KPMG

Internal Audit: key risk areas 2026

Internal Audit: key risk areas 2026

In today's rapidly evolving risk landscape, internal audit faces a new generation of threats that demand sharper focus and greater agility than ever before. In this environment, the expectations for Internal Audit Functions have never been higher: they must illuminate the path forward, helping organizations to navigate uncertainty, adapt to change, build resilience, and seize opportunities.

Each year, the Internal Audit Function needs to utilize its (limited) resources on the risks that matter most for the organization. KPMG has identified and compiled the key risks areas below which align with the 'Risk in focus 2026[1]' report by the European Confederation of Institutes of Internal Auditing (ECIIA). These key risk areas may be used by internal auditors to prioritize the activities in the year ahead.

Our aim with this article is to provide audit departments with a clear overview of these evolving risks, along with practical considerations for how teams can respond effectively.

These top risks should be incorporated into a flexible and dynamic audit plan – one that continues to address longstanding critical risks while remaining responsive to new and fast-moving developments.

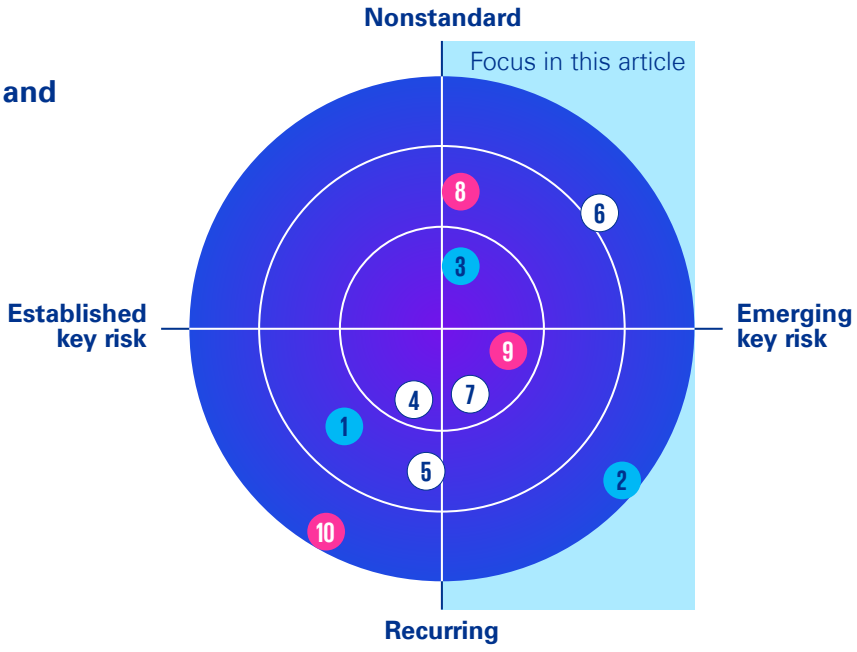
Each of these risks deserves attention, but we place particular emphasis on six risks that are expected to intensify in the near future[1]. Although our list is not an exhaustive list of key areas, it may serve well as a starting point from which the Internal Audit Function can gain leverage when assessing the organization's risk profile and control environment throughout the upcoming periods. By identifying and integrating these risks into their audit risk assessment and annual planning cycle, ambitious and resilient internal audit teams are able to remain agile and forward-looking.

Risk landscape:

overview of established and emerging risks

Risks legend:

- Technology risks
- External risks
- Operational risks



1. Data governance and privacy
2. **AI and digital disruption**
3. **Cybersecurity**
4. ESG
5. Supply chain
6. **Geopolitical tensions and macro-economics**
7. **Regulatory compliance and change**
8. **Human capital**
9. **Business Continuity Management and resilience**
10. Organizational governance and corporate reporting

[1] Risk in Focus 2026, hot topics for internal auditors

The role of Internal Audit in emerging risks

AI and digital disruption

Artificial Intelligence (AI) and digital disruption are rapidly reshaping the business landscape, and by 2029, they are expected to become the second most critical risk area for Internal Audit Functions. While these technologies offer transformative potential – automating routine tasks, enhancing decision-making, and unlocking new efficiencies – they also introduce complex risks that demand careful governance and ethical scrutiny.

AI systems are increasingly embedded in core business processes, influencing decisions that affect customers, employees, and strategic outcomes. Without robust oversight, these systems can produce unintended consequences, such as:

- **Algorithmic bias,** leading to discriminatory outcomes in hiring, lending, or customer service.
- **Overreliance on automation**, which may erode human judgment and introduce systemic vulnerabilities.
- **Data quality issues**, where low-quality or biased input data leads to flawed AI outputs, undermining trust and effectiveness.

