GSMA

04



Futureproofing Connectivity

Assessing weather- and climate-related risks

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 fourth 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.

Effective governance for resilient networks

Weather-related risks are already considered by all operators as part of day-to-day network operations, incident response and business continuity planning (BCP). However, the integration of forward-looking climate risk into strategic planning, capital allocation and external reporting is less consistent.

Functions responsible for assessing and responding to weather-related risk

Weather-related risk cuts across several parts of an operator's business. Immediate disruption is primarily an operational issue, but the same hazards can also affect long-term network design, capital allocation, financial exposure, regulatory compliance and climate-related reporting.

- **Network operations teams** manage real-time incidents, service monitoring, alarms, restoration and field force mobilisation.
- **Sustainability and ESG teams** typically lead climate-related disclosure, scenario analysis and responses to reporting frameworks such as CDP, TCFD, ISSB and CSRD.
- **Network planning and engineering teams** determine site design, equipment standards, route diversity, backhaul architecture, backup power and longer-term network upgrades.
- **Enterprise risk and finance teams** assess materiality, maintain risk registers and consider insurance, capital planning and wider financial exposure.
- **Regulatory, legal and public policy teams** manage incident reporting, compliance with licence and legal obligations, emergency communications requirements and engagement with public authorities.
- **Procurement and supplier management teams** manage dependencies on tower companies, electricity providers, fibre providers, contractors, fuel suppliers and equipment vendors.

Operators noted that teams within the same organisation can use different terminology, evidence and time horizons, creating two common disconnects:

- Sustainability teams may request information from network teams for disclosure purposes, but the resulting analysis may have limited influence on operational or investment decisions.
- Network planning and engineering teams may rely heavily on historical experience, existing technical standards and observed network performance. These approaches support resilience to current weather conditions but may not fully incorporate forward-looking assessments of how hazard frequency or severity could change over the life of an asset.



Case Study

Long-term risk evidence must inform near-term investment decisions

Interviews identified a common governance challenge with the time horizons used to assess risks and make decisions on resilience investments.

Interviews with Axa Climate and operators highlighted the risk of a gap between teams that assess long-term climate exposure and teams that approve near-term network expenditure.

An operator from Sub-Saharan Africa seeks to reduce this gap by involving technology, supply chain and finance teams from the outset and using workshops to test whether modelled risks reflect operational experience.

Case Study

Enterprise risk management frameworks can facilitate decision-making on resilience

MTN reported that it manages resilience through a governance model that connects operational accountability with strategic oversight. Day-to-day responses to weather-related disruptions are led operationally by its network teams, supporting the rapid restoration of services when incidents occur.

Where resilience risks have broader or longer-term implications, they are considered through its enterprise risk management processes, bringing together local market insights and relevant group sustainability, technology and risk functions. This integrated approach enables operational resilience challenges to inform executive decision-making, long-term planning and, where appropriate, board-level oversight.



