# Telecommunications
## Risk factor survey 2025/26

Executive summary

# Contents



All sources cited throughout this report can be found on this page

# Executive summary

**The 2025/26 Telecommunications Risk Factor Survey reveals a decisive pivot in the global telecoms and data centre sectors, marked by sharper operational, regulatory, and financial pressures.** This aligns with BDO's Global Risk Landscape 2025, which cautions that a reactive, compliance-led approach to risk is ill-suited to today's "permacrisis" environment, where systemic shocks have become the norm.

This year's findings highlight a significant shift in risk priorities from 2023, where regulatory and tax-based risks dominated, to more immediate operational concerns. **In 2025, Cybersecurity has surged to the top of the global rankings, with 85% of operators citing it as a critical risk.**

While supply-side fragility, driven by dependence on key vendors, is another defining theme, industry-specific risks remain pronounced. These include competitive pressures, natural disasters, and the uncertainties of 5G rollout – a new risk in 2025, shaping strategic outlooks. This shift in focus signals a broader recalibration, as the **industry moves from simply managing policy exposure to actively addressing tangible threats that directly disrupt continuity and resilience.**

Additionally, though coming in 10th position this year, **a notably larger proportion (70%) of telecommunications operators and data centres cite climate change and other environmental concerns as a growing risk.** This is likely to increase as a going concern in the years ahead, and one that all operators will need to plan and strategise around.

This executive edition has been designed as a concise companion to BDO's 2025/26 Telecommunications Risk Factor Survey. ***The Full Report*** provides extended commentary, methodological notes, and detailed regional analysis for those wishing to explore the underlying data and cross-market comparisons in greater depth. Readers are encouraged to consult that version for a complete understanding of the global and regional risk dynamics shaping the sector.

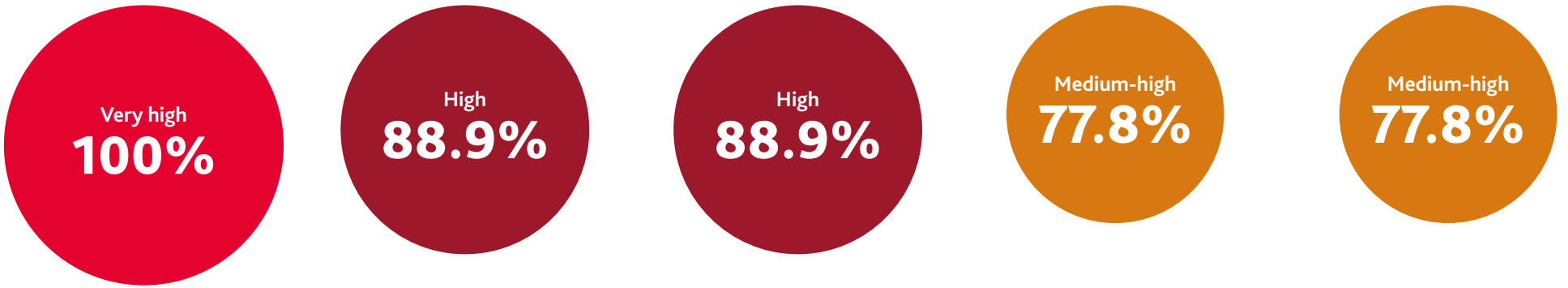
## TOP 10 GLOBAL RISK FACTORS – 2025 VS 2023

