expectations are reshaping the regulatory landscape, and organizations are under increasing pressure to adapt. Many are investing heavily in technology to strengthen compliance capabilities, but the real differentiator lies in how effectively businesses harness AI and data to anticipate and manage risk.

Over the past three years, regulatory frameworks have become significantly more intricate. While regulation is essential for maintaining a fair and transparent business environment, it also remains one of the greatest barriers to innovation and business model transformation. For many companies, compliance complexity has become a key constraint on value creation.

Against this backdrop, certain priorities stand out. Cybersecurity, data protection, and data integrity consistently top the compliance agenda, closely followed by corporate governance. To succeed, organizations need more than just compliance processes — they need a clear strategy, decisive leadership, and the courage to rethink traditional approaches. The ability to identify risks early, understand them in context, and act quickly is now a competitive advantage.

Reinventing compliance

Source: PwC Global Compliance Survey 2025

Compliance as a driver of growth

Forward-looking organizations are already reimagining compliance in bold ways. We see a range of strategies, from incremental improvements to enterprise-wide transformation. Common moves include:

- Centralizing and coordinating compliance activities
- Using AI to automate processes and unlock new insights
- Harnessing data to spot risks and support smarter decisions
- Embedding compliance early in product development

Earlier involvement of Compliance is one way companies are unlocking the value it can provide, positioning them as an advisor to the business to help identify risks and avoid issues sooner. This may be beneficial for companies with significant research and development (R&D) activities, where competition is increasing pressure to speed up development and bring new products and services to market faster. In the pharmaceutical sector, for example, the pandemic forced companies to find new approaches to drug development and clinical trials, including how virtual patient data is used. This spurred innovation around how traditional processes can be digitised and automated to move quicker, increase quality, and use data differently, including reporting to stakeholders and regulators.

At the same time, many companies are breaking down silos to foster stronger compliance cultures. With rising data volumes, increasing costs, and growing regulatory complexity, integrating technology into operating models is no longer optional, it's essential. And the results speak for themselves: improved visibility into risks (64%), faster issue detection and response (53%), more insightful reporting (48%), quicker and safer decision-making (46%), and measurable gains in productivity and efficiency (43%). Each of these outcomes positions compliance not as a burden, but as a driver of agility, resilience, and long-term value.

But there is one constant challenge: data. The effectiveness of even the most advanced compliance technology depends on accurate, consistent, and well-governed information. Without it, the system falters. With it, compliance becomes a true enabler of growth.

Reinventing compliance

> "Navigating the new compliance landscape means understanding how fast your company can move, including how quickly it can see and understand emerging risks, access reliable data at the right time, adopt new processes and technology, and train those responsible for compliance. Go too slow and risk being overtaken; move too fast without the right capabilities, and risk missing the gaps and tripping over new requirements. This requires a clear compliance strategy and plan – and the right strategic compliance leadership to drive it."

Shaun Willcocks
PwC Global Risk Markets Leader & Global Internal Audit Leader

Winning through compliance innovation

Ultimately, compliance is more than a regulatory requirement, it is a strategic asset. It shapes organizational culture, builds trust with stakeholders, and strengthens resilience in a volatile environment. As regulation and technology continue to evolve, the most successful companies will be those that embrace compliance not just as an obligation, but as an opportunity to lead with confidence and move faster in the market.

The level of regulatory change, shifting stakeholder expectations, and changes in industry ecosystems and macro risks, means that responding in a 'traditional way' - more people, more controls - is unlikely to be sustainable. New problems call for new thinking. This requires 'compliance by design' that brings together new technology, talent, and a strategic mindset to connect-the-dots across functions and build the data flows into the DNA of the organisation.

Done well, such a design can enable companies to 'see around corners' to predict threats and empower the business with confidence to navigate the compliance risk landscape faster, avoid hazards, and maintain trust. This is the only way that companies can stay ahead of the regulatory changes and issues that will continue to disrupt the market - and win the race.

Hot topics

- Cyber Security
- AI
- Sustainability & Internal Controls
- Third Party Risk Management
- Supply Chain
- Tax
- People & Organization

Cybersecurity

Enabling Digital Trust through smarter Cyber Risk Management

Geopolitical upheavals, increased regulation, the exponential rise of AI use and the ubiquitous plague of cybercrime on businesses have dominated the cyber landscape of the past 12 months. The security focus, in the face of the inevitability of some form of compromise, has moved towards resilience and swift recovery from cyber attacks, rather than creating an impenetrable digital fortress. The increased compliance burden leveraged on organisations from regulators and government entities is partially in response to the perception that businesses are not doing enough to secure themselves, and their supply chains, in the face of proliferating cyber threats.

However, the question of how much to invest in security in organizations - how much cybersecurity is enough? - remains a difficult one for many CISOs, CIOs and Boards to answer, given the ever-shifting nature of the risks they are facing. Indeed, compliance alone is not sufficient to ensure security in 2025. Many organizations are finding, more than ever before, that effective risk management is critical to making the right investment decisions, growing with confidence, innovating safely, and enabling digital trust across their entire cyber ecosystems.

Cybersecurity

Risk drivers

PwC conducts extensive research on over 400 cyber threat actors across 27 countries on an ongoing basis as part of its threat detection and monitoring service. It also supports PwC incident response teams in 46 countries, detects threats on PwC's own network spanning 154 countries worldwide, and monitors the Deep and Dark Web for data leakage and credential theft on behalf of a wide range of customers. Through this comprehensive visibility into the cyber threat landscape, the following trends have been identified.

- Exploitation of zero-day and n-day vulnerabilities, especially in edge devices like VPNs, is at record levels. Weak security in much software makes this a highly effective tactic for both criminal and state-sponsored actors. The reality is that security in much of this software is suboptimal, making it easy for threat actors to find weaknesses.
- Geopolitical conflicts (Russia-Ukraine, Middle East) have driven destructive malware campaigns and patriotic DDoS attacks against organizations linked to opposing sides.
- State-sponsored actors are becoming more sophisticated in their use of proxy infrastructure to conceal their identity and activities when carrying out espionage and intellectual property theft. They are also outsourcing some of this activity to commercial companies to increase the scale and reach of their operations.
- Large volumes of misinformation and disinformation were deployed during many of the elections throughout 2024, aiming to influence and interfere with democratic outcomes.
- Cybercrime, particularly ransomware and Business Email Compromise (BEC), has surged to new levels. It is clear that law enforcement interventions, such as those targeting the Lockbit ransomware group, have only limited and temporary effects on a highly resilient ecosystem that continues to generate record profits from victims. As more organizations migrate to the cloud, criminals are increasingly focused on stealing legitimate credentials to gain network access—identity has become the new frontline in high-profile cyber compromises.

Red flags

The indicators below are warning signs for organizations to reassess their approach to managing cybersecurity risks.