Case Study

Combining common group inputs with local decisions

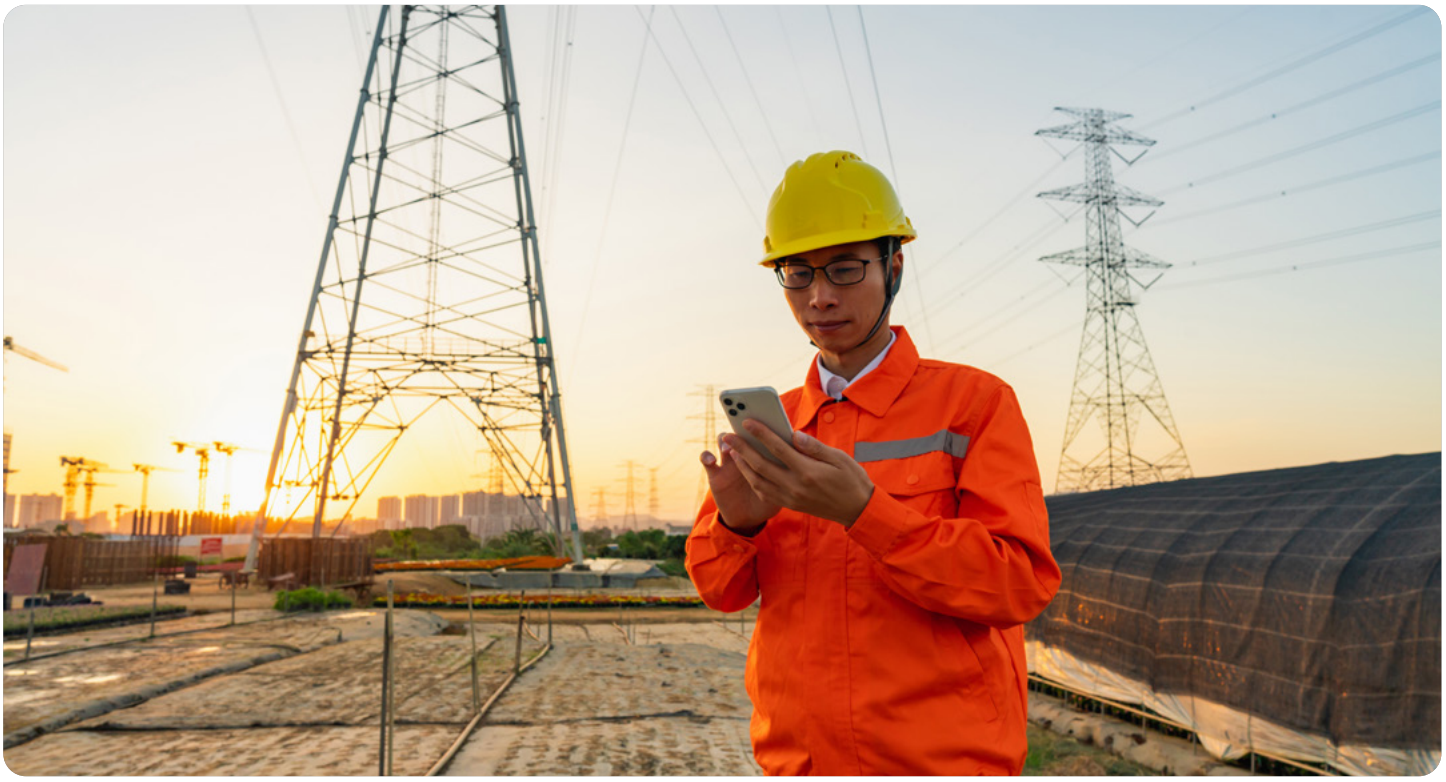
Operators can standardise climate evidence and methods while retaining local accountability for asset assessment and investment.

One European-headquartered operator has established a group-level climate adaptation programme led jointly by its sustainability and enterprise risk functions. The central team coordinates the programme and provides common inputs, including forward-looking climate data for 2030, 2040 and 2050.

A cross-functional community bringing together representatives from risk, environment, innovation, finance, business continuity, technical functions and human resources.

Another European operator combines central coordination with local accountability. Its group head office function provides common climate data and offers defined methodologies that can be used for all its country operators to assess weather-related risk.

Each country operator is responsible for assessing asset vulnerability, developing the business case and deciding whether to fund adaptation through local budgets. Decisions on whether to invest in adaptation measures, and the associated expenditure, currently remain within country budgets.



Managing accountability across disparate teams

No single team holds all the information or decision-making authority needed to manage weather-related risks effectively. Assessing, reporting and acting on these risks therefore needs to be led from the top with clear ownership. Operators noted that best practice governance has:

- A board-level executive with oversight and responsibility
- Clear decision rights
- Common terminology
- A process for reconciling short-term operational priorities with longer-term climate horizons

External datasets can provide a common reference point, but operators also need an agreed method for validating them against local evidence and engineering judgement.