These risks are not hypothetical. For instance, financial institutions have faced regulatory scrutiny over biased credit scoring algorithms, and healthcare providers have had to reassess AI-driven diagnostics that failed to account for diverse patient populations.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

- **Audit algorithmic transparency, biases and fairness:** Review decision logic and traceability in AI models.
- **Provide AI assurance:** Independently verify model robustness, explainability, and ethical alignment.
- **Advise on 'Responsible AI':** Support development of AI policies and best practices in innovation and risk management.
- **Enable real-time assurance:** Use AI tools for continuous monitoring of controls and risk signals. This helps organizations build trust, manage risks, and comply with regulations.
- **Strengthen AI risk awareness:** Identify where AI risks are overlooked due to low awareness and advise on clearer roles, responsibilities, and escalation paths.

Geopolitical tensions and macroeconomics

Geopolitical uncertainty has become a defining feature of the global business environment. From trade tensions and armed conflicts to shifting alliances and sanctions regimes, geopolitical developments can rapidly and significantly disrupt an organization's operations, supply chains, regulatory obligations, and financial stability. These risks are often unpredictable and can escalate quickly, leaving organizations exposed if they lack adequate preparedness and response mechanisms.

Recent examples underscore the breadth and impact of geopolitical risks:

- **Rising protectionism and trade barriers** have disrupted global supply chains, particularly in sectors reliant on cross-border manufacturing and logistics.
- **Sanctions and export controls** related to conflicts such as the war in Ukraine have forced companies to reassess supplier relationships, halt operations in certain regions, and navigate complex compliance requirements.

These developments highlight that geopolitical risk is not confined to multinational corporations – it affects organizations of all sizes and sectors, especially those with international operations, global suppliers, or exposure to foreign markets. The ripple effects can touch everything from procurement and compliance to reputation and strategic planning.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

- **Audit geopolitical exposure:** Include high-risk geographies and suppliers in audit scoping, and test whether controls exist to manage sanctions, trade restrictions, and regional instability.
- **Review crisis and continuity plans:** Test whether business continuity and crisis response procedures are up-to-date and effective under geopolitical scenarios.
- **Evaluate third-party risk management:** Verify that vendor due diligence includes geopolitical risk factors and that contingency plans are in place for critical suppliers.

Business Continuity Management and resilience

In today's unpredictable business environment, organizations face a wide range of threats that can disrupt operations and threaten long-term viability. For this reason, Internal Audit must treat business continuity and resilience not just as operational concerns, but as strategic risk areas.

By independently assessing the design and effectiveness of continuity frameworks, Internal Audit provides assurance that the organization is prepared to respond to and recover from disruptions. Examples of continuity risks include:

- **Natural disasters** that damage facilities and interrupt supply chains
- **Pandemics** that trigger shutdowns and labor shortages
- **Infrastructure failures** that halt critical services like payment systems

These scenarios highlight the need for robust continuity planning and resilience strategies. Internal Audit plays a key role in identifying control gaps, testing crisis response procedures, and validating recovery capabilities. By doing so, it helps to ensure that essential operations can continue, reputational damage is minimized, and critical assets are protected – even under adverse conditions.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

- **Assess the completeness and currency of Business Continuity Plans (BCPs):** Review whether BCPs are up-to-date, comprehensive, and tested against realistic scenarios such as cyberattacks, natural disasters, and supply chain disruptions. Internal Audit should verify that tabletop exercises or simulations are conducted regularly, and lessons learned are integrated.
- **Verify coverage through a Business Impact Analysis (BIA):** Evaluate whether the BCP addresses all critical business processes, key personnel, essential vendors, and IT infrastructure (including cloud services). Use BIA results to identify gaps in continuity coverage and prioritize remediation.
- **Evaluate backup and recovery strategies:** Confirm that backup procedures comply with the 3-2-1 rule (three copies, two media types, one off-site) and relevant standards such as ISO 27001. Internal Audit should also check whether recovery testing is performed periodically and documented.
- **Test Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs):** Review whether RTOs and RPOs are realistic, aligned with business needs, and validated through actual recovery tests. This ensures that expectations set in the BCP are achievable in practice.
- **Review escalation and crisis communication protocols:** Ensure that escalation paths, crisis team roles, and internal communication procedures are clearly defined and documented. Internal Audit can benchmark these against the NIST SP 800-34 or ISO 22301.