Trust & Access: Insufficient Privileged Access Management (PAM), Multi-Factor Authentication (MFA), and Role-Based Access Controls (RBAC) to protect user accounts and production systems from remote compromise by malicious actors raise significant red flags. Without these essential safeguards, the integrity and confidentiality of sensitive information and business operations could be severely at risk. With criminals increasingly using voice and SMS phishing (vishing and smishing), in addition to traditional email phishing, phishing-resistant MFA, hardened IT help desk processes, and risk-based authentication are now critical.

Neglecting Security Measures During AI Implementation: Organizations integrating AI tools should prioritize the simultaneous implementation of robust security measures to protect AI systems and associated data as "critical assets." While AI can significantly enhance cyber defense and overall productivity, it can also expose organizations to vulnerabilities if comprehensive policies to safeguard these assets and their use are not in place.

Unprotected and Unprepared: Gaps in Cybersecurity Resilience: Failure to test business continuity and disaster recovery plans, engage a Digital Forensics and Incident Response (DFIR) provider, and secure cybersecurity insurance leaves organizations unprepared to respond to and recover from serious cyberattacks, such as ransomware.

Failure to Apply a Framework for Control & Compliance: The absence of a structured cybersecurity approach, such as adherence to frameworks like ISO 27001 or the NIST Cybersecurity Framework (CSF), and lack of awareness of relevant cybersecurity regulations and laws, including NIS 2 and DORA, raise concerns about an organization's ability to effectively manage risks, maintain compliance, and protect sensitive information and its supply chain.

Cybersecurity

Critical Questions

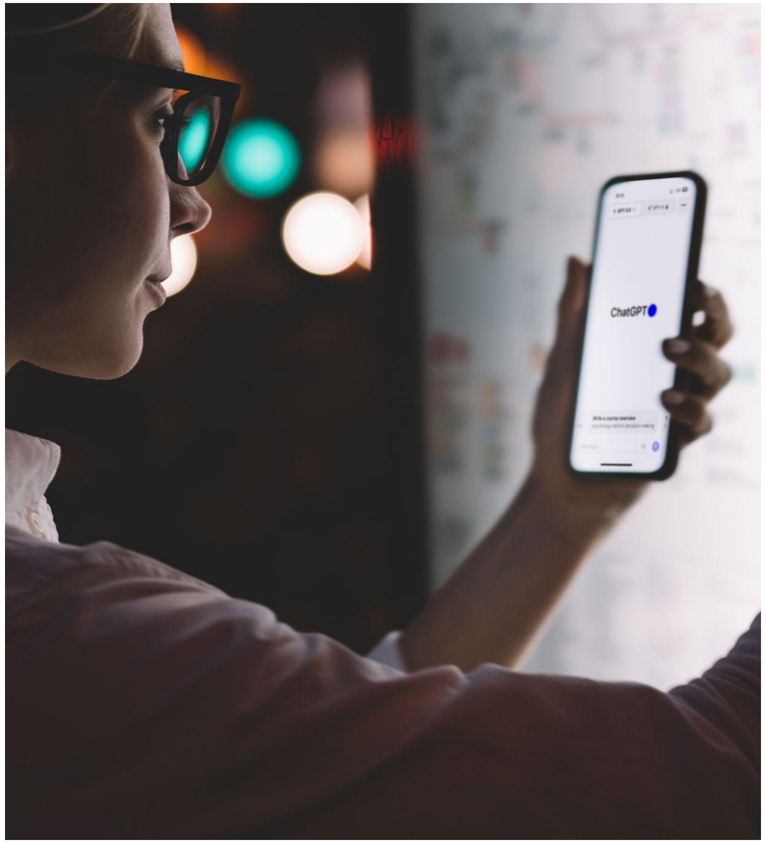
Cybersecurity is, more than ever, a board-level risk that must be managed holistically alongside other risks such as finance, safety, and sustainability. An organization's critical data and functions are cyber-dependent and need to be protected commensurate with the risk of their loss, damage, or unavailability, whether for short or extended periods.

As with all other risks, the organization needs a strategy to manage cybersecurity, a senior leader accountable for it, protections in place to prevent those risks from materializing, and a plan to mitigate or recover from them if they do. The connectivity of an organization to other entities through its supply chain also represents a significant risk.

However, even the most serious cyber risks are manageable through sound and proportionate security investments.

Consider these critical questions to your organization:

- Do you understand how your IT systems relate to your ability to deliver your business, and which systems are most critical to protect?
- Is your cybersecurity team working toward a cybersecurity standard such as ISO 27001 or NIST 2.0 Cybersecurity Framework (CSF) to ensure you meet minimum cybersecurity requirements?
- Do you have a plan in place to mitigate the risks of sharing your data, applications and systems with your suppliers?
- What measures does your business have in place to minimize the damage a hacker could do once inside your network?
- Do you have an incident response and disaster recovery plan that you regularly test to ensure you can recover from a serious cyber incident?
- Does your organization appropriately protect AI model user and system accounts, and monitor for unauthorized access and data exfiltration from AI systems?



Cybersecurity

> Don’t stop short on your journey for cybersecurity and resilience. Criminals and nation-state actors are becoming expert at finding unprotected seams: weak identity and access controls, unpatched devices and security misconfigurations.”
>
> **Rob Joyce**
> Cyber, Risk & Regulatory Senior Fellow, PwC US, former Special Assistant to the President & Acting Homeland Security Advisor

Business Insights

Cybersecurity is navigating uncharted territory amid a rapidly shifting geopolitical landscape and unprecedented technological breakthroughs that are expanding attack surfaces and introducing new threats. In this volatile environment, 60% of business and technology leaders rank cyber risk investment among their top three strategic priorities, highlighting its critical role in managing ongoing uncertainty.

However, resilience remains a challenge: only 6% of organizations feel confident in their ability to address all cyber vulnerabilities, while about half consider themselves only somewhat capable of withstanding targeted attacks. Despite this, just 24% invest significantly more in proactive cyber measures, such as monitoring, testing, and controls than in reactive responses like incident recovery and fines. Most organizations (67%) evenly split their budgets between the two, a costly approach given that reactive spending often understates the full impact of cyber incidents, including reputational damage and lost opportunities.

AI is at the forefront of the cyber defense transformation, with organizations prioritizing agentic AI deployment for cloud security, data protection, and operational defense over the next 12 months. To address persistent talent shortages, 53% are turning to AI and machine learning tools to close skill gaps, while many are also adopting specialized managed security services to rapidly scale expertise and modernize critical systems.

In this new era marked by fractured alliances, trade tensions, and supply chain disruptions, cybersecurity has evolved from a technical necessity into a strategic imperative. Organizations that invest proactively and embrace AI-driven innovation will be best positioned to withstand the increasingly complex and dynamic cyber threat landscape.

Source: 2026 Global Digital Trust Insights Survey

AI

Harnessing AI’s potential while managing its risks

Unlocking economic value and addressing the challenges of an AI-driven future. The AI landscape is evolving rapidly, driven by advancements in generative AI (GenAI). Large Language Models (LLMs) and AI agents are transforming everyday applications and delivering measurable business value.

The impact is already visible: 56% of CEOs report that GenAI has improved employee efficiency, while 34% have seen profitability gains, according to PwC’s 2025 CEO Survey. However, only 18% of Norwegian CEOs report profitability gains from AI.

