GSMA

05



Futureproofing Connectivity

Prevention, response and recovery practices

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 fifth 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.



Adaptation and resilience in action

Operators cannot eliminate all weather-related risk, nor would it be proportionate to harden every network asset against every possible event. Resilience therefore depends on a portfolio of complementary measures, integrated where possible into routine maintenance, technology upgrades and network renewal. The appropriate mix will vary according to the hazard, asset criticality, local infrastructure dependencies, restoration constraints, expected asset life and the relative costs of prevention and recovery.

This report distinguishes between three broad types of action:

1. Reducing exposure or vulnerability before an event occurs
2. Operational preparedness, response and recovery measures that limit the duration and service impact of disruption
3. Managing residual impacts

It then considers how operators can balance these measures to achieve a proportionate and cost-effective level of resilience across different network assets and locations.

Reducing exposure or vulnerability

Network equipment is renewed through normal technology and asset management cycles. Operators use capital budgets to maintain network condition, add capacity and deploy new technology. Many of the investments that improve resilience to weather hazards also improve resilience to other risks.

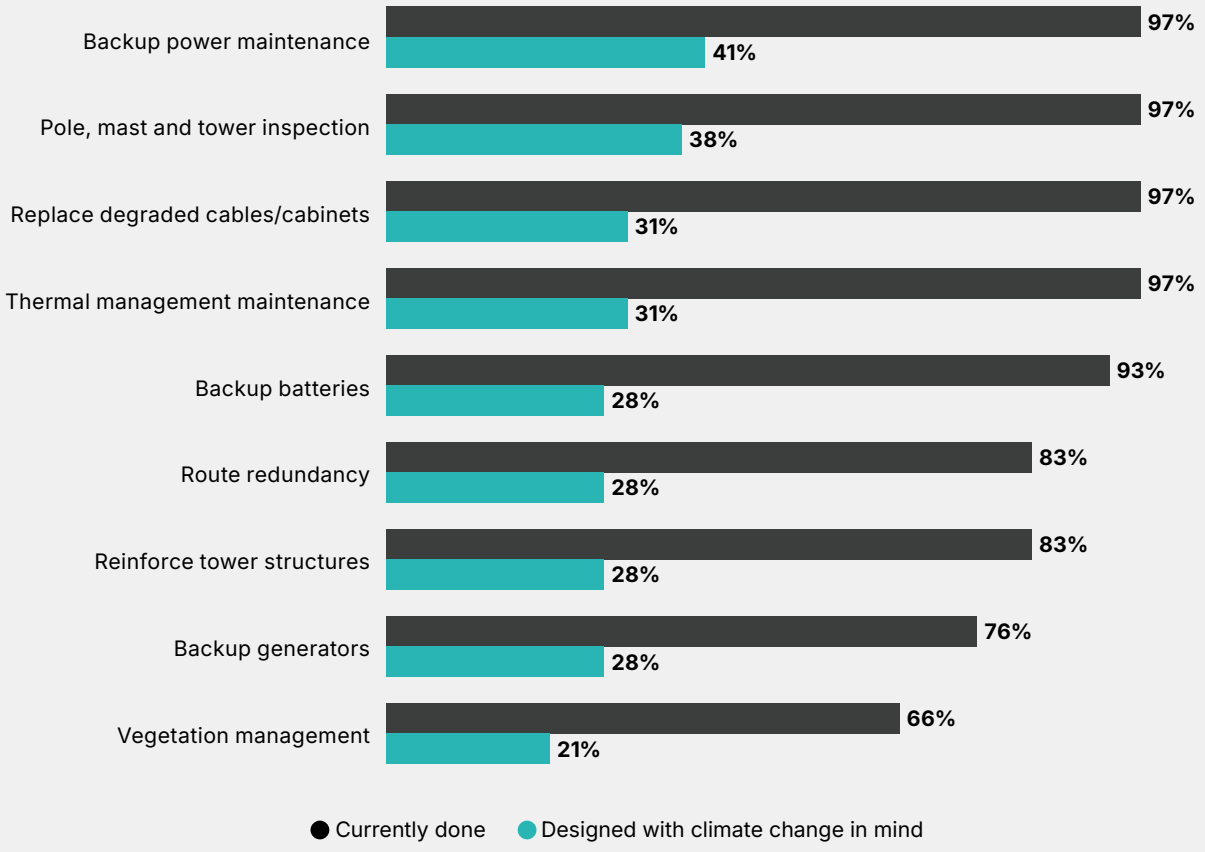
Most survey respondents have undertaken resilience work programmes, such as backup power maintenance, pole, mast and tower inspection, replacing degraded cables and cabinets and thermal management maintenance. However, the proportion of respondents reporting that these programmes were designed with climate change in mind is much lower and varies by programme.

