GSMA

01



Futureproofing Connectivity

Executive summary and recommendations

Copyright © 2026 GSMA

November 2026

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **gsma.com**

Frontier is a strategic consultancy with an economics lens. We aim to deliver not just great analysis but the best possible outcomes for clients. To do that, we combine cutting-edge technical skills with a human way of working – bringing things like emotion, challenge, ambition, conviction, and a sense of fun. We help clients get things done well.

www.frontier-economics.com

Acknowledgements

This report has been developed by the GSMA with Frontier Economics.

The GSMA would like to thank members of the GSMA Climate Action Taskforce, Regulators, Network Equipment Manufacturers and Insurers whose expertise and valuable insights helped to shape this report series.

Copyright © 2026 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Futureproofing Connectivity

This is the first report in a six-part series 'Futureproofing Connectivity: Climate Risk and Resilience in Telecommunications'. This collection of research identifies weather-related risks that telecommunications networks face, the associated financial impacts of these risks and what is needed to strengthen the resilience of networks in a changing climate.

By quantifying exposure to climate risk and showcasing best practices in network resilience, the research provides guidance for operators on climate-related planning, investments and reporting. The overarching goal of the series is to align the sector more closely and help prepare telecommunications networks for the impacts of a more volatile climate.













→ You can explore the other reports in the series **here**.

Report series structure

This research is split over a six-part series 'Futureproofing Connectivity: Climate Risk and Resilience in Telecommunications'

01
Executive summary and recommendations

Describes the research approach, key findings and provides practical recommendations for operators, policymakers, regulators, suppliers and investors to strengthen the resilience of telecommunications networks to the impacts of climate change.

02
Weather-related risks and impacts on telecommunications networks

Identifies acute and chronic weather-related risks and associated restoration costs that can affect telecommunications networks and maps these risks to different types of network infrastructure. This includes direct risks to mobile and fixed access networks, core networks, data centres, towers, backhaul, transport links and other supporting infrastructure. It also considers the sector's exposure to indirect risks and interdependencies, such as power supply and other critical systems.

03
Legal, regulatory and voluntary frameworks shaping network resilience

Assesses the resilience and adaptation obligations that telecommunications companies are expected to meet. These include telecoms-specific network resilience requirements, critical infrastructure obligations, corporate governance and risk management frameworks and climate-related reporting and disclosure frameworks.

04
Assessing weather- and climate-related risks

Reviews how operators currently assess risk. It covers the tools, methods, data sources, models and internal governance arrangements they use, together with the variables they need to understand the financial impact of physical climate risks and the cost of building resilience.

05
Prevention, response and recovery practices

Examines how operators respond to and manage weather-related risks in practice. This includes how resilience is embedded in network design, maintenance and renewal; the measures taken to reduce vulnerability and maintain service; how operators prepare for, respond to and recover from severe weather events; and how they manage the residual risks and financial impacts that cannot be fully prevented.

06
Annexes

Explains the methodology behind the modelling used to estimate infrastructure repair and replacement costs, and estimated telecommunications outages under current and future climate conditions. The inputs, sensitivities, assumptions and limitations are detailed, so that operators might use the approach in their own climate risk assessments.

Executive Summary



Climate change is increasing the scale of weather-related risks that mobile network operators face. Maintaining current levels of connectivity will become increasingly challenging as repair and replacement costs for damaged infrastructure grow. However, there are several ways for operators to assess and report weather-related risks more consistently and systematically, and to strengthen the resilience of their networks. This research offers these recommendations to operators, public authorities and other affected stakeholders.

Severe weather repair costs are already significant and will continue to grow

New modelling undertaken for this research finds that, globally, infrastructure repair and replacement for cell sites following severe weather events (storms and floods) currently cost mobile operators $1.7 billion a year. This is estimated to increase to $3.1 billion a year by 2050 under projected climate conditions. These costs are equivalent to around 1% of current global mobile operator capital expenditure (CapEx), and are estimated to increase by 80% based on projected mid-century climate conditions.

Severe storms account for more than half ($1 billion) of the total estimated costs associated with severe weather events, with riverine and coastal floods accounting for 34% ($577 million) and 7% ($124 million), respectively. Severe storms are also the fastest-growing source of risk, increasing from 59% of estimated costs today to around 76% under projected mid-century climate conditions.

Costs extend beyond repair to include wider social and economic impacts

The total costs of extreme weather arising from the climate crisis are expected to be much higher. The modelling includes the repair and replacement costs from damage to mobile tower infrastructure, but it does not quantify damage to fixed networks or the effects of hazards such as wildfire, surface flooding and extreme heat. Nor does it capture all the knock-on costs, such as higher energy and cooling requirements, service restoration, customer compensation, lost revenues, reputational impacts or rising insurance costs. Therefore, these should be viewed as conservative estimates of potential costs.