Climate transition planning provides a framework to apply mitigation and adaptation

Transition planning frameworks recognise the complementary nature of mitigation and adaptation actions. Investments that can reduce GHGs by using more efficient infrastructure can also be integrated with planning to boost resilience to severe weather. Transition planning (for example, as set out in the GSMA's Climate Transition Planning Guidance for Telecommunication Companies) provides a strategic framework for identifying risks and how they will be addressed.

The guidance recommends executive sponsorship, clear ownership across functions, cross-functional teams (engineering, operations, procurement and sustainability) and board oversight of physical and climate risks.[1] The Transition Guidance encourages operators to record climate risks and mitigation investment as CapEx and OpEx items within their financial planning.

1 GSMA. (October 2025). Climate Transition Planning Guidance for Telecommunication Companies, pp. 53–55.

Coordination between operators and other stakeholders

Operators remain accountable for maintaining and restoring telecommunications services, but they do not control all the infrastructure and resources on which those services depend. Weather-related outages may be caused by the loss of electricity, blocked roads, unavailable fuel, damaged third-party fibre, limited site access or delays in obtaining spare equipment. The vulnerability of operator equipment to severe weather also depends on equipment specifications, which are controlled by the equipment vendors.

Network resilience is an ecosystem outcome

Nokia's research with the Clinton Global Initiative (CGI) found that resilience challenges are often driven by gaps in coordination, preparedness and shared situational awareness, rather than the network infrastructure itself.

In response, Nokia is helping to co-create ecosystem approaches that combine elements such as hyperlocal weather intelligence, resilient connectivity and cross-sector collaboration.

Nokia is also working with a European telecommunications operator that has experienced significant weather-related disruptions to explore what an end-to-end resilience ecosystem could require, from technology to public safety coordination, community training, preparedness and crisis communication.

Nokia aims to help communication service providers (CSPs) respond to government, technology and reputational pressure in a holistic way, with citizen resilience their ultimate goal.

Coordination between operators and other stakeholders is needed in four practical areas:

1. **Information and early warning.** Some operators obtain warnings from meteorological agencies and civil protection bodies, and use them to prepare field teams, suppliers and temporary equipment. During an incident, operators and infrastructure providers may also need to exchange information on affected sites, power outages, access constraints, fuel availability and expected restoration times.
2. **Preparedness and allocation of responsibilities.** Contracts and operating procedures generally clarify which party is responsible for maintaining, protecting and restoring shared or leased infrastructure and include service-level agreements and escalation routes.
3. **Mutual assistance and alternative connectivity.** Operators often make arrangements with other operators to share generators on sites where they are co-located. They can also rely on temporary roaming agreements with other operators.
4. **Restoration priorities and public-sector support.** Operators may need to coordinate with electricity providers and public authorities to identify which sites should be restored first. Coordination may also be needed to secure road access, fuel, cranes, barges, temporary permits or emergency import arrangements.

Mutual support after a major outage

In Canada, following a significant outage in 2022, the industry Memorandum of Understanding on Telecommunications Reliability included emergency roaming, mutual assistance and communication protocols. A CRTC review subsequently recommended broader testing of emergency roaming and backup communications to ensure sufficient preparedness and effective allocation of responsibilities.

In a severe weather event, these measures could allow operators to support one another's restoration efforts and maintain services through unaffected networks, without transferring responsibility for repairing or restoring another operator's infrastructure.

Case Study

Regulator-led coordination is essential where the supply chain is disaggregated

An operator from Asia Pacific reports that telecommunications infrastructure is divided between licensed mobile operators, tower companies and fibre providers. This makes regulator-led coordination particularly important because an individual mobile operator cannot restore all the infrastructure needed to provide service.

During disasters, the regulator can bring infrastructure providers and government bodies together, collect information on network availability and prioritise sites serving district administrations, police, fire services and emergency response organisations.

In Bangladesh, the government is also using a sector fund to finance the initial purchase of generators for disaster-prone areas. Operators remain responsible for deploying and maintaining the equipment.

