Telecommunications
Risk factor survey 2025/26

Comprehensive edition

Contents

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 report forms part of BDO's Telecommunications Risk Factor Survey. A companion ***Executive Summary Report*** distils the key insights, visuals, and region-level highlights for senior decision-makers who require a concise, high-impact view of the findings. Readers are encouraged to access that version for a rapid strategic overview or to share with leadership teams seeking a snapshot of the global risk landscape.

TOP 10 GLOBAL RISK FACTORS – 2025 VS 2023

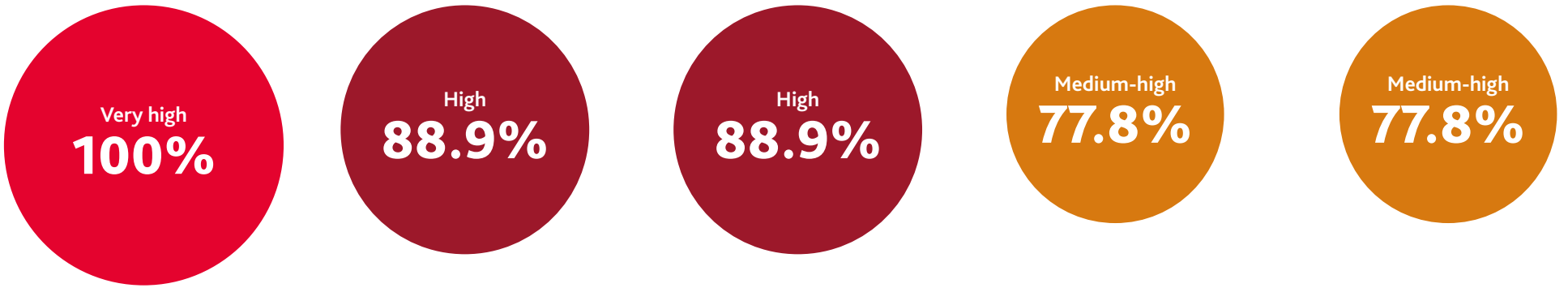
	2025		2023	
01	Cyber-attacks, information or security breaches, or technology disruptions	85.0%	Changes in tax laws and regulations, judicial interpretations or administrative actions	77.8%
02	Intense and increasing competition from other telecommunications services providers and competitors in related 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 centre 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

2025 INTENSITY



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 inthe 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

Sector Overview and Strategic Context

The telecommunications sector continues to experience rapid transformation, shaped by evolving regulatory frameworks, rising cybersecurity threats, and increasing pressure to deliver resilient, future-ready infrastructure. These challenges are compounded by the sector's growing role in enabling digital inclusion, cloud services, and national security.

This 2025/26 edition of the Telecommunications Risk Factor Survey builds on the foundation laid in previous reports, offering a consolidated global view of the top risk factors facing telecoms operators. In addition to sector-wide analysis, the report features comparative insights across EMEA, the Americas and APAC, as well as a new dedicated focus on risks facing data centres as a distinct and unique infrastructure category. Notable risk mitigation strategies employed by operators globally have also been included to provide a forward-looking gauge on what to consider.

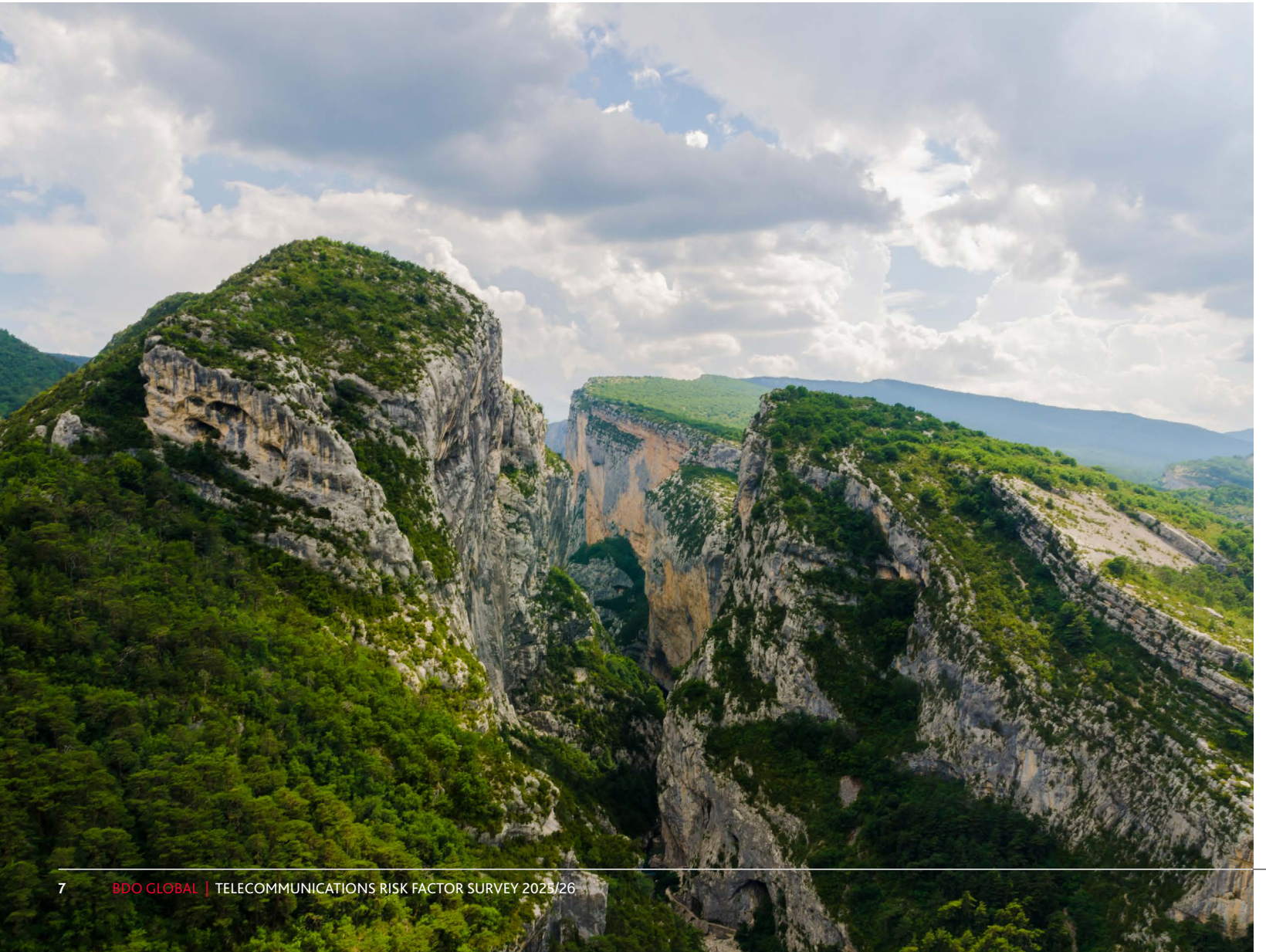
Growth in 2025

Both the telecommunications as well as the digital infrastructure sectors continue to evolve in response to rapid technological and geopolitical shifts. In 2025, operators globally are facing strong demand for secure, scalable connectivity driven by 5G, AI integration, and cloud services.

Spending across the sector is projected to reach US$1.9 trillion by 2027, led by 5G monetisation strategies and network upgrades.[1] Data centre growth is also accelerating, with global capacity expected to grow by 15% year-on-year in part due to demand from hyperscalers, AI workloads, and low-latency cloud solutions,[2] with CAGR projected to reach nearly 7% leading up to 2030.[3]

At the same time, operators are being pushed to build resilience into their supply chains, capital structures, and ESG compliance strategies to manage the risks identified in this year's study. The shift from reactive risk awareness to proactive risk mitigation is evident across most 2024 disclosures and mirrors broader corporate sentiment captured in BDOs "CFO Outlook 2025" where 60% of surveyed CFOs indicated that they plan to increase AI investment, and 44% noted that they will expand sustainability initiatives as a way to underscore how telco growth strategies are aligned with cross sector business priorities.[4]

Adding to the above, shifts in U.S. tariff policy in 2025 have introduced new cost pressures for telecom operators reliant on imported equipment which are yet to be fully felt, signalling that trade and supply-chain exposure will be an increasingly important theme to monitor for the rest of this year as well as in the year ahead.[5]



Methodology

The BDO Telecommunications Risk Factor Survey identifies the most commonly reported risks for telecom and data centre operators globally. Companies' FY2024 annual, integrated and sustainability reports were used as the foundation for risk data collection and analysis to ensure transparency and reliability. To provide a comprehensive view, our research also drew from other relevant sources, including reports from industry groups, regulatory bodies, and international organisations, in augmenting the findings.

In this year's edition, our analysis expanded to include 69 entities, up from 63 in 2023. These comprised 60 telecommunications operators across EMEA (32), the Americas (22), and APAC (6), along with nine data centre providers.