PwC research shows AI could boost global economic output by up to 15% over the next decade. However, realizing this potential requires more than just technical success, responsible deployment and sound governance are prerequisites to build the necessary trust in these solutions.

Early adopters are gaining competitive advantages, leaving others at risk of falling behind, potentially leading to a scenario where only a few companies dominate the AI-driven economy. To stay competitive, organizations must embed AI into their strategies, balancing innovation with robust risk management.

Source: PwC research “Value in motion”

AI

Risk drivers

The rapid evolution of AI brings several risks that organizations must address to remain resilient. Some of the most prevalent include:

- Cybersecurity: AI systems are prime targets for cyberattacks, with generative AI expanding the attack surface. However, the same technology can also enhance cyber defenses, creating a dual challenge.
- Misinformation: The rise of deepfakes and AI-generated content amplifies misinformation risks, especially in politically sensitive contexts such as elections. Over half of businesses express concern about this issue.
- Trust Issues: According to PwC's annual global CEO Survey, only 33% of CEOs trust AI in key processes, citing concerns over bias, transparency, and ethical considerations. These issues hinder adoption and limit AI's full potential.
- Regulatory Complexity: AI regulation remains fragmented. The EU AI Act introduces strict rules, while the U.S. lacks federal legislation, and countries like Japan and South Korea are implementing their own frameworks. This patchwork creates legal uncertainty for businesses operating across multiple jurisdictions.
- Bias and Legal Liabilities: AI can introduce biases, with one-third of businesses anticipating related challenges. Legal liabilities and reputational risks are growing concerns
- Geopolitical Tensions: The global AI race, particularly among the U.S., China, and the EU, increases risks of misuse, cyber conflicts, and supply chain vulnerabilities.

Proactively addressing these risks through governance, ethical frameworks, and cross-border collaboration is essential to harness AI's potential responsibly.

Red flags

Organizations should reassess their AI strategies if they encounter the following warning signs:

Lack of Strategy for Adoption: No clear plan for leveraging AI to achieve business objectives. Fifty percent of Norwegian CEOs report that they lack such a plan.

Weak Policies: Absence of guidelines on AI ethics, regulatory compliance, data management, and operational protocols.

Inadequate Risk Assessments: Failure to conduct comprehensive risk assessments related to AI deployments, including data privacy, security risks, and potential biases in AI models.

Poor Data Management: Insufficient protocols for data handling, leading to potential data breaches or misuse of sensitive information.

Insufficient Training and Awareness: Limited training for employees on AI risks and safe practices, indicating gaps in understanding and mitigating potential issues.

Lack of Transparency: No mechanisms to ensure transparency in AI decision-making processes, which could lead to trust issues among stakeholders.

Neglecting Ethical Considerations: Failure to address ethical implications of AI, such as fairness, accountability, and the societal impact of AI technologies.

No Incident Response Plan: Absence of a clear incident response plan for AI systems that malfunction or deviate from expected behavior.

AI

Critical Questions

To build trust and harness AI's potential, organizations must address these critical questions:

- Do you have a clear AI strategy aligned with your business objectives?
- Have you conducted a comprehensive assessment of AI-related risks and opportunities, dedicating sufficient resources to explore its benefits?
- Have you taken steps to ensure your AI systems are trustworthy, ethical, and aligned with organizational values?
- Have you assessed applicable regulatory requirements that may impact your use of AI?
- How does your organization mitigate biases in AI models to ensure fairness and equity?
- What governance structures oversee AI decision-making processes, and how are they monitored?
- How do you measure and track the performance, reliability, and impact of your AI systems?
- What contingency plans exist for AI system failures, unintended consequences, or ethical dilemmas?

Business Insights

Successful companies integrate AI into their core strategies, aligning it with digital initiatives, upskilling employees, and fostering a culture of innovation. They use AI to enhance decision-making, streamline operations, and deliver personalized customer experiences. By embedding AI into existing platforms, they ensure seamless adoption and maximize its value.

PwC's 28th Annual Global CEO Survey highlights AI's transformative potential: 56% of CEOs report that generative AI (GenAI) has already improved employee efficiency, while 34% have seen increases in profitability. Looking ahead, nearly half (49%) of CEOs expect GenAI to boost profitability in the next 12 months, underscoring its growing role in reshaping how companies create value.

To manage risks, leading companies implement robust governance frameworks that include ethical guidelines, transparency in AI processes, and regular audits to ensure compliance with evolving regulations. They invest in continuous monitoring systems to detect and mitigate biases, ensuring AI models remain fair and accurate over time. Data security and privacy are prioritized, with stringent measures in place to protect sensitive information and prevent breaches.

These companies also recognize that AI should complement human expertise. By fostering collaboration, they use AI to augment decision-making rather than fully automate complex tasks. This hybrid approach balances innovation with responsibility, ensuring long-term success and sustainability in a rapidly evolving digital landscape.

Sustainability & Internal Controls

Streamlined Sustainability: EU redefines corporate climate reporting for greater impact and efficiency

The Corporate Sustainability Reporting Directive (CSRD) took effect for large EU companies in the 2024 financial year, with reports due in 2025. It mandates detailed ESG disclosures using European Sustainability Reporting Standards (ESRS). The directive aims to improve transparency, comparability, and accountability in corporate sustainability, supporting the EU Green Deal.

The Omnibus Package for Sustainability Reporting, introduced by the European Commission in February 2025, proposes major changes to ease the regulatory burden of CSRD. Key measures include a two-year delay in reporting obligations for companies scheduled to report in 2026 and 2027, narrowing CSRD's scope to firms with over 1,000 employees, and making taxonomy reporting voluntary for companies with turnover below €450 million. It also introduces a voluntary SME standard, simplifies reporting requirements, and aims to reduce administrative complexity while maintaining the EU's sustainability goals.

The reduced compliance requirements have given companies the freedom to focus on sustainability reporting that provides value to their key stakeholders: customers, investors, partners, and other regulatory bodies. Companies are also beginning to look beyond reporting to focus on climate and circularity, nature, responsible supply chains, and responsible investments.

Sustainability & Internal Controls

Risk drivers

- **Sustainability reporting risks:** Regulatory changes, data quality issues, greenwashing, stakeholder scrutiny, and supply chain transparency can lead to reputational damage, legal penalties, and loss of investor trust. Companies must ensure accurate, consistent, and transparent disclosures to meet evolving standards and stakeholder expectations.
- **Climate and circularity risks:** Resource scarcity, carbon pricing, regulations, extreme weather, and linear business models can disrupt operations, increase costs, and create compliance risks. Transitioning to circular, low-carbon models builds resilience, enhances competitiveness, and supports profit growth, helping to mitigate these sustainability-related threats. Adopting sustainable business practices and taking climate action enables profit growth. Companies that challenge themselves to develop climate-friendly services, products, and technologies will succeed in the market. The alternative is stagnation and losing out to the competition.
- **Nature-related risks:** Biodiversity loss, land and water degradation, deforestation, and pollution threaten supply chains, increase costs, and trigger regulatory or reputational challenges. Strong risk management is crucial for long-term resilience and compliance.
- **Responsible supply chain risks:** Human rights violations, child labor, unsafe working conditions, poor traceability, and environmental harm can result in penalties, brand damage, and loss of trust. Companies must ensure ethical sourcing, transparency, and compliance across all tiers of their supply chain.
- **Responsible investment risks:** Weak ESG integration, shifting regulations, market volatility, and misconceptions about sustainability's financial impact can lead to misaligned portfolios, reputational harm, and financial losses. Strong ESG criteria are essential to navigate the evolving landscape sustainably.