Operators use a mix of proactive and reactive controls to make this coordination work. They rely on incident learning, formal agreements and operational monitoring to manage dependencies with electricity providers, tower companies, fibre providers, contractors and fuel suppliers, while escalation routes and backup suppliers help support preparedness and restoration when disruptions occur.

Operators depend on other organisations for critical elements of resilience, including electricity providers, tower and fibre companies, contractors, fuel suppliers and public authorities.

Improved coordination does not require every operational decision to be managed centrally. Rather, operators and the organisations controlling critical dependencies need to understand their respective roles before an event occurs, establish clear channels for sharing information and escalating issues and agree how they will coordinate during restoration.

These arrangements should be tested in advance so that they can function effectively during severe weather, when normal communications, access and supply arrangements may themselves be disrupted.

Figure 1 **Controls used to manage supplier and infrastructure dependencies**



Source: GSMA operator survey of 29 operators, consolidated responses dated 20 July 2026; Frontier Economics analysis.



Data, tools and models for risk assessment

While operator practice varies, all operators must answer four key questions:

- Where hazards could occur
- Which assets, dependencies and people are exposed
- How vulnerable their networks are
- What service disruption could follow

When assessing risk, operators typically start with historical incidents, engineering judgement and local knowledge. More advanced approaches add geospatial asset data, forward-looking hazard scenarios and asset-level analysis. This section describes current practice, maturity levels and the barriers for each of the four elements.

01. Hazard mapping

02. Exposure assessment

03. Vulnerability assessment

04. Risk of service impact

Hazard mapping

To identify material hazards, operators draw on national meteorological warnings, historical incident records, flood maps, climate projections, commercial risk tools and local operational knowledge.

Interviews with operators revealed that the outputs of models forecasting severe weather do not always align with their experience of observed events. This may reflect outdated or fragmented inputs,[2] insufficient geographic resolution or limitations in model construction. Operators' capabilities can also be constrained by the specialist skills and computational resources needed to combine and interpret climate datasets.

More mature operators use hazard maps to identify areas of relatively higher exposure and validate the results against incident records and local engineering knowledge.

Exposure assessment

Operators overlay hazard data with cell sites, towers, fibre routes, ducts, exchanges, core sites, data centres, landing stations and power systems. The level of geographic detail depends on the hazard and asset being assessed. Geocoded asset-level data can be particularly valuable for spatially localised hazards such as flooding, coastal inundation or wildfire. For broader or more uncertain hazards, such as heat or severe wind, analysis may focus on regional exposure, the upper limits expected or changes in hazard intensity, together with the vulnerability of relevant asset types.

However, the effectiveness of the analysis is often limited by the completeness and accessibility of asset data. Some operators reported that location data is not available to the teams assessing risk, while there can be less visibility of leased or shared infrastructure.

More mature asset inventories combine location with attributes such as asset type, age, condition, replacement value and operational criticality. This is collated in formats that can be integrated across business units and data sources.

Case Study

Heat risk can affect field operations before equipment fails

A European operator indicated that heatwaves currently present a more immediate risk to people than to much of its network equipment, particularly where strategic sites already have adequate cooling capacity. It is therefore examining measures to reduce heat stress for field technicians, including improved protective equipment and changes to working practices. Some of its technicians are currently invited, on a voluntary basis, to start and finish work earlier during heatwaves.

