KPMG

Addressing top-of-mind technology, media, and telecom issues

ESG

As businesses are about to adopt mandatory and regulated sustainability reporting frameworks, the 2022 KPMG Survey of Sustainability Reporting research is instrumental in helping TMT companies benchmark their sustainability reporting efforts against their peers and other industries.

Key insights for TMT companies include the following:

- **TMT is third in carbon reduction reporting:** TMT companies have long been socially conscious champions of environmental stewardship. Of the 15 industries surveyed, TMT ranks 3rd with 81 percent of companies reporting on carbon targets.
- **TMT is tops in reporting assurance:** Independent, external assurance of sustainability reporting enhances credibility of the information and fosters stakeholder trust. TMT leads all industries, with 64 percent obtaining reporting assurance.
- **TMT lags in biodiversity risk reporting:** The strengthening of the world's biodiversity and natural systems can mitigate climate change and its associated risks. However, only 30 percent of TMT companies report on the risk that the loss of biodiversity represents to their business, ranking 13th among 15 industries.

Thought leadership:

- Sustainability reporting at tech, media, and telco companies
- ESG in the crypto world: Climate reporting and decentralized finance
- What role might blockchain technology play in the future of Scope 3 environmental reporting?
- Four ways media & telecom financial executives are preparing for the SEC's proposed climate rule

Cyber

As digital-first business strategies continue to be pushed to the forefront, many have achieved extreme transformation velocities—**substantially decreasing exposed digital surface areas most vulnerable to cyberattacks**. Concurrently, **a significant uptick in adversarial activity and an ever- changing threat landscape increases the risk of an event occurring**. Threat actors have invested in highly sophisticated attack tools, techniques, and procedures.

Key focus areas include:

- **Aligning business with security:** Cyber teams must flex their priorities to support evolving business needs and technology strategies.
- **Digital trust:** Customer expectations around stewardship, data protection, and transparency are elevated by new and enhanced customer engagement methods.
- **Cloud transformation:** Cloud security teams must develop a cloud-first security strategy and approach including cloud-native controls, cyber resilience, cloud provider security assessment, and cloud security governance.
- **Evolving cybersecurity teams:** Address capacity gaps in critical skills areas through managed service providers, novel resourcing approaches, and investment in upskilling employees.

Thought leadership:

- Building customer trust through effective cyber security risk management
- Mitigating risk in an increasingly digitized world
- Tech companies lean on cyber to go faster and gain trust
- Cyber considerations for the Metaverse
- Taking a byte out of cybercrime

INSIGHTS

The 2022 KPMG U.S. Technology Survey Report reflects the responses of more than 1,000 cross-industry enterprise technology leaders about their organizations' current level of digital maturity, technology investment plans, major transformation challenges, and more.

› 2022 KPMG U.S. Technology Survey Report

The 2022 KPMG U.S. Technology Industry CEO Outlook, has been released in a unique time period on the heels of the pandemic and amid a business environment marked by high inflation, new geopolitical tensions, and fears of a recession. It delves into key topics at the top of today's technology agenda.

› 2022 KPMG U.S. Technology Industry CEO Outlook

Monitor trends and identify potential opportunities that could impact your strategic objectives in this economic environment.

› Office of the Chief Economist

kpmg.com/socialmedia

Addressing top-of-mind technology, media, and telecom issues (continued)

2022 fraud outlook

Technology companies are navigating overlapping challenges related to fraud, noncompliance, and cyberattacks. How is your organization keeping up with the evolving threat landscape? The old rules don't always apply–and overconfidence can be dangerous.

As Mark Gibson National Sector Leader for TMT states, "Fraud, cyberattacks, and other threads are on the rise. To serve the needs of customers, employees, suppliers, and society, prevention, detection, and responsiveness should be top of mind for TMT companies. Those who remain focused on these areas not only will protect their organizations' and customers' sensitive information but also will build trust and create a competitive advantage."

The five things sector executives need to know:

- TMT companies face predictable fraud challenges related to their heavy use of information and communication technology but need to remember other vulnerabilities too.
- The sector's confidence in its antifraud policies may be displaced.
- TMT leaders would be well served to remember the reputational risks of noncompliance and due diligence when making investment decisions.
- Sector cyber defenses seem insufficient in the face of a growing, and increasingly diverse, challenge.
- TMT actively addressed the cyber risks of working from home, but most executives are now concerned about the ongoing challenges of hybrid working.

Thought leadership:

- Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook

Regulatory scrutiny of technology and data

Digitally enabled, automated, interconnected, and real-time services and innovations fuel business but with what current and emerging regulatory risks?

Did you know that:

- Bank information technology concerns constitute 25 percent of all cited supervisory concerns, with most related to risk management and controls, according to the Office of the Comptroller of the Currency (OCC).
- Insufficient data protection or information security can constitute an unfair practice, according to the Consumer Financial Protection Bureau (CFPB).
- Multiple investigations of companies' records preservation practices and employee use of unauthorized communication channels, including personal devices, have been initiated by the Security and Exchange Commission (SEC) and other regulators.
- A new approach to the data privacy and security framework is needed, and according to the Federal Trace Commission (FTC), particularly one that would involve substantive limits rather than procedural protections.

Priority areas of focus:

- Adequacy of risk assessments processes
- Vulnerability management
- Data and cloud governance
- Identity and access management
- Secure software development lifecycle
- Third-party risk
- Threat intelligence/insider threat
- Operational resilience
- Board reporting
- 2nd/3rd line of defense oversight

Thought leadership:

- Regulatory Scrutiny of Technology and Data

INSIGHTS

The business and risk environment has changed dramatically over the past year. This insight highlights the eight issues for audit committees to keep in mind as they carry out their 2023 agendas.

› On the 2023 Audit Committee Agenda

The 2023 KPMG Global Semiconductor Industry Outlook provides perspectives from a survey of 151 semiconductor leaders about their outlook for the industry in 2023 and beyond.

› Global Semiconductor Industry Outlook for 2023

The 3rd KPMG American Worker Survey sought to understand what American workers are thinking about their organizations and opportunities.

› American Worker Survey - Technology, Media, and Telecom

kpmg.com/socialmedia