Case Study

Regular replacement cycles to reduce heat exposure and energy demand

A European operator explained how adaptation can be incorporated into normal procurement and technology-upgrade cycles and why vulnerability assessments should consider equipment-operating thresholds and cooling requirements, not just projected external temperatures. It noted that suppliers are developing equipment capable of operating at higher ambient temperatures, while some indoor equipment is being replaced with outdoor equipment that requires less cooling.

Figure 1 **Resilience work programmes are widespread, but explicit climate design is less common**



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



Operational preparedness, response and recovery measures

In addition to routine renewal, which builds resilience to all kinds of threats and hazards, operators also use targeted measures to reduce exposure, vulnerability and service disruption.

Reducing exposure to weather hazards

Operators increasingly consider climate risks when selecting new sites, recognising that avoiding flood-prone or otherwise exposed locations can be more cost-effective than reinforcing existing infrastructure.

Preventive measures to reduce vulnerability and service impact

Operators reduce the impact of weather hazards on their services through preventive actions or incremental design changes during normal replacement and upgrade cycles. Typical measures reported by operators are summarised in Table 1.

Table 1 How operators manage different weather-related risks

Weather-related risk	Examples
Storms, wind and cyclones	Tower inspection, mast reinforcement, upgrade of antenna mounting standards, route redundancy and technology diversity (e.g. fibre + MW link backhaul), vegetation management, installation of backup power for grid outages
Heavy rain and flooding	Flood barriers, raised platforms, water ingress protection of cabinets and ducts, site drainage
Heatwaves and rising temperatures	Cooling system installation and maintenance, monitoring of equipment temperature, improved ventilation, battery management, installation of equipment designed for higher operating temperatures
Wildfires	Vegetation clearance around network infrastructure
Snow, ice and cold	De-icing plans, battery performance management, spare parts and field-force readiness

Operators in the hurricane belt have invested to harden their assets

After Hurricane Maria destroyed around 95% of cellular sites in Puerto Rico, operators redesigned networks with reinforced towers, elevated equipment and waterproof enclosures.

Following a $250 million loss in the 2017 Atlantic hurricane season, T-Mobile implemented AI-enabled network management to better predict weather impacts and better prepare their networks for future disasters.

Operators in the British Virgin Islands also focused on building resilient infrastructure following the devastation caused by Category 5 hurricanes, installing hurricane-robust mobile wireless towers with better internet speeds and greater bandwidth capacity.