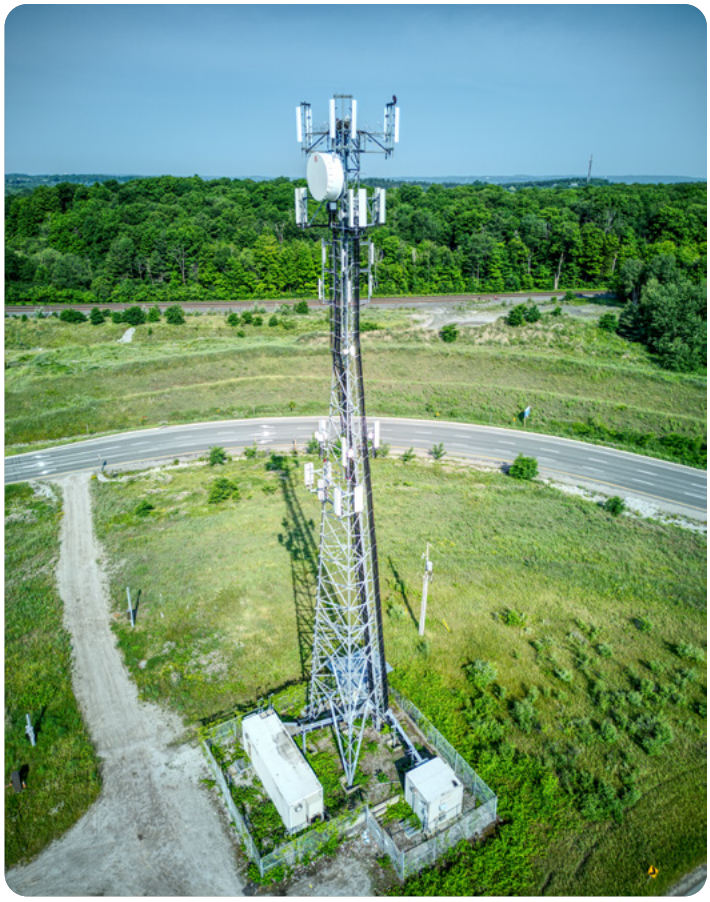
2 The technical characteristics and limitations of the types of datasets operators use are discussed in Report 6, Annex 2.

Vulnerability assessment

Operators assess vulnerability using asset condition and age, site design, tower standards, equipment specifications, backup power duration and existing protection.

The main barriers for these assessments are incomplete information on the condition of assets, limited visibility of third-party infrastructure and a shortage of telecoms-specific fragility evidence. Supplier specifications are useful inputs but cannot determine the resilience of a complete site because actual performance depends on how individual components are configured, integrated, maintained and operated under real-world conditions.

Less mature assessments apply generic engineering assumptions to an asset class while more mature approaches use site-specific information and observed failure, repair or sensor data to distinguish how assets with different designs and resilience measures respond to the same hazard.



Case Study

Design standards are critical to reduce vulnerability

An operator in the Caribbean explained that many legacy towers were designed to withstand winds of around 135 mph. However, given the number of Category 5 hurricanes that have hit the region in recent years, current tower-building standards now require them to withstand winds of approximately 200 mph. New towers are built to the updated standard, while older towers remain more exposed unless inspection shows they need be reinforced or replaced.

Case Study

Supplier specifications are a starting point, not proof of site resilience

A European operator reported that initial discussions with major equipment suppliers have not identified higher temperatures as a significant equipment issue.

Suppliers commonly point out that their products already operate in demanding environments, including deserts and high-altitude locations. This suggests that, in some cases, equipment specifications may already provide substantial tolerance to changing conditions.

However, operators still need to assess whether the complete installed system, including enclosures, cooling, power supply and site-operating practices, can perform under local conditions.