Weather-related disruption also affects the users and services that depend on telecommunications networks. In more than 50 countries between 2022 and 2024, there were, on average, about 150 telecommunications outages a year that directly coincided with a major storm or flood in the affected region. GSMA estimates suggest that these severe weather-related outages directly affected just under 215 million telecommunications service users globally per year.[1] Based on projected mid-century climate conditions, the number of outages is estimated to rise to around 170 per year and affect approximately 280 million telecommunications service users every year.[2]



1 Between 2022 and 2024, there were 450 outages affecting 640 million users.
2 These estimates are indicative and assume that weather-related outages change in proportion to the modelled change in climate-related physical damage to mobile infrastructure.

Network resilience requires a whole ecosystem approach

Access networks that provide the “last mile” of connectivity to a cell tower, or connectivity from the cell tower to the handset, are generally the most exposed part of the network. Network resilience depends not only on the robustness of physical infrastructure, but also on effective network planning, redundancy, operational preparedness, business continuity arrangements and coordination with other infrastructure providers.

For example, severe weather affects power supply to telecommunications networks. Operators report that, in many cases, weather-related network outages are not caused by damage to network equipment but by interruptions to power supply. Resilience therefore requires a whole ecosystem approach, from equipment vendors and power providers to public authorities and emergency services.



Enhanced geographic modelling would help operators manage future risks

Operators have long managed physical, operational and cyber risks that could affect network availability, performance and functionality. Many measures that improve general network resilience to physical risks (accident, earthquake, damage) or other risks (such as cyberattacks) also improve resilience to weather hazards.

Despite the growing risks associated with climate change, operators are at different levels of maturity when it comes to assessing and planning for future risks. While 97% of mobile operators surveyed for this research had undertaken resilience programmes to strengthen their networks, only 21% (for vegetation management) to 41% (for backup power maintenance) reported that these programmes were designed specifically with climate change in mind.

Less mature approaches tend to rely on historical incidents, local knowledge and judgement. More advanced approaches also incorporate geographic risk modelling, combining geo-datasets of asset inventories, severe weather forecast models and scenario analysis.

However, our research found that operators face several barriers to conducting risk assessments. For example, they may lack data on the location of some assets (especially if they do not own the assets), have limited access to weather hazard data, lack the knowledge and specialist data skills to interpret and analyse climate models. This makes a quantitative or financial assessment of risk much harder to undertake.

Forward-looking resilience needs to be coordinated across operator functions

To improve resilience, operators need to ensure that climate risk assessment influences operational and investment decisions. However, internal barriers can make it difficult to share information effectively. Sustainability and environmental, social and governance (ESG) teams often lead climate-related disclosure, while network operations, engineering, finance, enterprise risk, procurement and regulatory teams each have relevant evidence that contribute to a risk assessment. Coordinated internal leadership is needed to ensure that weather-related risk analysis is not only used for reporting but also informs network planning.