Managing power supply disruptions

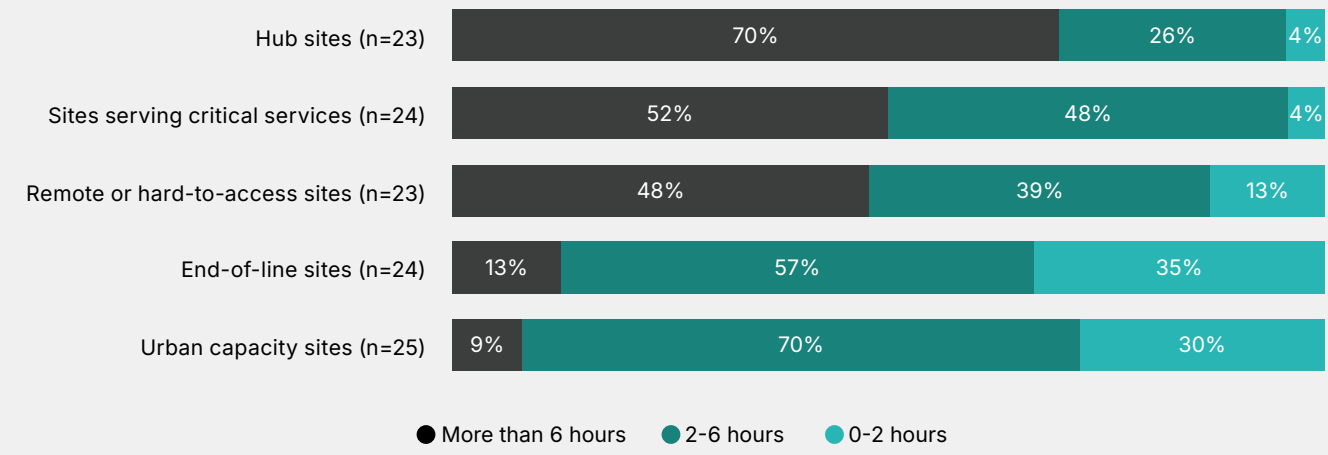
Disruptions to power supply is usually considered the key limiting factor in maintaining services during extreme weather events. Operators manage this risk through two complementary approaches.

First, they can install local backup power through batteries, generators and, where appropriate, solar or hybrid systems, with the type and duration of backup based on site criticality, expected outage duration and restoration constraints.

Second, operators can reduce the electricity required by network equipment and supporting systems such as cooling. Lower consumption extends the period a given battery capacity or fuel supply can maintain service. This can be done through more efficient hardware, network modernisation and intelligent sleep modes, which also support climate mitigation efforts.

Operators differentiate backup power by site criticality. In the survey, almost all hub sites had at least two hours of autonomy and most had more than six hours.

Figure 2 **Reported backup power autonomy, by site type**



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

Case Study

Energy efficiency can improve heat resilience

A European operator reports that electricity accounts for around 95% of total energy consumption while cooling can represent around 40% of network electricity use. It therefore introduced measures to deploy equipment capable of operating at higher temperatures and to replace indoor equipment with outdoor equipment where appropriate.

Reactive response and recovery

Even with proportionate investment in network design, some risk to disruption remains. Operators therefore need operational response capabilities that allow them to anticipate severe weather, prepare resources and maintain services while an event is unfolding, restore affected services and use the experience to strengthen the network.

Before a severe weather event

Operators monitor meteorological warnings, review hazard alerts, check backup power, pre-position generators, fuel and spare parts, schedule field teams, check access to critical sites, contact suppliers and contractors, prepare customer communications and notify relevant authorities where required. Operators may also monitor power, temperature, humidity, battery voltage, traffic, signal levels and packet loss.

Before events, operators in Bangladesh, Türkiye and the United States have reported pre-positioning generators, mobile sites, specialist teams and spares.



Case Study

Effective preparedness combines official hazard data with live operational signals

Turkcell uses government maps covering wildfire, flood, desertification and avalanche risk to assess whether base stations are located in exposed areas. It supplements these with forecasts from the national meteorological authority, including regional wildfire and flood warnings issued around a week ahead.

Turkcell also monitors unusual changes in emergency calls and voice or data traffic, alongside local social media activity and disaster-related keywords. These inputs generate alerts for its network teams and help identify where closer monitoring or preparation is required.

During a severe weather event

Network operations monitor alarms and traffic flows, reroute traffic where routes remain available, balance load across sites, prioritise voice or emergency traffic where technically and legally possible, deploy temporary mobile sites, activate backup power and coordinate with field teams.