Cybersecurity

Cybersecurity continues to dominate the risk landscape for organizations, consistently ranking as the top concern among Chief Audit Executives (CAEs). As digital transformation accelerates and organizations become increasingly reliant on interconnected systems and cloud-based platforms, the volume of sensitive data flowing across networks grows exponentially. This expanding digital footprint makes organizations more vulnerable to cyber threats, ranging from ransomware attacks and phishing schemes to insider threats and third-party breaches.

Recognizing this, the Institute of Internal Auditors (IIA) has introduced a mandatory Cybersecurity Topical Requirement, effective February 2026. This Requirement sets a global baseline for how Internal Audit must assess cybersecurity governance, risk management, and controls.[2]

The frequency and sophistication of cyberattacks are rising, with recent incidents demonstrating how a single breach can disrupt operations, damage reputations, and expose critical weaknesses in governance and control environments. For example:

- **Ransomware attacks** have shut down hospital systems, delaying patient care and forcing manual operations.
- **Phishing campaigns** have led to unauthorized access to financial systems, resulting in fraudulent transactions and data leaks.
- **Third-party breaches** have compromised customer data due to inadequate vendor oversight, highlighting the need for robust supply chain security.

These scenarios underscore the importance of Internal Audit's role in evaluating the effectiveness of cybersecurity controls. Internal audit teams are uniquely positioned to provide independent assurance on whether cybersecurity frameworks are not only in place but also agile enough to respond to emerging threats.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

- **Apply frameworks:** Use ISO 27001, NIS2 or DORA to review governance, identity management, training, data protection, and incident response.
- **Verify data privacy:** Check if personal data is securely collected, stored, retained, and disposed of, and whether third-party access is properly managed (e.g., GDPR compliance).
- **Evaluate incident response:** Confirm that response plans are tested, documented, and improved – covering escalation and crisis readiness.
- **Challenge emerging risks:** Review how the organization addresses threats like deepfakes, AI-driven attacks, and cloud misconfigurations.

[2] The Institute of Internal Auditors (IIA), 'Cybersecurity Topical Requirement', issued February 2025, effective February 2026. Available at: https://www.theiia.org/en/standards/2024-standards/topical-requirements/cybersecurity/.

Human Capital

In today's dynamic business environment, human capital risks are increasingly recognized as central to organizational resilience and long-term success. Organizations that fail to attract, develop, and retain the right talent face declining productivity, weakened innovation, and difficulty executing strategic priorities. As workforce expectations evolve – driven by hybrid working models, shifting cultural norms, and growing emphasis on well-being – managing people-related risks has become more complex and more critical.

Human capital risk is now recognized as one of the top concerns for executive leadership and is expected to remain a key priority in the years ahead. When talent strategies are misaligned with business goals, organizations may experience:

- **Skills shortages** in critical areas such as cybersecurity, data analytics, and AI, slowing down innovation and transformation efforts.
- **High turnover and disengagement,** often stemming from deficient organizational culture or lack of career development opportunities.
- **Challenges in talent acquisition,** particularly in competitive markets where attracting top talent requires a compelling employee value proposition.
- **Inadequate succession planning,** which can leave leadership roles vulnerable and disrupt continuity during periods of change.

These challenges reflect broader organizational vulnerabilities that can impact strategic execution, operational efficiency, and long-term competitiveness. Addressing human capital risks is therefore not just an HR concern, it i's a risk for the organization.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

- **Workforce planning and talent management:** Assess if the organization has a competent workforce, and review how it attracts and retains talent.
- **Development and performance:** Audit training programs and performance management to ensure employees are supported and goals align with business needs.
- **Culture and engagement:** Evaluate initiatives for employee well-being, workplace culture, and engagement to identify risks related to turnover or low morale.
- **Compensation and compliance:** Review fairness of pay and benefits, and verify compliance with labor laws and HR regulations.
- By auditing and integrating soft controls into risk management, Internal Audit can go beyond assessing hard processes and structures, providing deeper insight into the behavioral and cultural factors that underpin sustainable performance.

Regulatory compliance and change

Regulatory compliance and the pace of legislative change continue to be among the most significant challenges facing organizations today. As governments and regulatory bodies introduce new requirements – often in response to technological advances, environmental concerns, or geopolitical shifts – organizations must remain agile, informed, and proactive in their approach to compliance.