| | 2025 | | 2023 | |
|---|---|---|---|---|
| 01 | Cyber-attacks, information or security breaches, or technology disruptions | 85.0% | Changes in tax laws and regulations, judicial interpretations or administrative actions | 77.8% |
| 02 | Intense and increasing competition from other telecommunications services providers and competitors in related industries | 83.3% | Extensive and evolving governmental legislation and regulation (numerous surcharges and fees) | 76.2% |
| 03 | Challenges from changing industry regulations | 80.0% | Cyber-attacks, information or security breaches, or technology disruptions | 71.4% |
| 04 | Natural disasters, extreme weather conditions, and terrorist or other hostile acts | 76.7% | Challenges from changing industry regulations | 71.4% |
| 05 | Interest rate risk (significant fluctuations in the fair value of financial instruments) | 76.7% | Climate change and other environmental concerns | 58.7% |
| 06 | Dependence on key suppliers and vendors to provide necessary equipment and services | 75.0% | Foreign exchange risk (fluctuations in exchange rates) | 57.1% |
| 07 | Changes in tax laws and regulations, judicial interpretations or administrative actions | 71.7% | Political instability in operating markets | 57.1% |
| 08 | 5G Deployment and Evolution Risk | 71.7% | Compliance issues with data privacy and confidentiality | 57.1% |
| 09 | Changes in the technologies and business models of the telecommunications industry | 70.0% | Failure to ensure information technology infrastructure reach and resilience | 55.6% |
| 10 | Climate change and other environmental concerns | 70.0% | Interest rate risk (significant fluctuations in the fair value of financial instruments) | 52.4% |

## Spotlight: data centres

Our latest report includes **a new, dedicated assessment of risks in the global data centre segment**, where financial and cyber vulnerabilities are even more acute. All of the data center operators that were surveyed flagged supplier dependence, cost inflation, and interest rate exposure, underscoring the fragility of capital-intensive business models. Climate risks and reputational exposure linked to energy and water use further amplify these vulnerabilities.

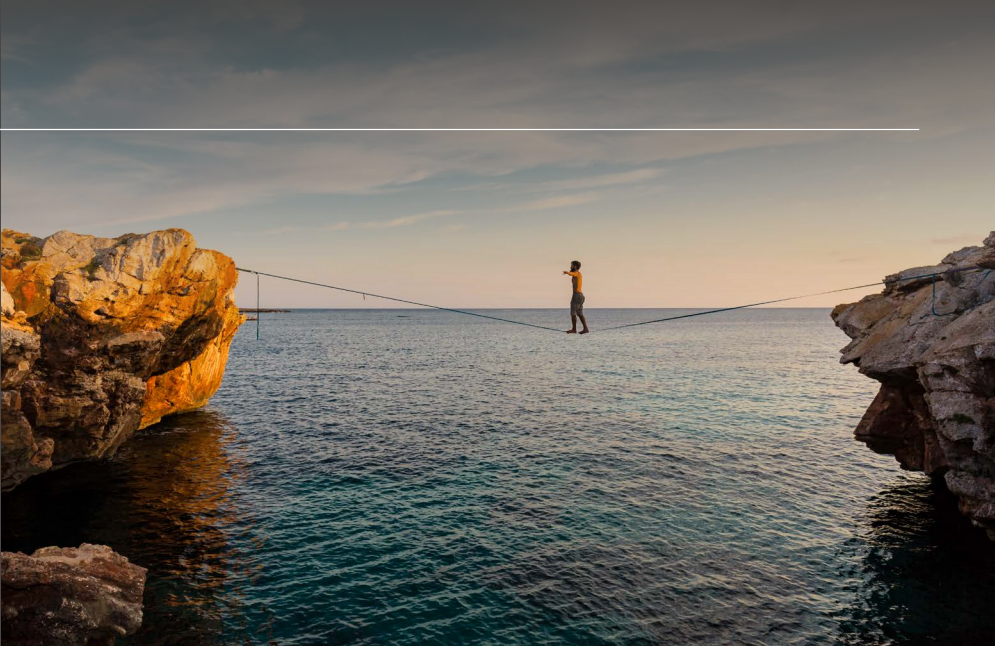
### DATA CENTRE VS TELECOM RISK VULNERABILITIES