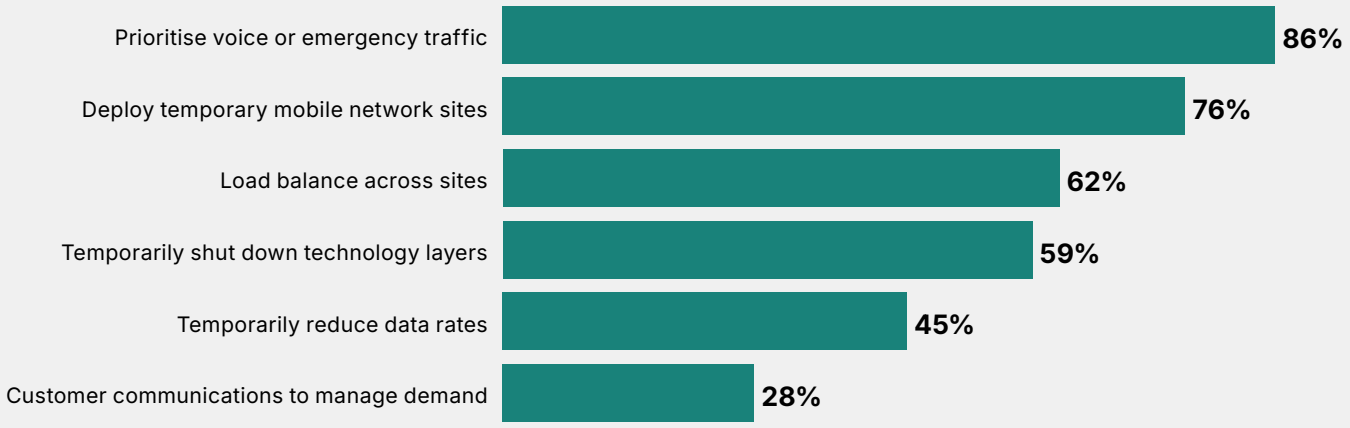
Operators also coordinate with emergency services, regulators, civil protection authorities, power companies, tower companies, local authorities and other operators.

During a severe weather event, operators in Chile combine continuous network monitoring, regional availability reporting, emergency roaming, public alerts and coordination with electricity restoration.

Operators in Bangladesh have used regulator control rooms, military logistics and Very Small Aperture Terminals (VSATs) during widespread floods. These examples show that resilience is not a single engineering intervention but a repeatable preparedness, response and learning cycle.

During major disruptions, operators take a range of temporary operational measures to preserve essential connectivity. Prioritising voice and emergency traffic is the most common approach, while operators also use temporary mobile sites and load balancing to maintain coverage and capacity. More restrictive measures, such as temporarily shutting down technology layers or reducing data rates, are less common.

Figure 3 Operational practices used during major disruptions



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

Direct-to-device satellite can provide a temporary coverage layer

Satellite-based direct-to-device, or D2D, technology allows ordinary mobile devices to connect directly to satellites without requiring a dedicated satellite handset. In resilience terms, this can provide a temporary coverage layer when terrestrial mobile networks are damaged by large-scale weather hazards.

Responses to Hurricane Melissa in Jamaica and wildfires in Spain illustrate the role this technology can play. In Spain, MasOrange tested Starlink's direct-to-cell technology using 5 MHz frequency division duplexing (FDD) of its licensed mobile spectrum in the 2.6 GHz band. The capability was subsequently activated during the July 2026 wildfires in areas affected by network outages, enabling customers of MasOrange and Movistar to access basic messaging and limited low-bandwidth data services.

After a severe weather event

Operators replace damaged equipment, repair fibre, restore power, replenish spares, review the performance of backup systems, analyse user impact, report incidents, support customers and update plans. For example, The Bahamas' outage mitigation framework requires restoration information, root-cause analysis and mitigation planning. Post-incident reviews are particularly important because they reveal whether risk models, asset data, supplier arrangements and restoration assumptions matched reality.



Case Study
Vodafone's continuous resilience cycle

Vodafone frames resilience as a continuous cycle of Predict, Prepare, Respond, Recover and Rebuild. This framework is applied flexibly across its operations with practical actions that vary by geography. Operators can use or adapt this framework to operationalise their response to severe weather risk.