The addition of the nine data centres as well as three new telecommunications operators has broadened the scope of this year's findings and introduced new complexity to the comparative analysis. While this expansion naturally shifts some percentage ratings, the emphasis in 2025 is placed on understanding how the industry's identification of risk has evolved, especially in light of emerging digital, environmental and financial pressures.

As in previous editions, all risks were grouped into macro-economic and industry-specific categories – top risks were ranked globally and regionally. Additionally, 18 newly identified risks were introduced this year: 13 specific to telecommunications operators, and five unique to data centres, capturing emerging concerns around interconnections between AI, climate exposure, cybersecurity, revenue fragility, and risk transfer mechanisms.

In total, the analysis assessed a comprehensive set of 72 risk factors, with the aim of drawing out critical insights and offering a deep understanding of the current global telecommunications risk landscape.

This report is based on independent research commissioned by BDO SA from leading market research firm, In On Africa (IOA).

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

Market coverage

This year's survey covers a total of 69 entities across both telecommunications operators and data centre infrastructure providers, showcasing a wide-ranging view of the global digital connectivity landscape.

Telecommunications operators

EMEA

Total companies: 32

53.3%

Countries represented

- 3 Germany
- 5 UK
- 3 France
- 3 Belgium
- 3 Spain
- 5 South Africa
- 1 Netherlands
- 1 Switzerland
- 1 Sweden
- 1 Finland
- 1 Israel
- 1 Kenya
- 3 Middle East

AMERICAS

Total companies: 22

36.7%

Countries represented

- 12 United States
- 3 Canada
- 4 Brazil
- 1 Argentina
- 2 Others

APAC

Total companies: 6

10%

Countries represented

- 3 China
- 1 Australia
- 1 India
- 1 Hong Kong

New risk factors

A deeper lens into the evolving digital infrastructure landscape

As noted, the number of risk factors has increased to a total of 72 in 2025 as a way to take into account the evolving landscape of the industry, while also accounting for the broader macro-economic environment that is increasingly influencing strategy planning among operators. This expanded risk scope allowed for a more comprehensive view, while also ensuring that no critical risk factors were overlooked in the data analysis process. Despite the addition of these new risks, their presentation has been collated and refined in showcasing the most important risks for stakeholders to be aware of across regions.

In total 18 new risks were included, with a number being unique to data centres and worth keeping in mind as the prerogative for their contribution to the global technology revolution increases.

These included:

- **13** new risks identified across **telecommunications operators**, and
- **5** additional risks identified solely within **data centre operators**.

This expansion of the risk profile of the industry reflects a growing awareness of threats related to artificial intelligence, cybersecurity evolution, business model fragility, and internal operational vulnerabilities. As risk disclosures become more nuanced, emerging trends around governance influence, digital disruption, and ESG exposure have also featured more prominently.

TOP 7 NEW RISK FACTORS – TELECOMMUNICATIONS OPERATORS

01 5G deployment and evolution risk — 71.7%

Concern over cost overruns, infrastructure delays, and uneven commercial rollout of 5G networks amid unclear returns on investment.

02 Revenue model fragility — 70%

Risk that traditional income streams (e.g. voice/data plans) are losing relevance or stability as user demand and platforms evolve.

03 Business model innovation failure — 61.7%

Risk that telcos fail to effectively pivot to digital platforms, cloud, IoT, and service bundling models, limiting future growth.

04 Government and ownership influence risk — 61.7%

Risk that ownership structures or shareholder activism constrain strategic decision-making, particularly under geopolitical or market pressure.

05 Artificial intelligence (AI) risk — 58.3%

Concerns over ethical use, job displacement, and unintended outcomes from implementing AI in customer service, fraud detection, or network automation.

06 Geopolitical and AI-driven cybersecurity threats — 51.7%

Concerns over the growing sophistication of cyber attacks (e.g. hybrid warfare, ransomware) and increased vulnerability from digital integration.

07 Lagging in next-gen tech adoption — 50%

Risk that telcos delay or underinvest in integrating next-generation technologies such as 6G, edge computing, or private networks.

TOP 5 NEW RISK FACTORS – DATA CENTRE OPERATORS

01 Artificial intelligence (AI) risk — 77.8%

Concerns over data centre overuse due to AI workloads, rising energy use, and uncertain legal frameworks for data processing.

02 Stock market and investment volatility — 77.8%

Fluctuations in capital markets may undermine financing plans or investor confidence for infrastructure expansion.

03 Governance and ownership influence risk — 66.7%

Board dynamics, shareholder agendas, or ownership complexity could delay key investment or operational decisions.

04 Inadequate insurance coverage or risk transfer mechanisms — 66.7%

Firms are underinsured against events like cyber breaches, contract disputes, or liability claims.

05 Sales process inefficiencies threats — 66.7%

Poorly structured B2B sales pipelines or unclear SLAs may reduce competitiveness and client retention.

To ensure consistency in analysis, all telecommunications risk factors, as well as the five unique data centre risk factors, were categorised into two overarching groups:

Industry-specific risks:

These are tied to the internal operations and sector-specific dynamics of telecommunications and data centre providers. Examples include failures in digital transformation, talent shortages, evolving customer demands, and technology lag in next-generation systems.

Macroeconomic risks:

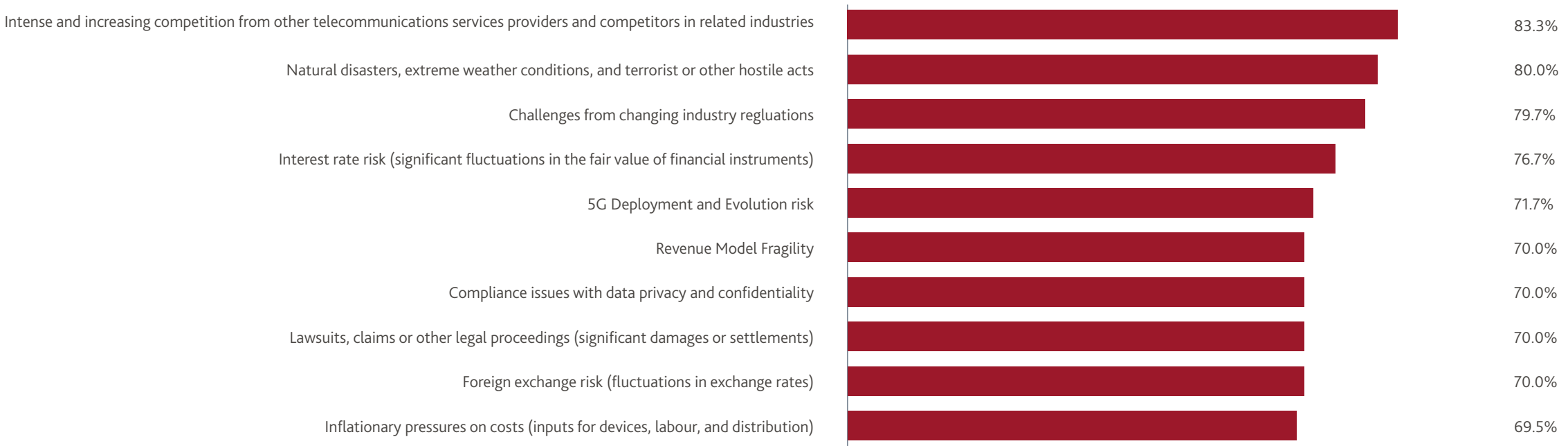
These stem from broader market, financial, geopolitical, or environmental volatility. They affect the telecommunications and data infrastructure sectors regardless of operational context. Examples include adverse financial market shifts, cyber threats, regulatory complexity, and geopolitical instability.

This classification enabled the clear mapping of how risks differ in visibility, frequency, and priority across both regions and infrastructure types.

Industry-specific risks

The 2025 risk profile for telecommunications operators reveals a sector under coordinated stress across competition, regulation, infrastructure, and financial resilience.

TOP 10 INDUSTRY – SPECIFIC RISKS



Competitive pressure

- **The fight for market share has evolved over the last 12 months with 83.3% of operators flagging intensifying competition** – particularly from digital-native and OTT entrants – while traditional service margins are being eroded, and the strategic value of core connectivity offerings is being reassessed
- Operators are increasingly expected to transition toward integrated digital solutions, bundled services, and customer-centric platforms, yet monetisation remains elusive.[6] This high-level industry pressure is acutely felt by operators in emerging markets.

Natural disaster vulnerability

- **A key development in 2025 is the elevation of natural disasters, extreme weather events, and hostile incidents to the second most cited risk (80%)** – up from a lower-tier ESG concern in 2023
- This shift points to growing real-world impacts of climate volatility on telecom infrastructure and continuity. The strategic conversation has moved from future-facing climate adaptation to immediate climate resilience, with operators recognising the operational and financial implications of outages, physical damage, and other exposure[8]
- This threat is a top priority for companies across the sector, and their internal assessments reflect a deep understanding of its potential for disruption.