Red flags

There are several red flags that indicate your organization may not be proactive enough in addressing sustainability risks. Key indicators to watch for include:

Sustainability Reporting

- Reporting that does not meet key stakeholder requirements -Many companies focus too much on regulatory compliance without identifying what is vital to their key stakeholders.
- No Third-Party Verification - If reports aren't independently audited, the data may not be reliable or trustworthy.

Climate and Circularity

- No Net-Zero Plan – Claims of climate action without a clear, time-bound net-zero roadmap are concerning.
- Linear Business Model – Heavy reliance on virgin materials or single-use products signals a low commitment to circularity and a lack of insight into how disruptive or new business models could help build additional revenue.

Nature

- No Biodiversity Data – If a company doesn't report on impacts to ecosystems or species, it may be ignoring key nature-related risks.
- Land Use Blind Spots – Lack of transparency regarding deforestation, water use, or land conversion suggests poor stewardship of natural resources.

Responsible Supply Chain

- No Supplier Transparency – When a company doesn't disclose key suppliers or sourcing regions, assessing risks becomes difficult.
- Lack of Labor Standards – Missing policies or audits on fair wages, working conditions, or human rights is a major concern.

Responsible Investment

- No ESG Integration –If environmental, social, and governance (ESG) factors aren't incorporated into investment decisions, sustainability risks may be overlooked.

Sustainability & Internal Controls

Critical Questions

To evaluate the effectiveness of sustainability risk mitigation, consider the following questions:

Sustainability reporting - How does your organization ensure accuracy and transparency in sustainability reporting to prevent accusations of greenwashing or regulatory scrutiny?

Climate and circularity - What steps are you taking to transition to low-carbon and climate-resilient business models to mitigate risks associated with resource scarcity, regulatory changes, and climate impacts? How are you redesigning products and processes to minimize waste and keep materials in use throughout their lifecycle?

Nature - How is your company addressing nature-related risks such as biodiversity loss and pollution to prevent supply chain disruptions and increased operational costs?

Responsible Supply chain - What measures are in place to ensure ethical practices across all tiers of your supply chain, and how do you address issues like human rights violations or lack of traceability?

Responsible investment - How thoroughly are ESG criteria integrated into your investment decisions to align your portfolio with sustainability goals and reduce exposure to market volatility and reputational risks?

Business Insights

Insights from PwC's 28th CEO Survey reveal a nuanced understanding of the role sustainability plays in corporate strategy. One-third of CEOs reported that climate-friendly investments made over the past five years have resulted in increased revenue, while two-thirds noted that these investments have either reduced costs or had minimal impact on expenses.

According to the Global Investor Survey 2024, 50% of investors believe it is very or extremely important for companies to alter how they create, deliver, and capture value in response to climate change. Additionally, 26% consider such changes at least moderately important. Notably, 71% of investors agree that companies should incorporate ESG and sustainability directly into their corporate strategies, a sentiment consistent with previous findings. Furthermore, one-third of investors strongly agree that companies should invest in addressing ESG and sustainability issues relevant to their business, even if it may reduce short-term profitability, with an additional 35% somewhat agreeing with this perspective.

Despite strong investor trust in management boards to make long-term decisions, 44% of those surveyed expressed concern that corporate reporting on sustainability performance, particularly regarding environmental and social issues, contains unsupported claims. These findings underscore the critical need for businesses to integrate sustainability into their strategies to drive revenue growth, manage costs, and enhance profitability.

Additionally, the connection between investor support and CEO compensation tied to sustainability metrics further highlights the significance of these initiatives in today's business landscape.

These insights emphasize the importance of embedding sustainability into business strategies to foster revenue growth, control costs, and boost profitability. Moreover, linking CEO compensation to sustainability goals demonstrates the growing priority of these efforts in the modern business environment.

Sources: PwC's Annual Global 28th CEO Survey and PwC's Global Investor Survey

Third Party Risk Management

Building and delivering trust through robust programs with increased reliance on third party service providers

The use of third-party service providers continues to grow as firms embrace new technology, scale operations, and manage cost pressures. As third-party ecosystems expand in scale and complexity, many organizations struggle to keep pace. In the Nordics, numerous organizations lag behind their global peers.

Regulatory expectations are rising, with enforcement through legislation such as the Digital Operational Resilience Act (DORA). Yet, third-party risk management (TPRM) remains fragmented, lacking clear ownership, coordination, and alignment. This disconnect not only slows onboarding but also prevents organizations from empowering stakeholders and leveraging modern TPRM technologies.

Additionally, the current geopolitical climate adds further complexities to supply chains, making it challenging to identify exposures, mitigate risks, and pivot direction in a timely manner if needed. The result? Missed opportunities to realize the full strategic value of third-party relationships.

Third Party Risk Management

Risk drivers

The need for robust third-party risk management procedures continues to grow. While historically this focus was concentrated and driven by regulatory requirements within the financial services sector, the demand is now expanding across various industries.

- The regulatory landscape is evolving, with increasing expectations from regulators and key stakeholders regarding the management of third-party relationships, especially as the scale and complexity of these relationships continue to expand. New frameworks and standards are setting clearer expectations.
- There is also increased reliance on third parties due to the accelerated adoption of cloud, AI, and other technologies. If not managed properly, these dependencies can have significant impacts on organizations, customers, and markets. Organizations must also build greater resilience to respond effectively when issues arise.
- Organizations continue to be cost-conscious in managing their internal operating expenses. With the availability of better technology, they are finding opportunities to streamline their third-party risk management (TPRM) processes and support better decision-making.
- AI is rapidly changing the status quo in TPRM, prompting organizations to rethink their practices. Many third-party vendors have embedded AI into their products or services but have not provided transparency to customers about its use.

Red flags

The following red flags indicate inadequate procedures in managing third-party risks:

- There is a lack of clear ownership and accountability for TPRM activities, with no defined escalation pathways. Management of third parties is siloed within the organization, and there is no centralized team or function providing oversight. Coordination, alignment, and ownership over relationships are lacking.
- There is no single point of entry for all third-party arrangements, making it difficult to obtain a comprehensive and complete overview of third-party relationships and their associated risks. Systems may be fragmented, and procedures often rely on manual processes, such as using Excel spreadsheets. Consequently, ongoing monitoring is not performed dynamically through technology.
- There is data quality issues with:
    - Lack of clarity on which data attributes are needed to support internal and external reporting obligations
    - No single “golden source” for the data collected
    - Absence of ownership and robust quality controls over all data points.
- Intragroup relationships are not considered or monitored within the TPRM framework.
- Third parties are not segmented, and proportionality is not applied when performing risk assessments based on inherent risk.
- There is no standardized method to identify, evaluate, and monitor third-party AI use.