- **Predict – UK**: Vodafone is using changes in microwave network signals along the River Severn to support near-real time rainfall forecasting and flood monitoring, complementing radar and rain gauges. It also supports scalable warning systems, including cell broadcast (CB) in Germany and geolocated alerts in Mozambique.
- **Prepare – Greece and Türkiye:** In wildfire-prone Greece, Vodafone's "Always Ready" model combines continuity plans, backup power, vegetation clearance, remote monitoring and alternative connectivity. When a fire approached Patras in 2025, teams assessed exposure early and prepared to reroute traffic before conditions deteriorated. In Türkiye, Vodafone raised a critical regional hub by two metres after identifying increased flood exposure, without interrupting service.
- **Respond – Germany:** During the 2021 Ahr Valley floods, Vodafone reconfigured and boosted neighbouring sites and deployed satellite-linked instant networks where roads were inaccessible. Almost 90% of mobile coverage was restored within 24 hours, supporting emergency responders and affected communities.
- **Recover – Portugal:** Following Storm Kristin in 2026, Vodafone mobilised engineers and worked with civil protection, the regulator and electricity distributor e-REDES, deploying mobile network trucks, generators, satellite connectivity and emergency response kits to restore critical locations, including fire stations and an isolated community.
- **Rebuild – South Africa:** In KwaZulu-Natal, where repeated floods and storms have damaged infrastructure, Vodacom now allocates around 20% of regional capital expenditure to strengthening network resilience. Following major floods, it has also used digital lending and e-vouchers to help households and businesses resume activity while physical infrastructure is restored.



Managing residual impacts

To manage residual impacts, operators need to understand how such disruption could affect their cash flow and balance sheet or reputation.

Residual outages

Beyond the need for repair and restorative actions, weather-related disruption can also affect operators in the following ways:

- **Lost revenues.** Outages may reduce usage-based or traffic-related revenue while services are unavailable or degraded. The immediate impact on revenue may be limited for short outages where customers pay fixed subscriptions, but it can become more material where disruption is prolonged, repeated or usage-based revenues are significant. For example, one African operator reported that most of its users rely on volume-based charging and that network unavailability directly reduces its usage revenues.
- **Customer compensation and contract liabilities.** Operators may have to provide refunds, service credits or compensation where services are unavailable or repairs are delayed. Enterprise contracts may also include service-level commitments and contractual penalties.
- **Regulatory penalties.** Where an outage results in a breach of obligations relating to emergency communications, network security, resilience or incident management.
- **Reputational harm and churn.** Particularly where outages are prolonged, communications are poor or disruption affects essential services.

Operators need to plan for contractual and regulatory liabilities

In the UK, the national regulator for communications services, Ofcom, has a voluntary automatic compensation scheme applies to residential fixed line and broadband services supplied by participating providers. It covers delayed repairs following a total loss of service, missed appointments and delays to the start of a new service. Mobile services are outside the scope of the scheme, although mobile customers may seek redress through their provider's complaints process and, where the complaint remains unresolved, an Ofcom-approved alternative dispute resolution scheme.

Insurance and risk retention

Even after operators have taken proportionate steps to reduce vulnerability and prepare for restoration, they still face some financial risk. Operators must decide which losses to transfer through insurance and which to retain directly, including through self-insurance or captive insurance arrangements.

Insurance can help fund asset replacement, business interruption and rapid recovery, but it does not prevent outages and may not cover the full loss as insurers require deductibles before compensating for loss. The protection available depends on policy terms, limits and exclusions, while the cost of cover reflects the value and location of assets, expected hazard losses and the insurer's assessment of network vulnerability.