Regulatory volatility

- **Regulatory volatility remains prominent (79.7%) but has been slightly outpaced by more commercially acute risks.** In 2023, regulatory complexity dominated operator concerns
- While still highly ranked, the 2025 sentiment suggests that policy turbulence, which remains elusive to an extent, is now accompanied by more urgent pressures from the competitive and financial environment
- That said, operators continue to flag the unpredictability of licensing, spectrum allocation, infrastructure mandates, and data governance as key inhibitors to long-term planning.[9]

> **"The landscape across our markets is constantly evolving due to pricing changes, competitive behaviours, and the entrance of new players, intensifying competition pressures profit margins but can benefit customers through more compelling offerings. With entrants like fintechs, we must innovate continuously to differentiate and deliver leading digital solutions for Africa's progress."**
>
> (MTN, 2024)[7]

> **"Changes to the regulatory framework under which we operate could adversely affect our business. Ongoing efforts to expand regulation of services such as broadband Internet may increase costs, intensify competition, and limit our ability to offer services in ways that maximize revenue, highlighting the uncertainty and financial risk posed by regulatory shifts."**
>
> (Spectrum, 2024)[10]

Financial fragility

- Financial fragility has emerged as a defining challenge for telecom operators in 2025, reflecting the sector's heavy reliance on capital-intensive investment
- **Rising interest rate risk (76.7%) and FX exposure (70%), both driven by global monetary tightening, are compounding the financial pressures linked to large-scale fibre and data centre rollouts.** With debt servicing costs increasing and multi-currency operations under pressure, this risk cluster signals a broader constraint on infrastructure investment momentum[11]
- BDO's "Global Risk Landscape 2025" similarly warns that excessive risk aversion can hold back growth, reinforcing the danger that cautious investment approaches in telecoms may delay critical innovation and market positioning.[12]

5G deployment and evolution challenges

- **As a new risk, ranked as the fifth most cited risk in 2025, 5G deployment and evolution risk (71.7%) reflects ongoing challenges in achieving commercial scale from infrastructure-intensive investment**
- Operators continue to struggle with balancing the high cost of spectrum, rollout delays, and uncertain timelines for return on investment
- Operators risk slower payback periods and weaker investor confidence if commercial models fail to keep pace with the speed of infrastructure spend
- Without a strong 5G backbone, adoption of emerging services such as IoT, edge computing, and AI-driven applications will stall, undermining broader digital ecosystem growth.

> **"Every time you have to cover a country with a new technology, we're talking about billions… Investors expect to make a return on their capital and so companies have to strike the right balance between investors' interests on the one hand, and not charging the end consumer luxury prices for something that is an everyday essential on the other hand."**
>
> (Cellnex, 2024)[13]

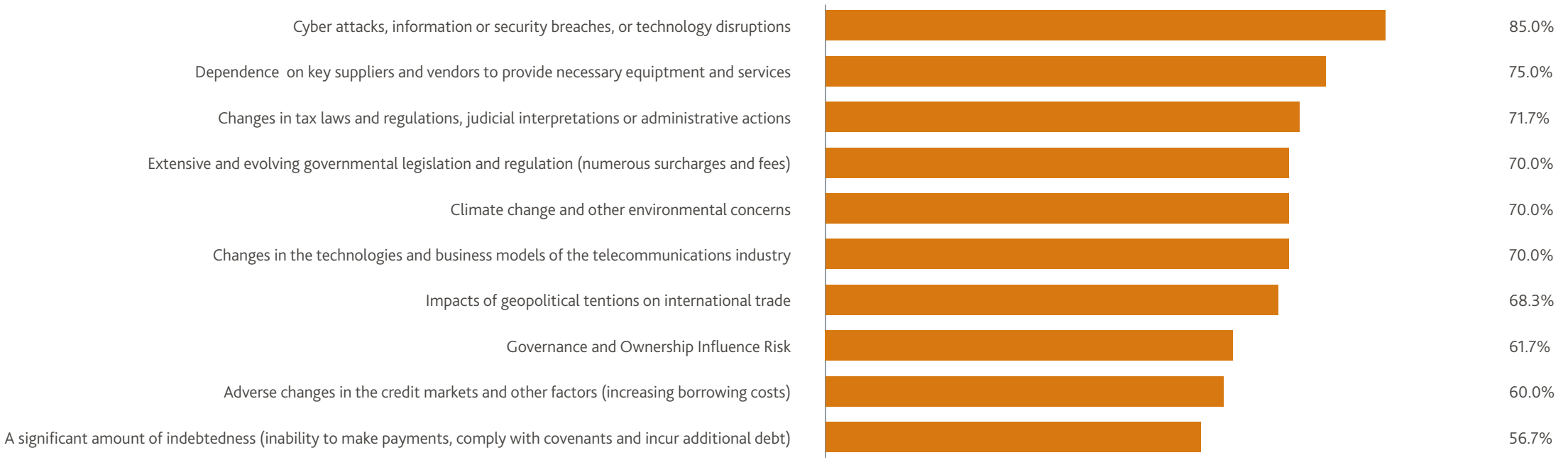
Finally, the appearance of a new core risk, revenue model fragility (70%), highlights the widening gap between traffic growth and value capture. Operators are finding that even with increasing data consumption, average revenue per user remains stagnant, and cross-selling into adjacent digital services is not yet yielding material revenue uplift. This reinforces a sector-wide challenge in creating sustainable growth beyond the core connectivity layer,[14] with fragility being driven in large part by the rise of OTT operators, whose free or low-cost messaging, streaming, and voice-over-IP services, bypass traditional telco revenue streams and intensify margin pressure.[15] Unless operators adapt business models and monetisation strategies, the growing dominance of OTTs will continue to erode value and weaken long-term competitiveness.

While not ranked within the top 10 risks by prevalence in 2025, **adjacent technological disruptions, particularly those linked to artificial intelligence, are beginning to reshape the industry-specific risk landscape.** Operators are cautiously monitoring the implications of AI-enhanced automation, predictive analytics, and content moderation challenges. These developments are expected to influence future perceptions of trust, security, and operational control, and may elevate cybersecurity back to a top-tier concern as the interplay between AI and network vulnerabilities becomes more pronounced.

Macroeconomic risks

The macroeconomic environment facing telecommunications operators in 2025 is one of heightened volatility, systemic complexity, and overlapping global shocks.

TOP 10 MACROECONOMIC RISKS



Cybersecurity vulnerabilities (general risk)

- **The most cited macroeconomic risk was cybersecurity and technology-related disruptions,** flagged by 85% of entities, making it not only the top macroeconomic concern, but the highest-ranked risk overall across both macro and industry categories
- This marks a meaningful escalation from 2023, where cybersecurity ranked among the top concerns but was overshadowed by regulatory and tax-based risks
- **In 2025, the rise of hybrid warfare tactics, and broader critical infrastructure exposure has pushed cybersecurity to the centre of strategic risk management agendas.**[16 17] The indirect effects of geopolitical conflicts, such as the wars in the Middle East and Ukraine, serve as a potent example of this, leading companies to take direct action.

Supply-side fragility

- **Supply-side fragility has emerged as a major theme, with 75% of entities citing dependence on key suppliers and vendors,** and many others noting supply chain ESG risks further down the list, operators are signalling growing concern around equipment sourcing, vendor concentration, and geopolitical entanglements that complicate access to hardware and critical components
- This is particularly pressing as network upgrades (e.g. 5G, cloud core migration) require globally interconnected procurement pathways, many of which are vulnerable to disruption[19]
- Operators that fail to diversify suppliers, build regional redundancy, and strengthen ESG due diligence in their supply chains risk exposure to cost spikes, rollout delays, and reputational damage from unsustainable sourcing practices.

Regulatory volatility

- **Taxation, legislation, and regulatory burdens remain prominent as they did previously, but no longer dominate the macroeconomic landscape as in 2023**
- Risks tied to tax law volatility (71.7%), broad regulatory expansion (70%), and international trade friction (68.3%) still reflect sector-wide uncertainty, especially in jurisdictions undergoing fiscal tightening or digital services tax reform
- Yet their relative ranking has fallen behind more operationally immediate concerns such as cyber risk and supply chain disruption. This shift suggests a recalibration in boardroom risk priorities, from policy exposure to tangible threats affecting continuity and resilience[36]
- Pillar Two is already reshaping the tax landscape, having major implications for multinational telecom operators. The OECD's 2024 Assessment of Global Minimum Tax reports 55 jurisdictions moving ahead with new tax regimes, which are already having material revenue impacts[21] – an added layer of compliance and margin pressure, particularly for telcos with complex cross-border footprints.