Third Party Risk Management

Critical Questions

When assessing the health of your organization's Third-Party Risk Management (TPRM) framework and practices, consider the following questions:

- Does the TPRM framework comply with the laws and regulations of each jurisdiction in which the organization operates?
- Is the TPRM aligned with the Board's strategy and risk appetite?
- Does the TPRM include at minimum the following activities
  - Segmentation, due diligence, and risk assessments completed for all types of third parties
  - Assessment activities proportionate to the inherent risk and criticality of the services provided by the third party
  - A policy outlining the process for continuous reassessment, taking into account any changes in the third party or the services provided
  - There is a clear process in place to report, track, risk-accept, and/or monitor remediation activities for any identified risks
  - There is a clear governance structure where the TPRM function integrates with the 2nd Line of Defense and various risk areas
- Are adequate resources available to meet ongoing expectations, particularly for those in scope of DORA, given the transition from a project-style approach to readiness toward operating under DORA requirements as part of day-to-day operations?
- How does the organization proactively manage AI-related risks among third parties? Is this incorporated into the risk tiering process? How have due diligence procedures been enhanced to account for AI deployment? Are existing vendor contracts updated to require disclosure when vendors use AI in delivering their services?

Business Insights

According to PwC's Digital Trust Insights 2025 survey, third-party breaches rank among the top three cyber threats that financial services institutions are most concerned about. Additionally, the survey highlights that one in three organizations feel unprepared to handle a third-party incident that could impact core business operations. Similarly, PwC's Global Compliance Survey 2025 found that almost one-third of respondents consider third-party and supply chain management as key compliance priorities for their organizations.

The proliferation of AI now introduces further complex risks from various sources across the enterprise, as third parties increasingly integrate AI into their product and service offerings. Without proper governance and oversight, third-party use of AI solutions can lead to security, reputational, and compliance risks for your organization. Implementing responsible AI practices is essential to ensure the reliability and trustworthiness of AI used by third parties and, most importantly, to safeguard your organization and its customers or clients.

Given these trends, it is critical for organizations to reevaluate their Third-Party Risk Management frameworks to ensure risks are kept at an acceptable level.

Supply Chain

Performance and compliance in a constantly evolving landscape

Ensuring Business Resilience in the Face of Disruptions While Adhering to Increasing Regulatory Requirements

In today's rapidly changing global landscape, operational and compliance risks, especially those related to sustainability, are more pronounced than ever, posing significant challenges to effective supply chain management. Organizations must navigate complex geopolitical, environmental, and economic factors while complying with growing regulatory demands.

As disruptions become more frequent, companies must ask themselves: Are we resilient enough to handle unexpected challenges? Do we have the agility and collaboration needed to ensure sustainability and maintain performance? By analyzing potential risk drivers and adopting proactive strategies, businesses can stay ahead of the curve.

Supply Chain

Risk drivers

Identifying and understanding the drivers of operational and sustainability risks is key to strategic decision-making for maintaining business resilience and complying with external requirements. Here's a quick overview:

- Ready for the unknown: Companies are facing more frequent and severe disruptions on multiple fronts. Geopolitical factors, such as conflicts, sanctions, pandemics, cyberattacks, and trade tensions, combine with economic pressures from rising energy costs, interest rates, resource shortages, and inflation. Environmental drivers, including rapid climate change, natural disasters, and capital market expectations, further compound these challenges. To respond effectively while maintaining supply chain performance, companies must develop agile and collaborative supply chain solutions that enable them to manage surprises and sustain operations.
- Adhering to increasing regulatory complexity: While navigating operational uncertainties, companies must comply with growing regulatory ESG requirements to avoid financial penalties, reputational damage, and exclusion from public offerings. The EU's Corporate Sustainability Reporting Directive (CSRD), Corporate Sustainability Due Diligence Directive (CSDDD), and the EU Deforestation Regulation (EUDR) underscore the importance of transparent supply chains and integrating sustainability objectives into operational supply chain planning.

Red flags

There are several red flags that indicate your organization may not be proactive enough in addressing operational and sustainability risks. Here are some key indicators to watch for:

- **Considering only Traditional Decision-Making Drivers in Supply Chain Management:** While traditional drivers such as cost, service, and quality remain important, incorporating factors like agility, resilience, and sustainability is essential for navigating uncertainties and responding effectively to unexpected challenges.
- **Reactive Decision-Making:** Responding to challenges only after risks have materialized, rather than proactively addressing anticipated issues, may lead companies to take unwanted risks, resulting in missed opportunities and potential sanctions related to non-compliance.
- **Unclear End-to-End Processes and Roles and Responsibilities:** Both operational and regulatory requirements for supply chain management demand collaboration among various functions within the organization, such as IT, compliance, and sustainability, as well as third-party partners. Working in silos can leave key risks unidentified and unmitigated.
- **Poor Data Availability:** Lacking relevant real-time information can lead to slower responses to emerging risks, missed opportunities, and difficulties meeting reporting requirements.
- **Lack of Talent and Workforce for Future Supply Chains:** The interconnected and technology-reliant supply chains demand new skills from the workforce. Shortages in talent and necessary skills may undermine productivity and efficiency.

Supply Chain

Critical Questions

To evaluate whether your organization is effectively managing operational and sustainability risks in the supply chain, consider the following questions:

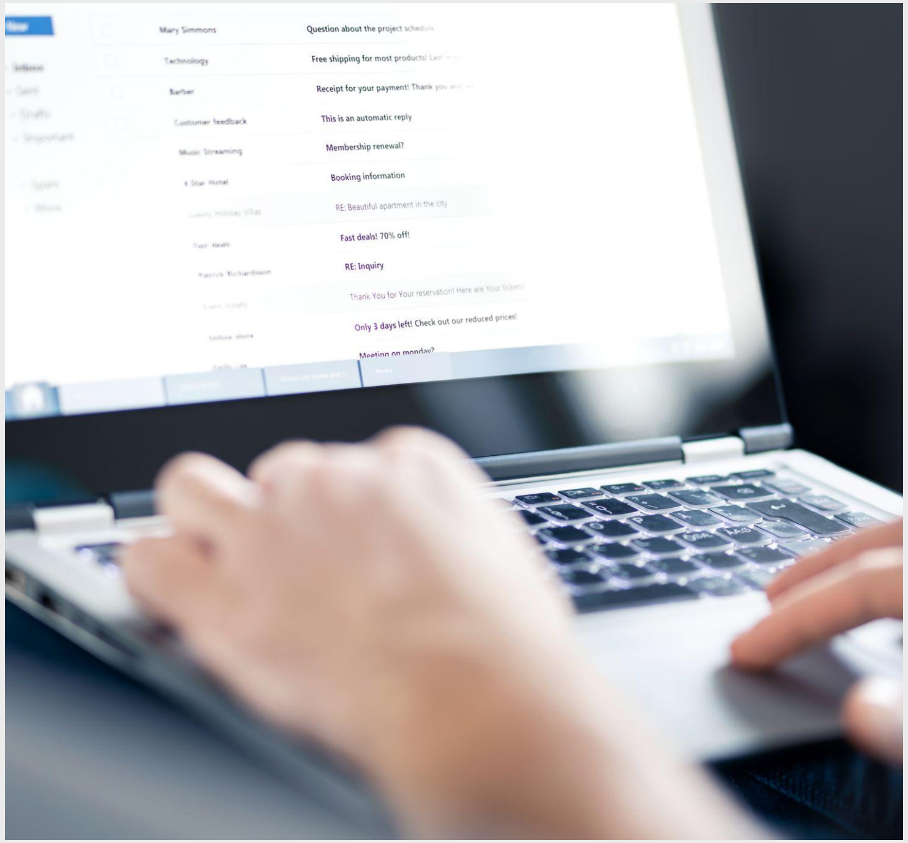
- Have we assessed how to maintain business resilience across various scenarios influenced by geopolitical, environmental, and sustainability factors? Do we fully understand these risks? Have we designed our supply chains to adapt quickly to changes? Have we integrated sustainability considerations into our supply chain processes?
- Are we proactively monitoring potential changes in the operational and regulatory landscape, or do we only react after changes occur? Do we assess lessons learned from past challenges and adjust our approaches to prevent recurrence?
- Have we mapped out our end-to-end supply chain processes and identified key process steps, associated risks, and involved stakeholders? Are the roles and responsibilities of cross-functional teams clearly defined and understood?
- Are we able to collect and analyze relevant information to support strategic decision-making and external reporting? How do we ensure that our data is accurate, complete, and timely?
- Are we attracting and retaining the right talent to support agile, interconnected supply chain processes?

Business Insights

Managing supply chain risks in today's evolving landscape requires a holistic approach that incorporates enterprise risk management, business continuity planning, and internal controls, alongside operational planning. For example, this may involve:

- **Understanding risks from various sources:** Taking a holistic, end-to-end view of the supply chain enables leaders to identify, assess, and respond to diverse risks arising from a complex environment.
- **Being ready to change direction:** Develop scenarios and action plans to adapt the supply chain to risks originating outside the company and to maintain operational performance under unusual circumstances. Define clear triggers that initiate alternative actions and establish how these actions are communicated and executed through a cross-functional process.
- **Broaden the scope of internal control:** The increasing demands on the supply chain, from both operational activities and external disruptions, must be reflected in internal control measures. Expanding the scope and enhancing collaboration both internally and with third parties enables more effective internal controls and ensures potential weaknesses are identified and addressed.

Tax


Mary Simmons
Question about the project schedule
Technology
Free shipping for most products!
Barber
Receipt for your payment!
Customer feedback
This is an automatic reply
Music Streaming
Membership renewal?
Booking information
Fast deals! 70% off!
RE: Inquiry
Only 3 days left! Check out our reduced prices!
Meeting on monday?

Transfer Pricing vigilance is the order of the day

In the wake of the OECD/G20 Base Erosion and Profit Shifting (BEPS) project, the focus is on ensuring that taxation aligns with actual value creation.

Tax structures that allocate profits to low-tax jurisdictions have become highly risky, as tax authorities worldwide prioritize protecting their taxation rights based on value creation within their jurisdictions.

Transfer pricing lies at the heart of this development. Tax authorities closely scrutinize intra-group transactions and balances to ensure that multinational enterprises comply with the arm's length principle. Non-compliance often results in costly and time-consuming tax disputes, expensive reassessments, and the risk of double taxation.

In this challenging tax environment, it is more important than ever for multinational enterprises to remain vigilant in managing their transfer pricing risks.

Tax

Risk drivers

When considering Transfer Pricing (TP) in today's tax climate, several core risks are crucial for effective risk mitigation and management. These core tax risks include: *i) Compliance and Financial Risks; ii) Regulatory and Audit Risks, iii) Operational and Strategic Risks;* and *iv) Reputational Risks*. Although the key risk drivers vary somewhat across these categories, the following are common risk factors throughout:

- Volume and Complexity of Intra-group Transactions: High volumes or high-value transactions between related parties increase the risk of incorrect pricing and attract greater tax authority scrutiny. Transactions involving complex interactions between related entities are inherently more challenging to price accurately than straightforward service or goods transactions.
- Intangibles and Intellectual Property (IP): Transactions involving the transfer or use of intangibles are often difficult to price due to their unique nature and lack of comparable market transactions. Unclear ownership or development arrangements for IP can lead to disputes over where profits should be taxed.
- Business Restructuring and Value Chain Changes: Shifting key business functions, valuable intangibles, or significant risks between group entities can attract attention, especially if profits shift to lower-tax jurisdictions. Centralizing procurement, R&D, or management functions may alter the allocation of profits and risks, raising questions about arm's length pricing.
- Inadequate or Inconsistent Documentation: Failure to maintain proper transfer pricing documentation can lead to penalties and reassessments. Discrepancies between transfer pricing documentation and other filings (such as statutory accounts or tax returns) can trigger audits. The absence of legal agreements governing intra-group transactions increases the risk of discretionary reassessments.

Red flags

Key risk drivers related to Transfer Pricing (TP) should be evaluated from two core perspectives: risk management in terms of operational efficiency and cost of tax (CoT). Inappropriate transfer prices can negatively impact operational performance, leading to reduced value creation. They may also increase overall tax costs, due to suboptimal profit allocation and the risk of double taxation. Although both perspectives are influenced by the same risk drivers, the level of exposure they cause may differ.

The following red flags should be regarded as indicators that risks are not being adequately addressed from either perspective:

- **Absence of Group-Wide TP Policy**: No formal, consistently applied, and regularly updated transfer pricing policy across the group.
- **Lack of Economic Substance**: Entities with minimal or no personnel, assets, or decision-making functions in the relevant jurisdiction retain significant profits.
- **Outdated or Missing TP Documentation**: Failure to prepare or update local files, master files, or country-by-country reports as required by local regulations.
- **Outdated or Missing Legal Agreements**: Intra-group transactions are conducted without legal agreements in place or in ways that do not comply with existing agreements.
- **Inconsistent Pricing**: Significant variations in pricing for similar transactions across jurisdictions without clear justification.
- **Frequent TP Adjustments or Disputes**: Recurring transfer pricing adjustments by tax authorities and/or a high number of ongoing transfer pricing disputes.