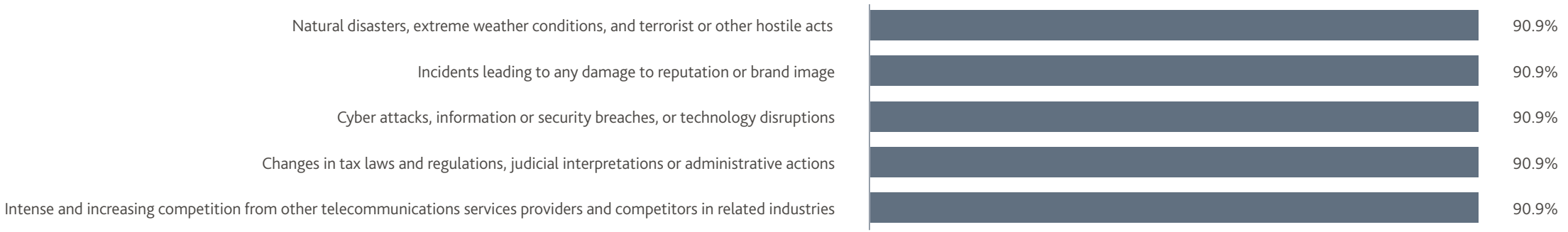

| RISK THEME | Financial fragility | Cybersecurity and digital threats | Climate and environmental fragility | Macroeconomic volatility | Revenue/investor concentration |
|---|---|---|---|---|---|
| CHARACTERISTICS | **Dependence on suppliers, inflationary cost spikes, interest rate volatility** | **AI-enhanced intrusions, hybrid cloud vulnerabilities, reputational exposure from data breaches** | **Extreme weather, ESG scrutiny on energy/water use** | **Stock market swings, FX exposure, trade/geopolitical disruptions** | **Future cash flow uncertainties and liquidity or deterioration in the capital markets (changes in credit ratings)** |
| DIFFERENTIATION VS TELECOMS | More acute than telcos due to concentrated capital cycles and hyperscale demand | Shared with telcos but amplified by scale of third-party data holdings | Impacts magnified by fixed, power-dense infrastructure | Directly tied to REIT valuation and investor confidence | Unique vs. telcos' broad consumer base |

## Regional and strategic outlook

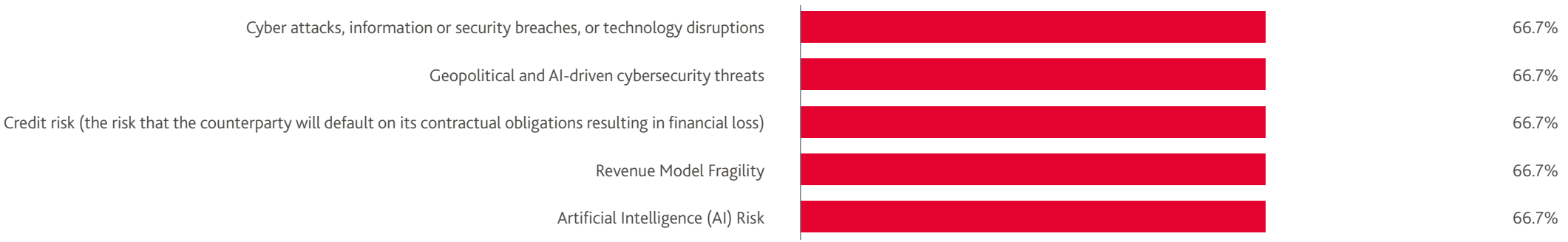
Regionally, risk intensity varies, but a common pattern emerges: The Americas show the highest risk intensity (legal and structural pressures), while EMEA exhibits a more balanced concern of digital, legal, and financial challenges. In APAC, however, the balance of risks has shifted, with operators grappling with the convergence of AI-driven cybersecurity threats, credit fragility, and uneven regulatory readiness, signalling that resilience in 2025 depends as much on digital governance as on infrastructure expansion. Leading operators are responding with proactive, opportunity-seizing measures such as zero-trust cybersecurity, modular infrastructure, and ESG-aligned governance. **Risk management, in this context, has become a competitive differentiator rather than just a compliance task.**