"**Although the 1 & 1 Group is not active in the countries involved in these wars, it is still confronted with the indirect effects. In light of the heightened cybersecurity threats associated with the wars in the Middle East and Ukraine, the Company is intensifying its investments in cybersecurity measures.**"

(1&1, 2025)[18]

"**Emerging regulations around data privacy across different jurisdictions are complicating the integration of customer data across digital assets.**"

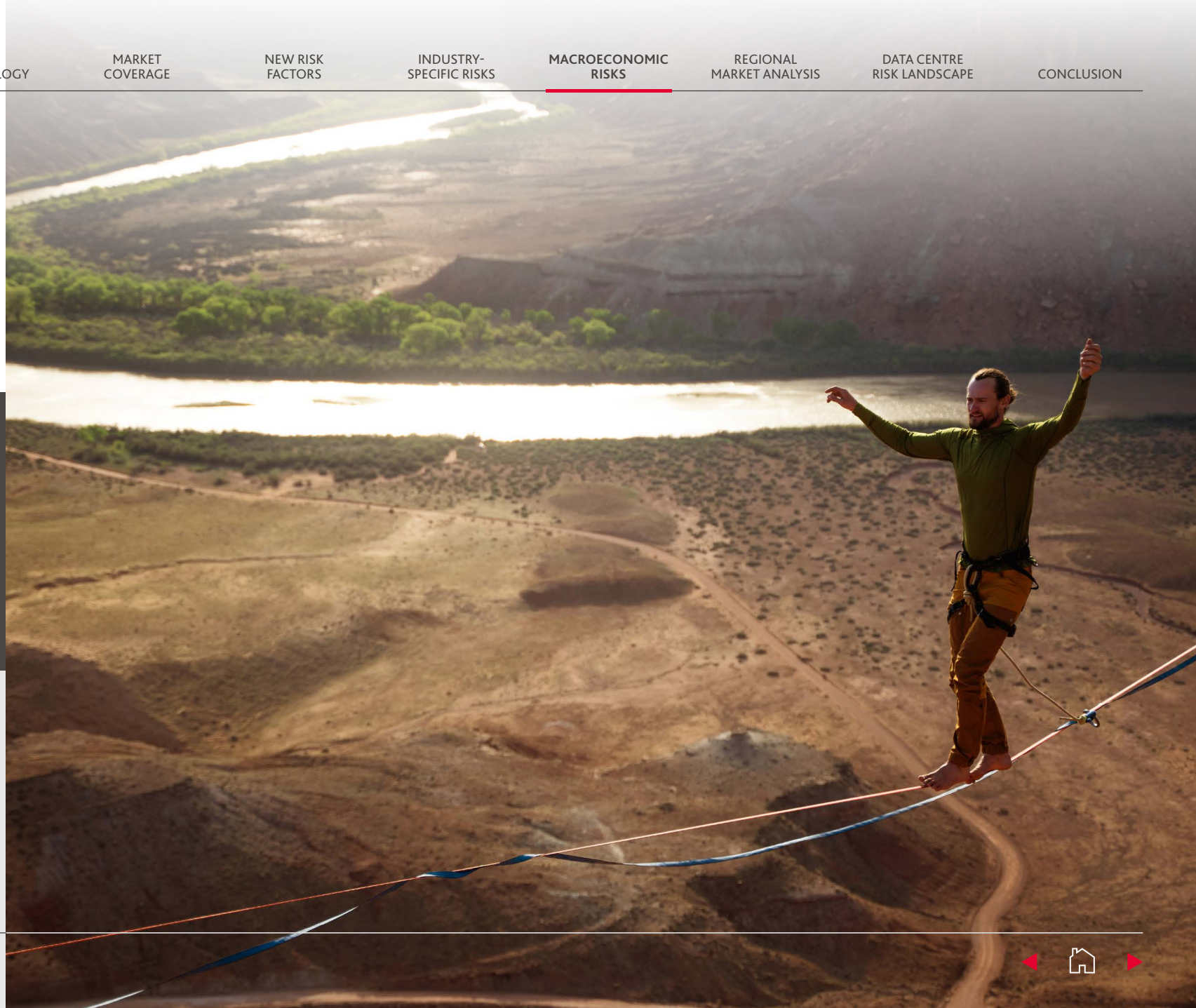
(e&, 2024)[22]

Climate and environmental risk

- Climate and environmental risks have shifted from long-term considerations to immediate operational and financial concerns
- **In 2025, 70% of operators flagged climate change, with specific references to water stress and ESG in supply chains emerging within the broader dataset**
- These issues are increasingly material to operational continuity and investor scrutiny, particularly in markets facing regulatory tightening on disclosure or carbon accountability.[23]

> **"Climate change and extreme weather events present growing operational and financial risks for Telefónica. Flooding in Spain during October 2024 disrupted services across more than 100 municipalities for up to 10 days, while droughts and flooding in Latin America caused further outages."**
>
> (Telefonica, 2024)[24]

Finally, the financial risk cluster remains a foundational pressure point. **Credit market volatility (60%), debt load risk (56.7%), and counterparty credit exposure (53.3%) reflect persistent concerns about funding models for next-gen infrastructure, especially in emerging markets.** Operators are finding it increasingly difficult to finance digital expansion at scale without encountering higher cost of capital, constrained liquidity, or balance sheet stress.[25]



Regional market analysis

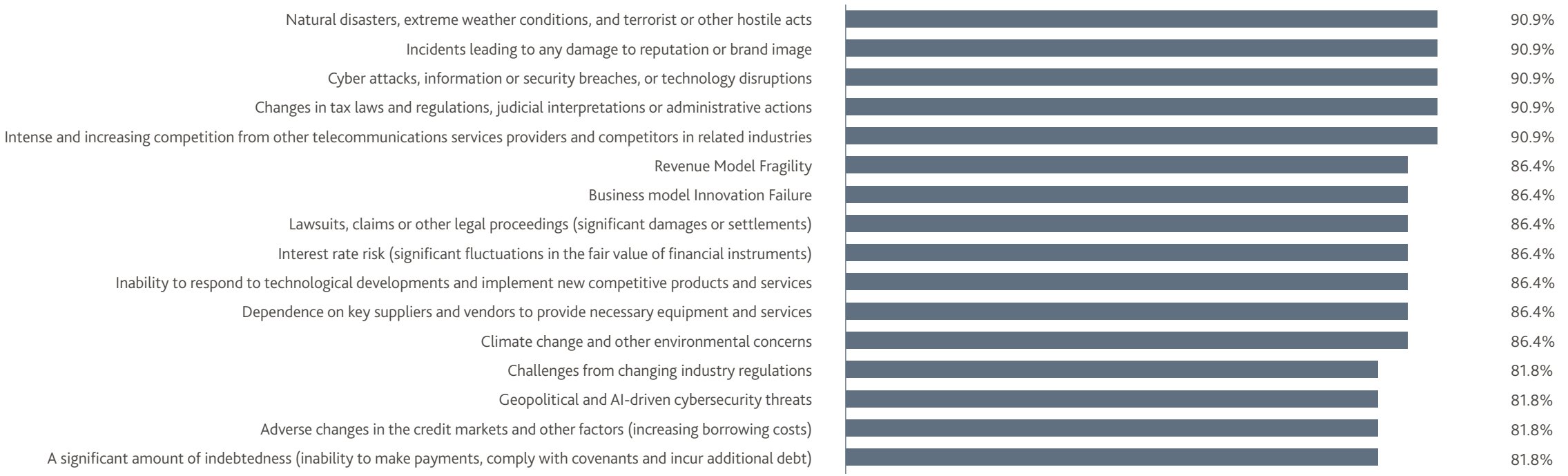
Across EMEA, the Americas, and APAC, risk intensity varies, but a common pattern emerges: a mix of macro and industry-specific risks, with cybersecurity, regulatory change, and business-model pressure being universal themes. The Americas region shows the highest overall risk intensity, with structural and legal pressures dominating. APAC's exposure is shaped by innovation volatility and climate disruption, while EMEA reflects more balanced concern across digital, legal, and financial fronts.

	Cybersecurity and digital threats	Regulatory and legal pressure	Climate and environmental risk	Revenue and business model fragility	Innovation and emerging tech disrupton
EMEA	**High** Focused on infrastructure resilience and data integrity	**High** Tax, spectrum policy and cross-border compliance	**Moderate** ESG-linked financing emerging as a key angle	**Moderate** Tied to de-industrialisation and competitive pressure	**Moderate** Uptake linked to regulation and investment gaps
AMERICAS	**Very high** Top-rated across all macro risk categories	**Very high** Multiple layers of fiscal and legal risk exposure	**Moderate** Increasingly visible, but not yet top-tier	**Very high** Flagged across multiple structural dimensions	**High** Pressure from OTTs, hyperscalers and AI uptake
APAC	**Very high** Driven by AI-integrated cyber threats and fragmented regulatory oversight	**Moderate** Uneven AI and data governance regimes creating operational uncertainty	**High** Climate volatility, energy resilience, and insurance exposure increasingly material	**High** Sustained ARPU compression, delayed monetisation of 5G and platform diversification	**Very high** AI-led transformation now a structural risk as well as a growth driver

Risk watch: Americas

Telecommunications operators across the Americas are contending with a convergence of policy instability, climate fragility, and value chain pressure. Unlike in previous years where macroeconomic volatility dominated, 2025 presented a more complex landscape: the sector's top concerns are relatively evenly spread between regulatory disruption, reputational vulnerability, environmental volatility, and strategic positioning. The common denominator is systemic risk – and a growing recognition that even historically secondary concerns now carry board-level consequences.