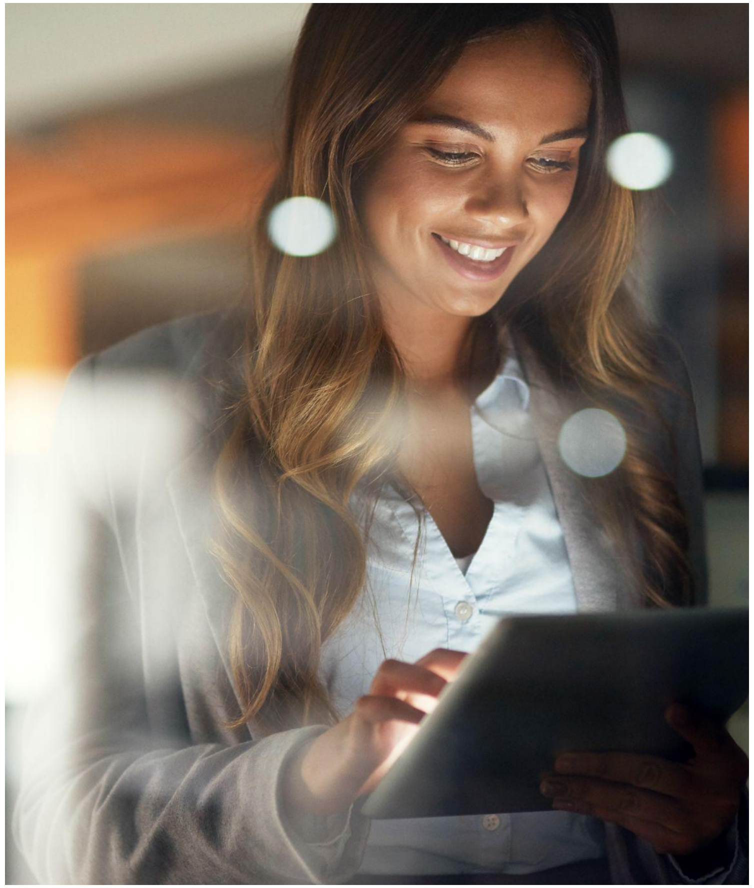
Tax

Critical Questions

The following questions should be asked to identify potential weaknesses, ensure robust compliance, and proactively mitigate transfer pricing risks:

- Does the group have a transfer pricing policy, and is it up to date?
- Are all intra-group transactions and balances clearly identified, documented, and mapped?
- What is the business rationale for each significant intra-group transaction?
- Have there been any recent or planned restructurings, relocations, or changes in the value chain, and how have these changes impacted the allocation of functions, assets, and risks among group entities? Have the changes been carried out in line with the arm's length principle, and have transfer pricing policies been updated to reflect these changes?
- Are there any transactions involving hard-to-value intangibles or unique arrangements that require special attention?
- Is contemporaneous transfer pricing (TP) documentation prepared and updated annually for all relevant jurisdictions? Does the documentation align with statutory accounts, tax returns, and other regulatory filings? Are there any inconsistencies or gaps that need to be addressed?
- Which legal entity is the legal and economic owner of key intangibles, and is this clearly documented? Are there robust agreements and supporting analyses for the transfer or licensing of intellectual property (IP)? Are profits from intangibles allocated to entities with sufficient substance and economic activity?
- Do we have a strategy for managing TP audits, including ready access to all supporting documentation required during an audit?
- Do we have access to Mutual Agreement Procedures (MAP) or Advance Pricing Agreements (APA) where needed?

Tax



Business Insights

Managing transfer pricing (TP) risks is an ongoing process that demands vigilance, adaptability, and collaboration. By implementing robust policies, leveraging technology, and fostering a culture of compliance, groups can effectively mitigate TP risks.

It is strongly recommended that the group develop a centralized TP policy outlining clear guidelines for all intra-group transactions. This approach ensures consistency across jurisdictions and aligns TP practices with the group's overall business strategy. Centralized oversight also enables timely updates in response to regulatory changes or business restructurings.

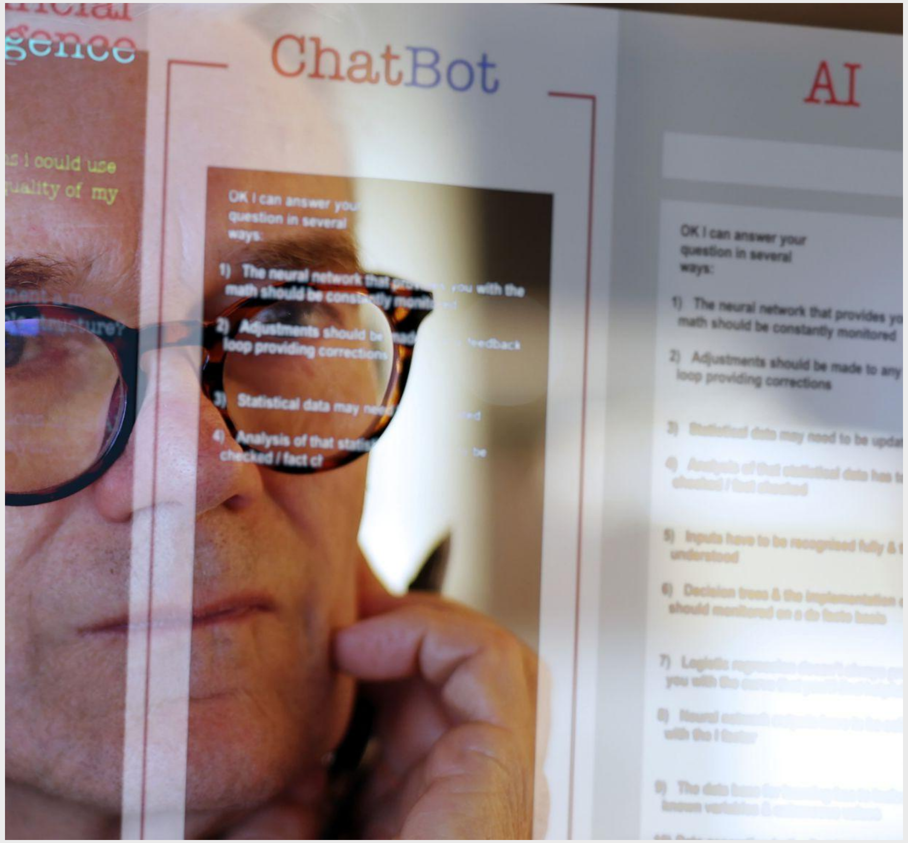
Effective TP risk management requires collaboration among tax, finance, legal, and business operations teams. Regular communication ensures that TP policies, agreements, and documentation accurately reflect actual business practices and that all stakeholders understand their roles in maintaining compliance.

Comprehensive and contemporaneous documentation is critical. Leading groups invest in technology solutions, such as transfer pricing (TP) software and data analytics tools, to automate data collection, benchmarking, and documentation processes. This not only improves accuracy and efficiency but also ensures documentation is readily available in the event of an audit.

Proactive groups conduct regular risk assessments and internal audits of their TP arrangements. This includes reviewing the accuracy of TP calculations, the appropriateness of comparables, and the alignment of TP outcomes with actual value creation. Internal audits help identify potential issues before they escalate into disputes with tax authorities.

It is recommended to develop a clear TP audit response strategy, including maintaining a repository of supporting documentation and designating a team to handle inquiries from tax authorities.

