KPMG

Shaping the future

Internal Audit Hot Topics 2027

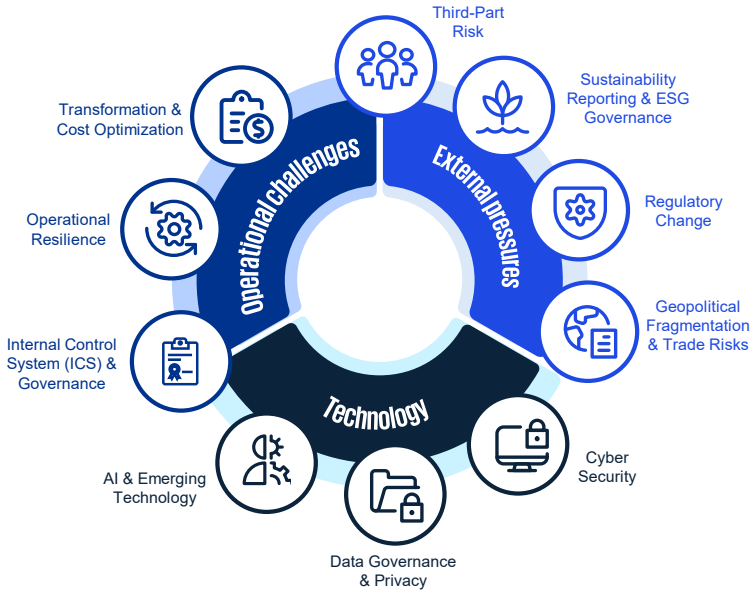
A curated view of the risk priorities shaping Internal Audit

KPMG. Make the Difference.

In 2027, organizations are operating in an environment defined by compounding uncertainty and accelerating change. Globalization pressures, climate volatility, geopolitical disruption and heightened regulatory expectations continue to converge, while the rapid, enterprise-wide adoption of artificial intelligence (AI) is fundamentally reshaping how decisions are made, risks emerge and controls operate.

In this context, the role of Internal Audit is evolving beyond periodic assurance to a more dynamic, forward-looking function – one that anticipates emerging risk and adapts audit approaches in step with the pace of change.

To support Heads of Internal Audit, we have developed a curated portfolio of key thematic areas and associated risks to inform the development of 2027 Internal Audit plans. These topics are organized across three overarching priorities: **external pressures, operational challenges and technology**.



External pressures

Geopolitical Fragmentation & Trade Risks

- Trade restrictions impact Swiss exporters.
- Supply chain disruptions continue to increase.
- Sanctions and export controls require monitoring.

Regulatory Change

- Regulatory focus shifting from compliance to resilience and accountability, with increased board and executive liability.
- Governance expectations continue to rise, and compliance must be demonstrated and documented.

Sustainability Reporting & ESG Governance

- CSRD impact on Swiss groups and ESG reporting requirements are expanding.
- Data quality remains a key challenge.
- Greenwashing risk is under greater scrutiny.

Third-Party Risk

- Growing reliance on third-parties for critical operations.
- Increased regulatory focus on third-party and concentration risk.
- Greater complexity in outsourcing and global supply chains.

The role of Internal Audit

- Assess exposure to tariffs, export controls and sanctions across the value chain.
- Evaluate trade compliance, customs control, supply-chain resilience and contingency arrangements.
- Support scenario analysis of financial and operational impacts.

- Embed high-accountability regulatory obligations into audits.
- Test readiness for major regulatory reforms.
- Identify gaps before regulatory intervention occurs.
- Use AI tools to support identification of relevant regulatory obligations, identify controls and assess effectiveness.

- Assess readiness for mandatory ESG and climate disclosures.
- Review governance, controls and data quality supporting ESG reporting.
- Evaluate alignment between ESG risks, strategy and risk management.
- Provide assurance over ESG governance frameworks.

- Review third-party risk management governance and frameworks, including due diligence, contracting and ongoing monitoring.
- Test resilience planning for critical third-party dependencies.
- Provide assurance over third-party controls supporting compliance.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member of the KPMG global organization of independent firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Technology	The role of Internal Audit
AI & Emerging Technology • Rapid AI adoption outpacing governance and controls. • Increased scrutiny of bias, transparency and explainability. • Growing use of autonomous tools and AI agents. • Increasing regulatory focus through the EU AI Act and related AI governance requirements.	• Inventory AI use cases and assign risk tiers. • Assess AI governance, ownership and human oversight. • Review controls over data, models and third-party providers. • Perform pre- and post-deployment reviews for bias, drift and monitoring. • Assess readiness for emerging AI regulatory requirements.
Cybersecurity • Increasingly sophisticated cyber threats, including ransomware. • Shift from framework alignment to control-level testing. • Growing volume of critical cyber vulnerabilities and exposures. • NIS2 and Cyber Resilience Act (CRA) increase compliance expectations.	• Assess incident detection, response and recovery capabilities. • Test ransomware and cyber incident scenarios. • Coordinate assurance over IT general controls. • Review vulnerability management and patching processes. • Assess readiness for evolving cyber and technology regulations.
Data Governance & Privacy • Stronger privacy obligations and enforcement. • Heightened impact of data breaches and poor data quality. • Greater use of automated decision-making and analytics.	• Review data governance roles, frameworks and accountability, and controls over data quality, access, retention and security. • Test data breach response and notification processes. • Evaluate readiness for enhanced privacy requirements.

Operational challenges	The role of Internal Audit
Transformation & Cost Optimization • Continued cost pressures driving restructuring, automation and outsourcing. • Risk of control gaps as cost initiatives accelerate. • Tension between efficiency and resilience objectives.	• Assess alignment of cost initiatives with risk appetite. • Identify control weaknesses arising from restructures or automation. • Review governance over major cost-transformation programs. • Provide assurance that savings do not undermine key controls.
Operational Resilience • Increasing frequency and severity of operational disruptions. • Heightened regulatory expectations for resilience and continuity, with stronger focus on critical operations, tolerances and dependencies.	• Test critical operations mapping and tolerance setting. • Review business continuity and disaster recovery plans. • Assess third-party dependencies and resilience measures. • Perform scenario testing and tabletop exercises.
Internal Control System (ICS) & Governance • Strong governance remains a board priority. • Internal Control Systems face increasing scrutiny. • Assurance over key controls remains essential.	• Evaluate the effectiveness of key controls. • Assess the maturity of the Internal Control framework. • Provide assurance over governance and risk management processes.

Contact us

For further guidance, please contact KPMG's Risk, Controls & Internal Audit team.



Karolis Jankus
Partner - Risk, Controls & Internal Audit
+41 58 249 68 76
karolisjankus@kpmg.com



Klaus Klingler
Manager - Risk, Controls & Internal Audit
+41 58 249 24 45
kklingler@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/ch

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member of the KPMG global organization of independent firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public