TOP 16 RISKS – AMERICAS



Natural disaster vulnerability

- Hurricanes, wildfires, and floods are increasingly destabilising physical infrastructure across both North and Latin America
- **Almost a quarter (22%) of mobile towers in vulnerable geographies are still not climate-hardened, and over 40% lack sustainable power alternatives** in case of grid failure
- Operators also warn that climate change can intensify water stress and disrupt supply chains, driving up resource costs and threatening energy security in markets such as Brazil
- Resilience planning must therefore move beyond compliance into asset hardening, diversified energy sourcing, and climate-adaptive infrastructure to secure operational continuity and investor confidence.

Reputational fragility

- **Once a secondary concern, reputational risk is now on par with climate competition, and cyber risk**
- Brand-damaging events – from network outages to data breaches – are rising in visibility and systemic impact across North, Central, and South America, fuelled in part by social media amplification and heightened consumer scrutiny
- In 2023, this risk didn't make the top five, but in 2025, **public perception linked to service failures, data breaches, and social accountability has made brand erosion a fast-moving concern.**[27] [28]

Cybersecurity (general risk)

- **The Americas now face the dual strain of rising threat sophistication (malware, insider ransomware) and fragmented regulatory regimes that vary across states and countries**
- Efforts to harmonise standards and invest in proactive security architecture are intensifying in response.[30] [31]

"**Exposure to natural disasters can damage facilities and infrastructure, resulting in high repair and maintenance costs. Climate change can affect water availability, increasing the business's vulnerability due to the high dependence on water sources in Brazil's energy matrix. Climate change can affect the supply chain, impacting the availability of resources and production costs.**"

(TIM Brasil, 2025)[26]

"**Our corporate reputation is susceptible to material damage by events such as disputes with customers or competitors, cyber-attacks or service outages, internal control deficiencies, delivery failures, compliance violations, government investigations or legal proceedings.**"

(Lumen, 2025)[29]

"**For example, In September 2024, we became aware that we were the subject of a cyberattack by a highly sophisticated nation-state actor known as Salt Typhoon. In that case, the threat actor was able to access portions of our network. While we were able to contain the Salt Typhoon attack, we may be unable to contain or mitigate the impacts of a significant cyberattack in the future.**"

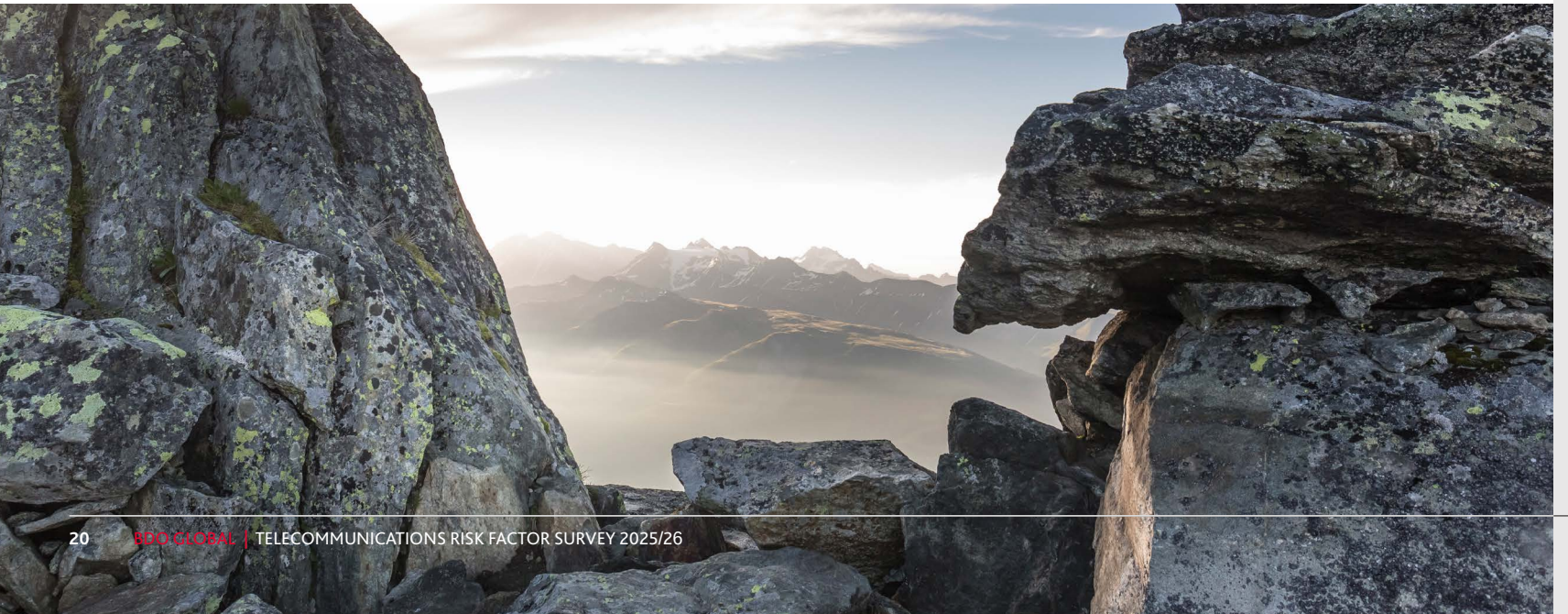
(Verizon, 2024)[32]

Regulatory volatility

- **The sharp rise in concern around regulatory and tax-related risks (90.9%) marks a return to prominence for this issue, reclaiming the top spot it last held in 2022 and overtaking cyber threats in perceived criticality**
- In countries like Mexico, Colombia, and Brazil, operators are navigating a wave of digital service taxation, retroactive regulatory changes, and unpredictable court rulings that are reshaping operating environments.[33] This environment of uncertainty poses a significant financial threat to telecommunication companies
- BDO's "CFO Outlook 2025" reinforces this context, warning that U.S federal policy shifts on trade, tax, and AI regulation remain a major source of uncertainty for growth strategies across the Americas, underscoring why regulation is seen as a top-tier risk for telecoms in the region.[34]

Competitive pressure

- **The pressure from intensifying competition has in turn remained persistently high, now flagged by 90.9% of respondents**
- Telecom operators are facing bundled service encroachment from hyperscalers, fintech-adjacent providers, and digital-native OTT platforms. These dynamics are squeezing ARPU while simultaneously raising churn management costs, especially in prepaid-dominated markets.[35] This trend of escalating competition and market convergence is a significant concern for the industry.

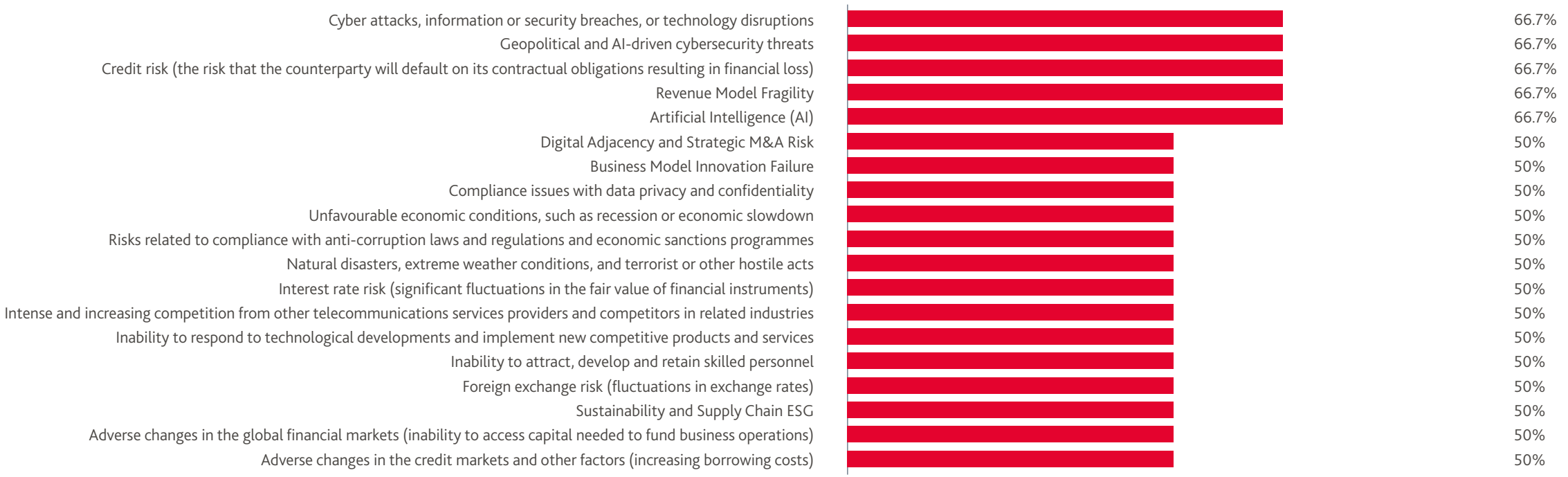


Structural fragility completes the top 10 cluster. Revenue model erosion, legal exposure, and dependence on limited supplier ecosystems all feature heavily, each cited by over 86% of operators. Legal disputes related to infrastructure damage, data mishandling, and spectrum terms are on the rise, particularly in Latin American markets with overlapping jurisdictional oversight. In parallel, operators are finding it increasingly difficult to innovate their business models fast enough to match evolving consumer expectations and digital monetisation pathways.[36]

Risk watch: APAC

Over the course of 2024, telecommunications operators across the Asia-Pacific (APAC) region navigated a shifting risk environment defined by concurrent technological acceleration and macroeconomic volatility. Cybersecurity, AI integration, and financial resilience now form a tightly interwoven triad of risk considerations, reflecting both the rapid digitisation of the region's telecom sector and the systemic dependencies this transformation has created. Unlike prior cycles, operators are simultaneously confronting technology, governance, and credit-based risks – revealing how market expansion and digital exposure increasingly move in tandem.