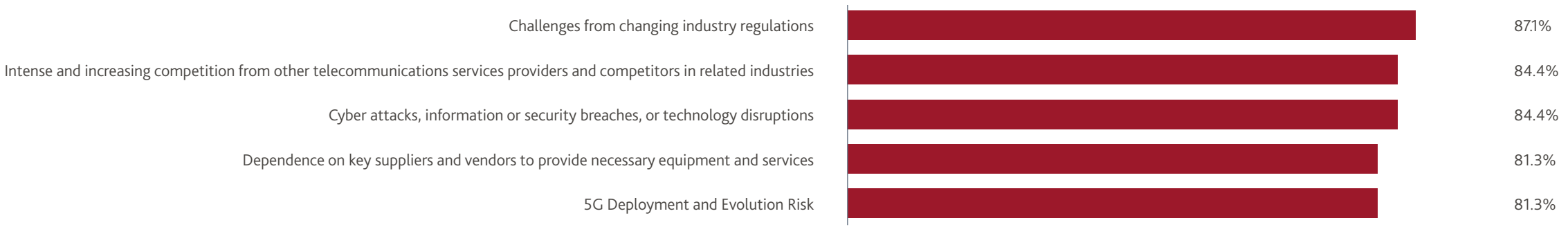
### TOP RISKS – AMERICAS



## TOP RISKS – APAC



## TOP RISKS – EMEA



# Risk mitigation

**In response to the evolving risk landscape over 2025, both telecommunications and data centre operators are implementing a range of mitigation strategies tailored to the unique pressures they face.** Drawing on our assessment of 60 telecommunications operators worldwide, along with a number of data centres, clear trends have emerged in how companies are adapting to challenges across cybersecurity, climate resilience, financial exposure, regulatory complexity, and geopolitical disruption.

**These interventions span technical, operational and strategic domains, reflecting a shift toward long-term resilience planning rather than reactive risk response.** The table below consolidates the key risk themes that dominated our 2025 analysis and highlights the corresponding mitigation strategies that operators are deploying.

| RISK THEME | Cybersecurity risk | Regulatory complexity | Capital cost and financial fragility | Climate and environmental risk | Geopolitical and trade exposure |
|---|---|---|---|---|---|
| CHARACTERISTICS | **Rise in AI-enhanced cyberattacks, API vulnerabilities, and high-volume phishing schemes targeting cloud and edge layers.** | **Ongoing ESG reforms, data protection laws, and spectrum compliance changes varying by jurisdiction.** | **Cost inflation, rising interest rates, and currency volatility disrupting infrastructure expansion and debt affordability.** | **Physical infrastructure exposure to extreme weather, energy instability, and water shortages.** | **Heightened supply chain dependency, cross-border procurement risks, and trade regulation uncertainty.** |
| MITIGATION STRATEGIES | ▶ Implementation of zero-trust architecture to limit lateral movement[1]<br>▶ AI-enabled threat detection systems embedded in core platforms[2]<br>▶ 24/7 cyber operations centres for incident response[3]<br>▶ Secure-by-design protocols applied across new product lifecycles.[4] | ▶ Formation of Board-level ESG governance and compliance structures[5]<br>▶ Integration of ESG reporting into annual risk disclosures[6]<br>▶ Enterprise-wide regulatory horizon scanning and reporting mechanisms.[7] | ▶ Adoption of modular infrastructure to reduce upfront capital outlay[8]<br>▶ Refinancing and restructuring of legacy debt portfolios[9]<br>▶ Increased internal cost-efficiency programmes tied to regional priorities.[10] | ▶ Launch of regionalised net-zero targets and scenario testing[11]<br>▶ Deployment of solar arrays and renewable backup systems[12]<br>▶ Energy efficiency programmes focused on emissions and operational resilience.[13] | ▶ Supply chain localisation and diversification through regional sourcing initiatives[14]<br>▶ Inclusion of multi-tier supplier certification and ESG audits[15]<br>▶ Increased transparency in supplier engagement through regulatory filings.[16] |



**www.bdo.co.uk**

FOR MORE INFORMATION:

**TOM MANNION**
Leader of Global Telecoms
tmannion@bdo.com

**CARL BOSMA**
Director, BDO South Africa
cbosma@bdo.co.za