Insurance should be part of an integrated resilience strategy rather than a substitute for preventive investment or business continuity planning. Resilience measures may reduce the amount of cover required or improve deductibles and limits, although partial improvements may not materially change the overall risk profile. Operators typically use three main types of insurance:

- **Property damage insurance** covers the cost of repairing, replacing or reinstating insured physical assets following damage caused by a covered event. Weather hazards can be included within a broader property policy, although particularly exposed assets may be excluded or insured separately. The main factors driving pricing for these products are the replacement value and the probability and expected severity of relevant hazards.
- **Business interruption insurance** covers defined financial losses that arise when a covered event interrupts or reduces an operator's activities. Depending on the policy, this can include lost income, additional expenditure incurred to maintain or restore operations, such as hiring temporary equipment or purchasing from an alternative supplier. Pricing depends mainly on the income or gross profit at risk and the potential duration of an interruption.
- **Parametric insurance** provides a pre-agreed payment when an independently measured physical parameter reaches or exceeds a specified threshold. A tropical cyclone policy might, for example, provide a payout when a storm of a defined intensity passes through a specific geographic area, while other products may use rainfall, wind speed, temperature or flood depth measurements.

  Unlike traditional indemnity insurance, payment does not depend on a detailed assessment of the operator's actual physical damage. This can provide liquidity substantially faster, supporting urgent restoration expenditure while a conventional property damage claim is still being assessed. The price is driven principally by the modelled probability that the parameter will trigger a payment, the size of the pre-agreed payout and the geographic area covered.

Climate risk may affect insurance coverage before it affects premiums

As climate exposure increases, operators may face higher insurance premiums in some markets. In others, premiums may remain stable while coverage narrows. Exclusions may be applied to particular regions or types of weather-related damage, depending on the perceived risk.

Operators may find that some risks may be uninsurable or only insurable at very high rates or exclusions. In these cases, operators may combine external insurance with risk retention and captive insurance. This can be a deliberate financing choice, but it may also be necessary where cover is unavailable, prohibitively expensive or subject to exclusions for certain hazards or locations.

Under self-insurance, the operator retains losses up to a chosen level and finances them from its own balance sheet or designated reserves. A captive is an insurance company owned by the corporate group that insures risks arising within the group. It can pool risks across subsidiaries and countries, retain predictable or otherwise difficult-to-insure losses and purchase reinsurance from the external market for less frequent but more severe events.

Resilience investment may reduce insurance costs, but premium reductions are not automatic

Investments in resilience do not necessarily reduce an operator's premiums. This is because:

- **Insurance pricing reflects both the vulnerability of assets and the value exposed to loss.** Lower vulnerability may therefore be partly offset where newer or upgraded infrastructure has a higher replacement value.
- **Resilience measures need to reduce vulnerability materially across the relevant network.** Upgrading only a proportion of assets may have little effect if the principal sources of loss remain exposed.
- **Insurance mutualises risk.** In the absence of recognised market-wide standards or resilience grades, insurers may find it difficult to distinguish and price individual operators according to their resilience and may instead rely partly on wider market or country-level experience.
- **Demonstrating operator-specific resilience may require detailed and up-to-date engineering assessments.** These can be costly, particularly for geographically dispersed telecommunications networks, while outdated or incomplete information may lead insurers to apply additional pricing margins.

For operators, the financial benefits of resilience may therefore emerge over time, rather than through an immediate reduction in their next annual premium.

Conclusion

Operators need to identify a proportionate portfolio of measures that reduce exposure and vulnerability before an event; maintain and restore services when disruption occurs; and manage the financial consequences of losses.

In principle, a preferred portfolio is one that minimises the total expected cost of disruption and resilience over the life of relevant assets while also meeting regulatory obligations and an acceptable level of service continuity.

In practice, precise optimisation is difficult. Many operators have incomplete information on asset-level exposure and vulnerability, particularly for third-party infrastructure. Climate datasets may be difficult to translate into operational parameters and operators may not have personnel proficient in climate science, network engineering, financial analysis and local operational knowledge. There is also a mismatch between the long time frames over which climate conditions and long-lived assets evolve and the shorter horizons commonly used in business planning. As a result, decisions are often made with substantial uncertainty and may not fully account for the costs and benefits of different options.

A practical resilience decision framework should:

- Compare portfolios of measures and their costs, avoided losses, service benefits and dual benefits for climate mitigation
- Test operational feasibility, dependencies and delivery constraints
- Review decisions as hazards, networks, costs and evidence change

Copyright © 2026 GSM Association