TOP 19 RISKS – APAC



Cyber attacks, information or security breaches, or technology disruptions

- **Cybersecurity continues to dominate the regional risk landscape**, cited by roughly two-thirds of operators surveyed, as attack volumes and ransomware sophistication intensify across hybrid and virtualised networks
- **Regulatory fragmentation across APAC** has complicated compliance for operators managing cross-border data flows, with uneven national cybersecurity standards creating operational blind spots
- **The widening attack surface from rapid 5G rollout and IoT integration** is pushing operators to adopt predictive defence systems that leverage AI-driven threat modelling and real-time detection - now seen as essential to sustaining trust and service continuity.[37]

Credit risk

- **Credit risk was flagged by 66.7% of APAC respondents,** reflecting tightening financial conditions and prolonged infrastructure payback cycles
- **Counterparty and vendor risks are intensifying**, particularly in emerging markets where smaller players rely on deferred payments or state-linked financing
- The combination of constrained liquidity and exposure to foreign exchange volatility is **forcing operators to rebalance their capital strategies**, often delaying network upgrades or pivoting toward partnership-based investment models.

Geopolitical and AI-driven cybersecurity threats

- **AI-enhanced cyber operations are amplifying geopolitical tensions**, as telecom infrastructure becomes both a strategic asset and a vulnerability
- Operators in markets such as India, Japan, and Australia are seeing **more coordinated attacks that exploit software supply chains and cloud interdependencies**, underscoring the need for defensive innovation[39]
- As BDO's "Tech Predictions 2025" notes, **AI has become the new battleground between cyber attackers and defenders**, with early adopters of predictive security systems gaining a measurable resilience advantage over slower movers.[40]

> **"The network and data security problems are showing characteristics of complexity and diversity. While the threshold for the occurrence of cyber-attacks has greatly lowered, the scale of the attacks have increased significantly. Security risks brought by new technologies and new scenes increased, and the dynamic characteristics of hybrid multicloud environments make security monitoring more complex."**
>
> (China Telecom, 2025)[38]

> **"3 Group Europe's net ARPU remained flat due to opposing forces: favourable revenue initiatives were offset by lower incoming mobile termination revenue from reduced EU-wide interconnection rates and a dilutive impact from a higher mix of low-value Internet of Things (IoT) customers."**
>
> (CK Hutchinson, 2024)[45]

> **"The cyber security threat environment has increased in scale and sophistication. Failure to effectively manage cyber security presents a material risk that has the potential to allow crime, espionage and errors to happen at an unprecedented pace, scale and reach. Telstra is currently operating in a heightened threat posture due to the geopolitical situation and increased risk stemming from global cyber security threats and events."**
>
> (Telstra, 2024)[41]

Artificial Intelligence (AI) risk

- **AI-related risks, cited by two-thirds of regional operators,** are evolving from an innovation frontier to a governance challenge as adoption expands across network optimisation, customer analytics, and fraud detection
- The region's **uneven regulatory readiness** is creating operational uncertainty, with some governments prioritising AI acceleration while others tighten oversight around ethical use and data sovereignty
- According to BDO's "Tech Predictions 2025", 2025 marks the pivot from experimentation to measurable outcomes, requiring operators to formalise AI strategies that balance deployment with accountability.[42]

Revenue model fragility

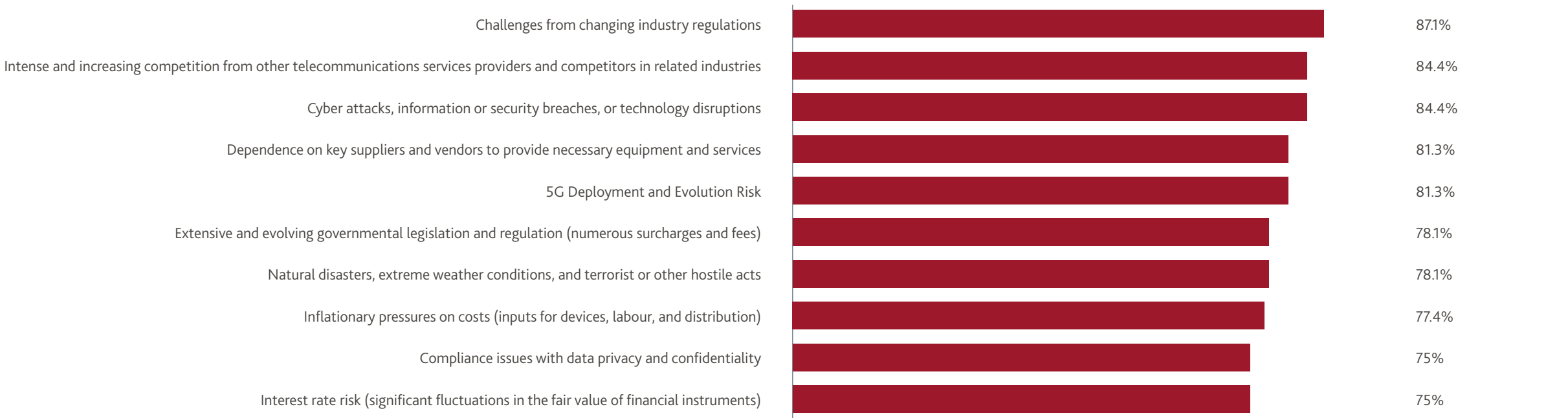
- **Revenue model fragility, also identified by 66.7% of respondents,** highlights the continued pressure on pricing and margins, even as digital demand expands
- In response, operators are pursuing **platform-based diversification,** such as fixed wireless access, cloud-hosted services, and edge computing - though monetisation remains uneven across markets[43]
- Regional data suggests that **the shift from subscriber growth to service innovation** will define the next phase of competitiveness, with data analytics, AI-enabled customer retention, and cross-sector partnerships at the core of sustainable growth.[44]

The APAC telecom environment is undergoing a **strategic pivot from reaction to reinvention**, with operators increasingly treating cyber resilience, AI governance, and balance-sheet strength as **interlocking levers of competitiveness** rather than isolated risk silos. **Two-thirds of those assessed are now reprioritising capital allocation and digital governance frameworks** to reflect this shift. Capital discipline is shaping how innovation is financed and deployed, while regulatory heterogeneity continues to challenge scalability across markets. At the same time, **emerging stressors such as rising borrowing costs, climate-linked disruptions, and talent scarcity, are reshaping operational resilience into a determinant of market leadership.**[46] Operators able to **industrialise AI securely and re-platform revenue models** (e.g., through enterprise 5G) will likely lead the region's next growth cycle; those slower to adapt risk compounding financial and reputational exposure in an increasingly AI-driven ecosystem.

Risk watch: EMEA

Telecommunications operators across EMEA navigated the 2024 landscape defined by regulatory turbulence, cyber disruption, and rising structural strain – the most significant risks are now converging. With capital deployment under pressure and competitive intensity accelerating, operators are shifting their attention from long-term growth ambitions to immediate resilience and recalibrated risk thresholds.

TOP 10 RISKS – EMEA



Regulatory volatility

- **The most pressing concern over 2024 was regulatory unpredictability, cited by 87.1% of respondents.** This reflects a marked increase from 2023, when regulation was flagged as a constraint but not at the top of the agenda
- New spectrum conditions, infrastructure surcharges, and cross-border data restrictions have raised the cost and complexity of compliance, especially in markets undergoing fast regulatory shifts such as South Africa,[47] Egypt,[48] and Poland[49]
- This environment of increasing complexity and risk is exemplified by the challenges faced by operators in adapting to stringent new data protection laws.