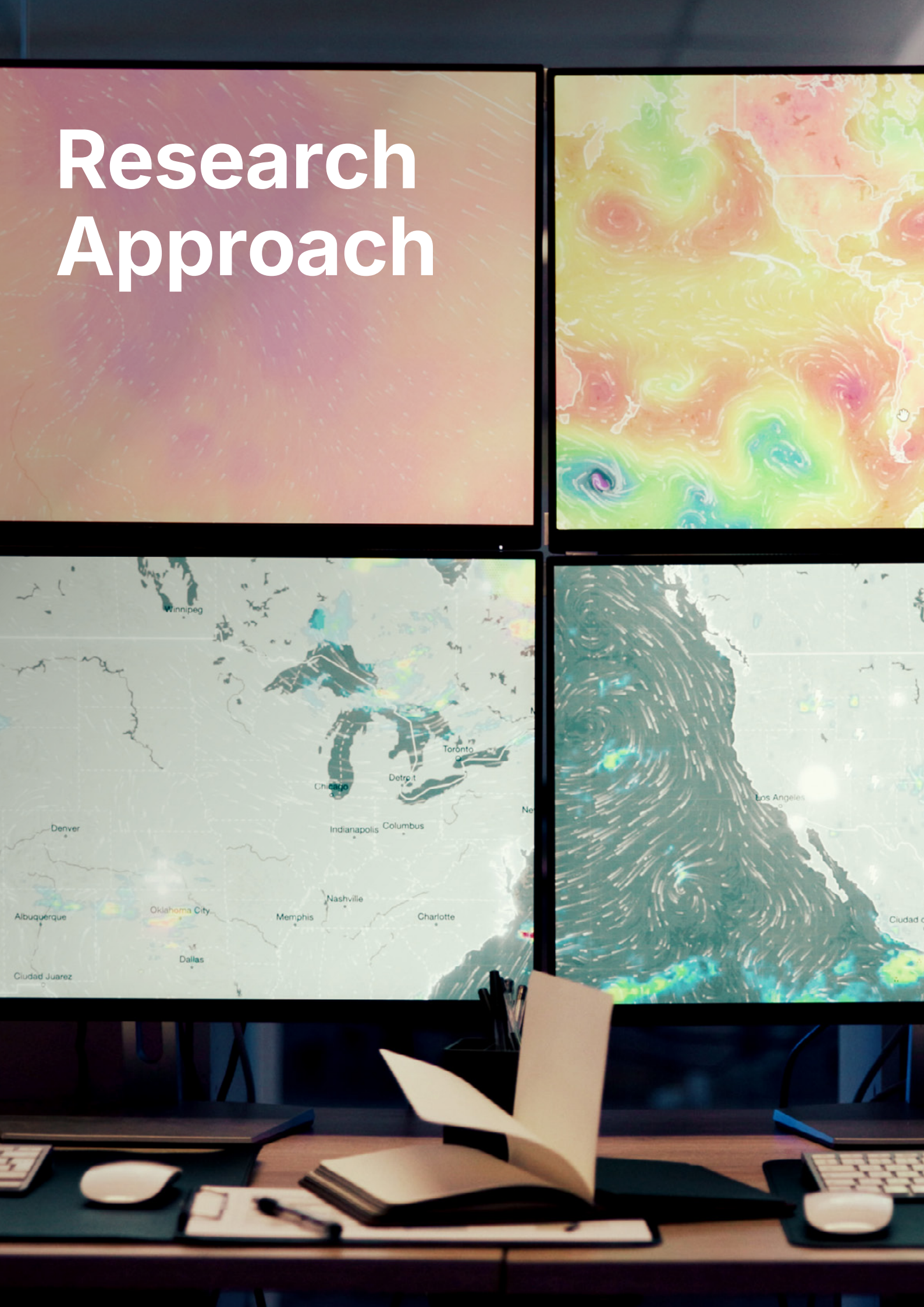
The regulatory and reporting landscape for climate resilience is complex

Mobile operators may be subject to telecoms-specific resilience and outage reporting rules, critical infrastructure obligations, disaster management requirements, corporate governance duties, climate-related financial disclosure rules and voluntary market-led reporting frameworks. These frameworks have different objectives:

- Telecoms and critical infrastructure rules tend to focus on service continuity, incident response, emergency communications and public safety.
- Climate disclosure frameworks tend to focus on governance, materiality assessments and financial exposure, and reporting for investors and other stakeholders.
- Corporate risk management frameworks provide the internal processes through which risks are owned, escalated, funded and monitored.

These frameworks can reinforce each other, but they can also duplicate efforts. A key issue for the sector is how to align reporting and resilience obligations so that they support practical network resilience without creating unnecessary administrative burdens.

Research Approach



Purpose of the research

This report series identifies weather-related risks that telecommunications networks face, the associated financial impacts of these risks and what is needed to strengthen the resilience of networks in a changing climate. By quantifying exposure to climate risk and showcasing best practices in network resilience, the research provides guidance for operators on climate-related planning, investments and reporting. Ultimately, this research seeks to align the sector more closely and help prepare telecommunications networks for the impacts of a more volatile climate.

Scope of the research

The research focuses on weather-related physical risks affecting mobile telecommunications networks. It covers both short-term risks, such as current and near-term weather-related disruptions, as well as longer-term risks that may affect network planning, asset design, investment cycles and resilience strategy.

Non-climate-related natural hazards, such as earthquakes, are outside the scope of the research. Transition risks, such as changes in carbon pricing, energy policy or decarbonisation regulation, are also not the primary focus except where they influence physical resilience, for example, through power supply, energy efficiency or backup power arrangements.

Methodology

The research draws on a combination of desk research, case studies, stakeholder interviews, a survey of mobile operators and new economic modelling.

Desk research was used to review evidence of weather-related risks (including examples of disruptions), telecommunications resilience frameworks, regulatory obligations, voluntary submissions to climate disclosure frameworks and public reporting (for example, in annual reports or stand-alone climate reports).