In the Netherlands, the Verklaring Omtrent Risicobeheersing (VOR) was introduced into the Dutch Corporate Governance Code, effective from January 1, 2025. Dutch listed companies are now required to include a formal statement in their annual reports on the effectiveness of their internal risk management and control systems covering regulatory compliance. Failure to comply with applicable laws and regulations can result in severe consequences, including financial penalties, operational disruptions, and reputational damage. For example:

- **Non-compliance with data protection laws** such as GDPR or the Digital Services Act can lead to multimillion euro fines and loss of customer trust.
- **Inadequate monitoring of ESG-related disclosures** may result in regulatory scrutiny and investor backlash.
- **Failure to adapt to industry-specific regulations,** such as those in financial services or healthcare, can lead to license revocation or legal action.

These risks are not limited to legal departments – they affect the entire organization, from strategic planning to day-to-day operations. As regulatory environments become more complex and dynamic, organizations must ensure that compliance frameworks are robust, well-integrated, and continuously updated.

The role of Internal Audit

To incorporate this topic into your Audit Plan, consider one or more of the following:

For Internal Audit, this means taking a proactive role in identifying and assessing the impact of regulatory developments. It involves evaluating whether the organization's compliance frameworks are robust, adaptable, and aligned with current and emerging obligations. Internal Audit must also ensure that regulatory risks are embedded into audit planning and that there is close collaboration with legal, compliance, and risk management functions.

- **Monitor regulatory developments:** Track emerging laws (e.g., VOR, DSA, CSRD) and assess their impact on internal controls and risk frameworks.
- **Evaluate compliance frameworks:** Test whether policies and procedures are up-to-date, well-integrated, and responsive to changing regulations.
- **Validate regulatory compliance:** Confirm adherence to a specific regulation and whether the organization complies with the requirements as included in the compliance framework.

How can KPMG assist?

Effectively managing risk is essential to building a resilient and future-ready organization. KPMG can support the internal audit function through either an outsourcing model or a co-sourcing model.

	Strategic and SME support Deliver deep expertise for specific areas to strengthen audit quality and provide strategic insight	Internal Audit sourcing (Flexible layer) Provide scalable audit execution capacity to meet urgent needs without compromising quality
WHAT WE DELIVER	• **Deep risk expertise:** Provide subject-matter experts for specific risk areas for the organization (e.g. Cyber, ESG, digitalization, regulatory and HSE). • **Strategic insight:** Lead and participate in deep-dive sessions to challenge assumptions, analyze trends, and deliver prioritized action plans. • **Benchmarking & analytics:** Leverage KPMG's global SME and Analytics center for advanced methodologies, benchmarking, and predictive insights.	• **Audit execution support:** Co-execute audits under direction of the internal audit function, covering urgent needs or regional scope. • **Global reach:** Auditors available across regions and time zones, ensuring local business understanding and global consistency. • **Efficiency tools:** Immediate productivity through playbooks, templates, and onboarding protocols aligned with the methodology of the internal audit function.
VALUE DRIVER FOR THE INTERNAL AUDIT FUCNTION	• Sharper scoping and more relevant procedures due to extensive subject expertise and experience. • Stronger challenge to management, clearer root causes, and reduced blind spots. • Enables proactive risk mitigation and strategic decision-making. • Accelerates delivery of high-quality findings and actionable recommendations.	• Rapid response to peaks and urgent audit requirements without re-contracting delays. • Maintains quality and consistency across geographies and languages. • Reduces cost through offshore delivery while preserving control and compliance.

Whether you choose strategic support or Internal Audit sourcing, we offer the following services:

- Serve as a dedicated partner for all matters related to the role, responsibilities, and audit agenda of your Internal Audit function.
- Support every stage of the internal audit process, from planning and execution to reporting and follow-up.
- Provide specialists (in areas such as compliance, IT systems, risk management, treasury, tax, and security) who possess an in-depth understanding of your business and processes.
- Deliver global, on-the-ground support with professionals who have specific language skills and knowledge of local regulatory requirements.
- Apply the lastest audit methodologies.
- Offer access to industry best practices and benchmarking.

With our proven methodology, extensive experience, and expertise, we are the ideal partner to help you fully realize the potential of your internal audit function.

Contact

Huck Chuah

Partner
Risk & Regulatory – Governance, Risk & Compliance Services

E: Chuah.Huck@kpmg.nl
T: +31 206 56 4501

Bart van Loon

Partner
Risk & Regulatory – Governance, Risk & Compliance Services

E: VanLoon.Bart@kpmg.nl
T: +31 206 56 7796

Jacco Pols

Senior Manager
Risk & Regulatory – Governance, Risk & Compliance Services

E: Pols.Jacco@kpmg.nl
T: +31 206 564531

Dominique Ten Berge

Manager
Risk & Regulatory – Governance, Risk & Compliance Services

E: TenBerge.Dominique@kpmg.nl
T: +31 204 262668