Competitive pressure

- **At the same level of concern is intensifying market competition.** With OTT entrants, bundling platforms, and hyperscalers entering traditional telco domains, **operators are under pressure to rethink pricing models, retention strategies, and service adjacencies**
- Margins are being squeezed, and the traditional value chain is fracturing across both consumer and enterprise markets.[51] [52]

Cybersecurity (general risk)

- **Cyber and digital security breaches are now seen as equally existential. 84.4% of operators named these among their leading concerns, matching competitive disruption as the second-most cited threat**
- The latest incident tracking shows a 20% increase in telecom-targeted events across the EU, underscoring how core networks, customer data, and trust-based services are all increasingly vulnerable[53]
- The critical nature of the threat landscape is further evidenced by specific operator data, with the focus shifting from the actual attacks to assessing external vulnerabilities.

> **"Due to new and more complex data protection legislation, in particular the General Data Protection Regulation (GDPR), which came into force in 2018, there are new, more extensive requirements for the handling of personal data, among other things. This could result in business processes no longer being able to be carried out as in the past and/or Freenet being subject to high fines."**
>
> (Freenet, 2024)[50]

> **"Our total S1 and S2 incident volumes in FY25 were down by 29%... Last year, we reported on the proportion of incidents at suppliers and third parties. In FY25, this proportion... were attackers exploiting weak credentials, social engineering, denial of service events and vulnerabilities being rapidly exploited."**
>
> (Vodafone, 2025)[54]

Supplier and vendor dependence

- **Closely related is the sector's structural fragility, particularly around its supply base. 81.3% of operators cited supplier dependence as a key risk,** underscoring concern around access to key components, geopolitical sourcing friction, and vendor concentration in high-value network assets like fibre, cloud switching, and energy provisioning[55]
- In EMEA, this dependence is amplified by vendor concentration, leaving operators exposed to cost volatility, compliance hurdles, and potential rollout delays-risks that directly threaten network resilience and long-term competitiveness.
- The challenge is compounded by regulatory fragmentation owing to varying localisation and procurement rules across EU, Middle East, and African markets, inflating costs and slowing deployment
- BDOs "Global Risk Landscape 2025" reinforces this, noting that European executives increasingly see regulatory unpredictability and compliance overspend as key inhibitors to proactive risk management, which mirrors why EMEA telcos struggle to scale efficiently under fragmented regulatory regimes[57]
- Such lack of harmonisation increases compliance burdens and rollout delays, undermining operators' ability to scale efficiently and weakening their competitive position against global peers.

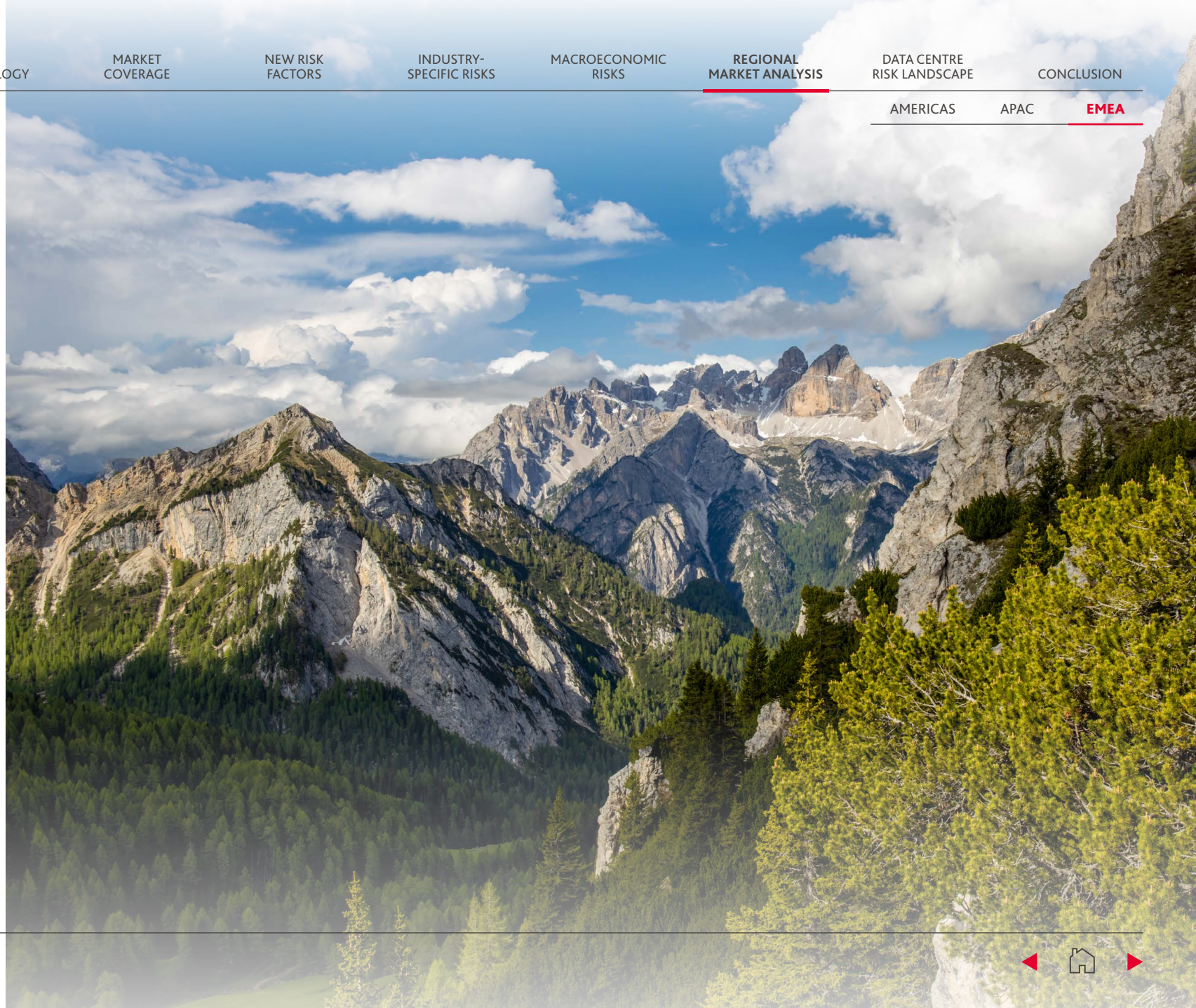
Network expansion

- Network expansion risks, particularly 5G, climb as a new risk. **Ranked fifth overall (81.3%), 5G deployment challenges now blend concerns around spectrum allocation, affordability, and cost-recovery timelines**
- With mobile traffic in EMEA forecast to triple by 2028, many operators are struggling to roll out next-gen capacity fast enough to monetise demand before costs erode returns.[58]

> **"The Directors and management are continuously monitoring and evaluating the operating environment to re-assess and appropriately adapt its strategies to ensure the continued operation of the Group into the foreseeable future. Some of the key strategies include negotiating with vendors and funders to structure long term funding options for the business commensurate with the long-term nature of the funded network equipment."**
>
> (Econet, 2025)[56]

Climate change

- **Climate-related risk has moved from long-term planning to a present operational and financial priority.** With 78.1% of operators citing natural disasters and extreme weather as an operational threat, and many linking environmental shocks to infrastructure loss, 2025 marked the point at which climate resilience became front-line
- **Asset hardening, energy-transition planning, and site-level mitigation are now core strategies, particularly in high-risk regions such as North Africa and Southern Europe.** These exposures intersect with persistent financial pressures: inflationary cost pressure (77.4%) and interest rate risk (75%) have climbed year-on-year as the aftershocks of 2023 monetary tightening continue to bite, making it harder for operators to sustain investment momentum while servicing rising debt costs[59 60]
- Company outlooks echo the challenge: sustaining investment momentum while balancing financial discipline, climate adaptation, and innovation in highly competitive markets.



Data centre risk landscape

In parallel to telecommunications operators, as the demand for digital infrastructure accelerates globally, data centres are playing an increasingly central role in enabling cloud computing, AI processing, and enterprise resilience. Their critical position in digital ecosystems exposes them to a widening array of macroeconomic, technological, and operational risks. Drawing on 2024 data from operators across markets, this section distils the top identified risks, several of which reflect the unique financial and structural profile of the data centre sector. Where relevant, it also contextualises how these risks compare and interact with trends in the broader telecoms space.