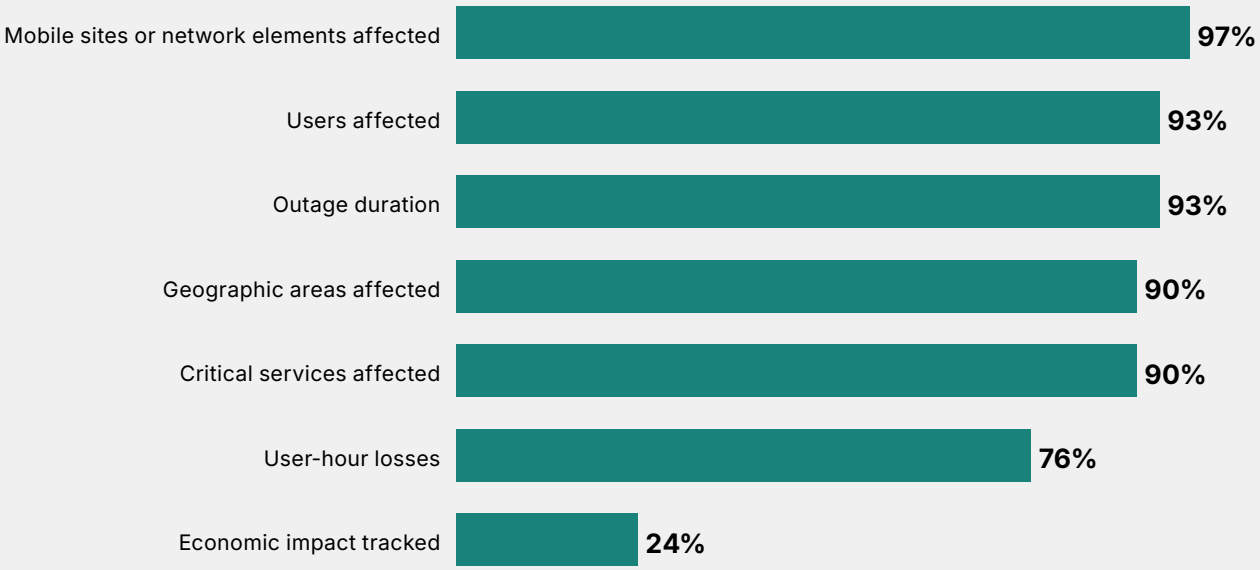
Risk of service impact

Operators assess service risk based not only the number of assets exposed, but also users affected, user hours lost, outage duration, geographic area, emergency communications and critical service dependencies.

More mature approaches link these operational metrics to asset criticality, restoration constraints and user hours lost. This allows risks to be prioritised according to the consequences of failure rather than the number of exposed assets alone.

Almost all operators reported that they track affected sites or network elements (97%); users affected and outage duration (93%); and the geographic area and whether critical services were affected (90%). However, relatively few track the economic impact, for example, the impact on end users (24%). Ensuring that management information can track, aggregate and report data on outages related to severe weather will allow operators to identify risks of severe weather more effectively.

Figure 2 **Operational outage metrics are tracked more often than economic impact**



Source: GSMA operator survey of 29 operators, consolidated responses dated 20 July 2026; Frontier Economics analysis.

Conclusion

When it comes to assessing weather-related risks, operators are at different levels of maturity. Most draw on historical incidents, engineering judgement and local knowledge, while more mature operators combine forward-looking hazard data with geocoded asset information, vulnerability evidence and service impact analysis. The aim is not more complex modelling, but to identify which assets and services are most at risk and where intervention is most valuable.

Governance is equally important, with responsibilities spread across network, sustainability, risk, finance and other teams. Clear accountability and cross-functional collaboration are needed to ensure risk assessments inform network planning, business continuity and investment decisions, rather than remaining primarily a reporting exercise. Coordination with infrastructure partners and public authorities is also important where resilience depends on power, towers, fibre, fuel or emergency access.

All this points to the following priorities:

- **Operators** should establish clear senior accountability and decision rights; bring network, engineering, sustainability, risk and finance teams together; improve geocoded asset, vulnerability and incident data; and embed longer-term, forward-looking risk assessments in asset planning, procurement and capital allocation.
- **Suppliers and infrastructure partners** should provide operators with usable information on asset condition, dependencies, design limits and restoration constraints.
- **Policymakers and public authorities** should facilitate coordination between operators and critical infrastructure providers and support consistent outage and service impact data.
- **Industry bodies and climate data providers** should develop common terminology, practical guidance and interoperable datasets that allow operators at different levels of maturity to undertake proportionate and comparable assessments.

Copyright © 2026 GSM Association