People & Organization



AI and the uncertainty evolving in the workforce landscape

In today’s rapidly changing work environment, employees face a unique set of challenges and opportunities influenced by the integration of AI technologies. More than half of the workforce perceives an overwhelming number of simultaneous changes, with approximately 44% of workers in the Nordics struggling to understand the necessity of these transformations. This atmosphere of uncertainty is further intensified by increased workloads, concerns about job security, and significant financial pressures.

Despite these challenges, many employees display remarkable optimism and engagement. Many express readiness to adapt to new ways of working, demonstrating eagerness to upskill and viewing generative AI as a tool to enhance their efficiency. Notably, over half of the workforce feels optimistic about their organization’s future, even amid current difficulties.

However, employee retention remains a pressing concern. A significant 28% of workers indicate that they are very or extremely likely to consider changing employers within the next 12 months, a notable increase from the 19% seen during the height of the “Great Resignation” in 2022. This trend highlights a disconnect between job satisfaction and the intention to stay; even among those who report being satisfied with their roles (56%), many are still contemplating departure.

The importance of skill development cannot be overstated in this context. Approximately 67% of employees indicate that opportunities to learn new skills strongly influence their decision to remain with their current employer. Moreover, employees who feel disconnected at work report a higher likelihood of seeking new job opportunities, with 50% acknowledging they have missed advancement opportunities due to a lack of connections.

With these dynamics at play, upskilling emerges as a crucial differentiator for organizations. Companies that prioritize skill development not only enhance employee engagement but also foster a culture of growth, vital for retaining top talent amid constant change. As the workplace continues to evolve under the influence of AI, understanding and addressing these workforce challenges presents an opportunity for organizations to invest in their employees, which will be key to successfully navigating the future of work.

People & Organisation

Risk drivers

Risk drivers in workforce management stem from multiple dimensions. Understanding these drivers enables organizations to develop strategies that mitigate risks and capitalize on emerging trends.

- Technological change demands continuous upskilling among employees. Without proper support, employees may feel overwhelmed, while investing in skill development fosters engagement, retention, and adaptability in an evolving technological landscape.
- Economic pressures and geopolitical tensions create an unpredictable environment that can significantly disrupt operational stability and hinder effective strategic planning. Organizations may face challenges such as supply chain disruptions, fluctuating market demands, and the need to quickly adapt to changing regulations or political climates, ultimately impacting overall performance and growth potential.
- Generative AI elicits diverse perceptions: while it offers opportunities for skill development and potential efficiency gains, it also raises concerns about increased workloads and job security.
- Climate change is increasingly perceived as a significant risk by the workforce, with 33% expecting it to significantly impact their jobs within a few years. This awareness underscores the urgent need for organizations to adopt sustainable practices, as employees seek to align their work with environmentally conscious initiatives, fostering a workplace culture that prioritizes sustainability and resilience against climate-related disruptions.
- Leadership communication gaps represent a critical business risk. In Denmark and Sweden, 44% of workers struggle to understand company transformations. When companies fail to communicate transparently and regularly about change, employees feel disconnected and may look for opportunities elsewhere. This is especially true for workforce segments leading the adoption of generative AI, including Gen Z. This highlights the need for companies to adopt transparent, frequent, and inclusive communication practices to close the gap and drive employee engagement.

Red flags

Identifying red flags is critical for proactive workforce management.

- **Lack of Upskilling Opportunities:** If employees do not have access to training and development programs to learn new technologies, they may feel overwhelmed and disengaged, potentially leading to higher turnover.
- **Increased Employee Turnover:** A noticeable rise in turnover rates may indicate that employees feel ill-equipped to handle technological changes and are seeking opportunities elsewhere.
- **Job Security Concerns**: Worries about job security, such as potential displacement due to AI, and apprehensions about the organization's financial health can elevate employee anxiety and stress, which may decrease morale and impact productivity.
- **Employee Discontent with Sustainability Practices:** If employees express dissatisfaction with the organization's environmental policies, it can lead to disengagement and negative perceptions of the company's values.
- **Infrequent or Missing Leadership Communication**:If employees report that leaders rarely communicate strategic decisions, recent changes, or their impact on daily work, motivation may drop, causing employees to consider leaving for better opportunities.
- **Workload Intensification:** Increased workloads without additional support, or a perception that leadership is not addressing the issue, can lead to burnout, reduced productivity, or turnover.
- **Skill Gaps in AI Utilisation**: A lack of adequate training to effectively use generative AI may result in underutilization of these technologies, limiting their potential benefits for the organization.

People & Organisation

Critical Questions

By addressing these questions, you can uncover insights into the effectiveness of your existing risk mitigation strategies and identify opportunities for improvement:

- How effectively are we supporting continuous adaptation and skill enhancement among our employees in response to technological changes?
- Are we providing ample opportunities for on-the-job training and mentorship to help employees develop and apply their skills?
- How well do we engage employees in discussions about the skills they need to thrive in our evolving workplace?
- How are we addressing employee concerns about workload and job security related to the introduction of generative AI in our processes?
- Are we effectively communicating the reasons behind organizational changes and engaging all segments of our workforce with our vision for the future?
- What measures are we taking to prioritize employee well-being and support them in managing workplace stress and changes?
- Do we regularly assess and update our skills inventory to understand the expertise within our workforce?
- Are our leaders adequately equipped to lead technological advancements and organizational change?

Business Insights

Drawing actionable insights from PwC's 2024 Workforce Hopes and Fears survey enables organizations to develop a responsive workforce strategy.

Addressing key drivers of job satisfaction, such as skill development and flexibility, can enhance retention and performance. Tailored training programs are essential, as over half of the workforce requires specialist skills and anticipates significant future changes.

Promoting an inclusive environment, fostering open and frequent communication, and increasing transparency in leadership help build trust and drive employee engagement during business transformations. With 70% of employees recognizing the importance of environmental responsibility, integrating sustainability into business practices aligns closely with their values.

Six percent of respondents experienced larger and more impactful changes in their jobs over the past year compared to previous years, highlighting that the current work environment is unique from a workforce perspective. Thoughtful use of generative AI can harness its potential for creativity and learning while addressing concerns about change, increased workloads, and job security.

Prioritizing these insights can help organizations adapt to workforce changes, driving growth and resilience in an evolving business landscape.

Contact details

If you have any questions on any of the topics in this document, or would like a planning session, please reach out to us!

Trine Vestengen Hopkins
Partner, Territory Risk Lead
Denmark

+45 52 15 00 03
trine.vestengen.hopkins@pwc.com

Christer Johnsson
Partner, Territory Risk Lead
Sweden

+46 70 929 28 93
christer.johnsson@pwc.com

Petri Näätänen
Partner, Territory Risk Lead
Finland

+358 50 3444445
petri.naatanen@pwc.com

Lars Erik Fjørtoft
Partner, Territory Risk Lead
Norway

+47 97 47 44 69
lars.fjortoft@pwc.com

For more information, please visit: pwc.dk - pwc.fi - pwc.no - pwc.se

Thank you

This publication or presentation has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication/presentation without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC's members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication/presentation or for any decision based on it.

pwc.com