TOP RISKS – DATA CENTRES

% OF ALL OPERATIORS	100%	88.9%	77.8%		
RISK	▶ Dependence on key suppliers and vendors ▶ Inflationary pressures on costs (devices, labour, distribution) ▶ Interest rate risk (significant fluctuations in the fair value of financial instruments)	▶ Changes in tax laws and regulations ▶ Cyber attacks, information or security breaches, or technology disruptions ▶ Natural disasters, extreme weather conditions, and terrorist or other hostile acts	▶ Stock market and investment volatility ▶ Adverse changes in the global financial markets ▶ Impacts of geopolitical tensions on international trade ▶ Stock market and investment volatility ▶ Foreign exchange risk (fluctuations in exchange rates) ▶ Intense and increasing competition from other telecommunications services providers and competitors in related industries	▶ Lawsuits, claims or other legal proceedings (significant damages or settlements) ▶ Public health crises, including the COVID-19 pandemic and resulting mitigation measures ▶ Risks related to compliance with anti-corruption laws and regulations and economic sanctions programmes ▶ Uncertainty in the future cash flow and liquidity or deterioration in the capital markets (changes in credit ratings)	▶ Unfavourable economic conditions, such as recession or economic slowdown ▶ Artificial intelligence (AI) risk

Financial and structural fragility

- **For data centres, cost inflation, interest rate volatility, and supplier dependence collectively underscore a deep fragility in the financial and operational foundations of the global data centre industry**
- All three risks were flagged by 100% of surveyed operators, reflecting the dual pressures of rising construction and energy costs, and tightening debt markets
- These challenges mirror cost pressures in the telecoms sector, but are arguably more acute in data centres space given their concentrated capital cycles and power-density needs. The strain is especially evident in markets pursuing rapid AI and hyperscale cloud expansions, where construction timelines are shortening but infrastructure pricing has grown more volatile.[61]
- BDOs "Tech Predictions 2025" reinforces this trend, noting that accelerating AI workloads and hyperscale demand are reshaping energy and capital planning, adding further strain to already fragile financing models[62]
- **Macroeconomic volatility, especially linked to global capital flows and supply chain resilience, compounds the above challenges.** Disruptions tied to geopolitical tensions, vendor instability, and credit uncertainty ranked among the top-tier concerns in 2025
- These risks closely align with those flagged by telecom operators in emerging markets, particularly around trade dependencies and access to dollar-denominated financing. As a result, data centre operators are increasingly adopting diversification strategies for vendors and regional buildouts to hedge against these global uncertainties.[63]

Cybersecurity, regulatory and climate risks

- **Cybersecurity is also a structural threat, much the same as with telecommunications operators.** Flagged by 88.9% of data centres surveyed, cyber risk continues to evolve as attack surfaces expand
- With both telcos and data centres migrating to hybrid, API-driven, and software-defined environments, **shared vulnerabilities are becoming more pronounced.** The data centres assessed in this report highlight this as an ongoing risk, with some also noting mitigation strategies
- Data centres also face heightened reputational exposure due to the volume of third-party data they hold. Investment in zero-trust architectures, AI-based detection, and physical-layer isolation continues to grow as mitigation responses.[65]

> **"We depend upon third-party suppliers for power and we are vulnerable to service failures and price increases by such suppliers and to volatility in the supply and price of power in the open market. Many factors, including global economic conditions, may cause our customers to experience a downturn in their businesses or otherwise experience a lack of liquidity, which may weaken their financial condition and impact our estimates as to the probability of collectability of payments..."**
>
> (Digital Realty, 2024)[64]

> **"Cyber threats and attacks are increasing in number and sophistication and continually evolving, particularly with the expanding availability of AI and generative AI tools and technologies, making it more challenging to defend against certain threats, attacks and vulnerabilities that can persist undetected over extended periods of time."**
>
> (Kyndryl, 2025)[66]

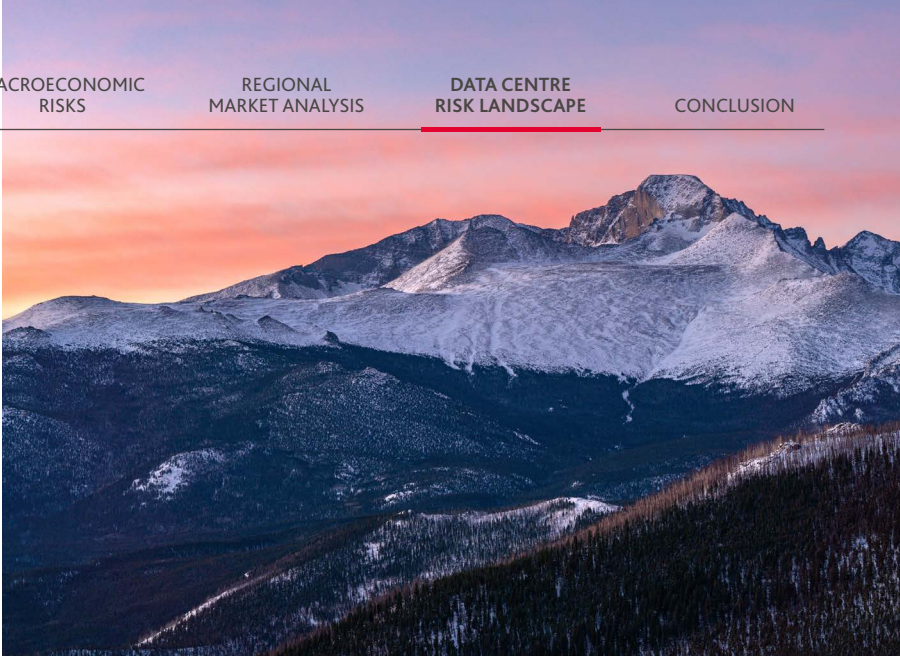
Environmental fragility

- **Environmental fragility, especially in the form of climate volatility and physical infrastructure exposure, is also at the top of the agenda for data centre operators**
- An increasing proportion of data centre operators are citing extreme weather and natural disasters as critical threats to uptime. While this mirrors patterns observed in the telecom space, the impacts on data centres are magnified due to their stationary power profiles and site specificity. **Emerging approaches such as modular cooling systems, green redundancy, and disaster-tolerant campus design are helping shift the risk profile**[67]
- Beyond physical risk, data centres face mounting reputational scrutiny over electricity use, grid strain, and cooling-water demand. As AI workloads surge, operators' energy and water footprints are becoming focal points for ESG-minded regulators, investors, and communities. New disclosure regimes in key markets (e.g., energy-efficiency and water metrics, renewable share, energy-reuse) are raising transparency and accountability, increasing the reputational stakes for operators
- By being transparent about energy and water use at a site level, operators and investors can gain trust and secure permits more easily. A lack of transparency often leads to backlash, higher costs, and project delays.[68]

Competitive pressure

- **Newly surfaced risks tied to investor confidence and client concentration present unique structural vulnerabilities for data centres.** With many facilities anchored by a small number of hyperscale tenants, even minor fluctuations in demand or contract terms can disrupt revenue stability
- **Furthermore, market sentiment toward digital infrastructure REITs and green asset qualification is influencing funding dynamics.** These risks remain less pronounced in telecoms, where revenue is more dispersed across millions of end users
- That said, the implications for long-term financial strategy are material and growing.[69] This financial fragility, particularly its connection to market sentiment and investor confidence, is explicitly addressed by key data centres in the sector.

> **"The trading prices of our ADSs and ordinary shares may fluctuate significantly, which could lead to substantial losses for investors…The market price and trading volume of our shares could decline. The distinct characteristics of the capital markets in Hong Kong and the U.S. may negatively affect the trading prices of our ADSs and ordinary shares."**
>
> (GDS Holdings 2024)[70]



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[71] ▶ AI-enabled threat detection systems embedded in core platforms[72] ▶ 24/7 cyber operations centres for incident response[73] ▶ Secure-by-design protocols applied across new product lifecycles.[74]	▶ Formation of Board-level ESG governance and compliance structures[75] ▶ Integration of ESG reporting into annual risk disclosures[76] ▶ Enterprise-wide regulatory horizon scanning and reporting mechanisms.[77]	▶ Adoption of modular infrastructure to reduce upfront capital outlay[78] ▶ Refinancing and restructuring of legacy debt portfolios[79] ▶ Increased internal cost-efficiency programmes tied to regional priorities.[80]	▶ Launch of regionalised net-zero targets and scenario testing[81] ▶ Deployment of solar arrays and renewable backup systems[82] ▶ Energy efficiency programmes focused on emissions and operational resilience.[83]	▶ Supply chain localisation and diversification through regional sourcing initiatives[84] ▶ Inclusion of multi-tier supplier certification and ESG audits[85] ▶ Increased transparency in supplier engagement through regulatory filings.[86]

Conclusion

The 2025/26 Telecommunications Risk Factor Survey illustrates an industry that has shifted decisively from awareness to action. Operators are no longer just cataloguing risks; they are embedding mitigation into the heart of strategy, governance, and operations. From zero-trust cybersecurity frameworks to modular infrastructure and ESG-aligned financing, the interventions captured in this report show a sector recalibrating for resilience in real time. The 'so what' is clear: risk management has become the new competitive frontier, separating firms that can adapt and sustain growth from those that remain exposed and fragile.

At the same time, the findings highlight that risks are increasingly interconnected and cascading – financial fragility amplifies operational weakness, while climate volatility magnifies supply chain and cyber exposure. This convergence means isolated approaches are no longer sufficient. For stakeholders, the true significance is recognising that it is not merely infrastructure at stake, but the trust of billions who depend daily on secure connectivity. The ability of telecoms and data centres to anticipate, absorb, and adapt to systemic risk will directly shape economic resilience, digital inclusion, and social stability in the years ahead. In this sense, risk mitigation is not merely defensive – it is the foundation for sustainable progress, allowing the sector to deliver on its promise of connecting people, businesses, and societies in an increasingly uncertain world.

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