Fourteen targeted interviews were conducted with operators and other relevant stakeholders to understand current practice, examples of resilience building and practical barriers to more effective resilience. These interviews helped validate the desk research, add operational context to the analysis and inform eight country case studies,[3] which systematically examined how climate hazards, regulatory frameworks and operator responses vary across different countries and market contexts.

Twenty-nine operators responded to a survey designed to gather structured evidence on each of the research objectives.

The research also draws on insights gathered from more than 20 mobile operators that attended the GSMA Climate Action Forum in June 2026. This provided an opportunity to test emerging findings with operators and identify common challenges across the sector.

Finally, the research includes modelling of the nature and scale of costs associated with severe weather hazards affecting telecommunications networks, together with an assessment of how these costs may change over the coming decades. The modelling relies on publicly available data on asset locations, weather hazards and infrastructure costs, as well as asset vulnerability relationships (sourced from economic literature, as described Report 6, Annex 1).

3 Case studies were conducted for The Bahamas, Bangladesh, Chile, Kenya, South Africa, Spain, Türkiye and the United States.

Recommendations



Recommendations for operators

Use modelled projections for severe weather and future risk scenarios to embed resilience by design

Forward-looking risk assessments should inform decisions with long-term consequences, including site selection, network design, asset renewal, technical standards, procurement and capital allocation. Operators should use intermediate climate scenarios for planning and higher-end scenarios for stress testing, rather than treating any single climate scenario as a forecast. The time horizon should reflect the expected life of the relevant assets and decisions. Operators may need to build internal capacity (technical expertise and IT equipment) to ensure they have access to the weather forecasts relevant to their networks.

Establish clear senior accountability and cross-functional governance for resilience

Operators should ensure they have clear senior accountability for weather-related resilience within their organisation. This will ensure that management information and resources are available to assess and record risk, and that information collected for climate reporting is reflected in operational and investment decisions. The same risk analysis that informs network planning should also be used for reporting.

Measure financial exposure and compare resilience options on a total cost basis

Operators should also improve the information that is recorded and collated on the financial consequences of weather risk, including repair and restoration expenditure, outage duration and user hours lost, additional operating expenditure and the costs of resilience measures. This will allow resilience options to be compared on a total cost basis, including the losses they are expected to avoid.

Treat network resilience as a cross-sector responsibility

Operators should plan and test resilience across the wider ecosystem. To improve resilience, operators should engage with other stakeholders, such as other network operators, infrastructure providers, suppliers and public authorities. They should agree on roles, escalation routes, information-sharing arrangements and restoration priorities with infrastructure partners and public authorities before major weather events occur. Exercises and post-incident reviews should test the full cycle of predicting and preparing for disruption, responding, recovering and rebuilding more resiliently where appropriate.

Recommendations for policymakers and regulators

Set proportionate, outcomes-based resilience requirements

New resilience frameworks should be developed through early consultation with operators and affected infrastructure providers. Any frameworks for resilience that include service continuity or public safety should be defined in close consultation with operators, giving them the flexibility to select the most appropriate measures to deliver the outcomes. Operator-led frameworks can be implemented more quickly, are more flexible and risk based, and will be more cost-effective.

Major incidents can be opportunities to reveal genuine gaps, which enable operators to improve resilience. Having more flexible frameworks allow any new learnings and targeted measures to be more easily incorporated in consultation with operators, rather than as a reflexive response to severe weather events.

Reduce duplication across resilience and reporting frameworks

Authorities should align definitions, metrics, time horizons and reporting formats across telecommunications, critical infrastructure and climate-related requirements wherever possible. Evidence already collected for one legitimate regulatory purpose should be reusable for others, subject to confidentiality and security safeguards.

Remove barriers to effective response and restoration

Public authorities should establish coordination arrangements with electricity and fuel providers, emergency services and other infrastructure providers. This should include priority restoration for critical telecommunications sites, temporary permitting and deployment arrangements, and prioritising access to critical sites, transportation and fuel and power to enable operators to maintain essential communications during major disruptions.

Recommendations for suppliers

Make infrastructure dependencies more transparent

Infrastructure partners should provide operators with sufficiently detailed information on asset location and condition, design limits, backup arrangements, dependencies, maintenance responsibilities and restoration constraints. This is particularly important for leased and shared infrastructure where operators currently have less visibility.

Equipment suppliers should also provide clear information on operating thresholds and expected performance under relevant future conditions and continue to improve energy efficiency and thermal tolerance where these can increase both resilience and operating efficiency.

Copyright © 2026 GSM Association