GSMA

03



Futureproofing Connectivity

Legal, regulatory and voluntary frameworks shaping network resilience

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.

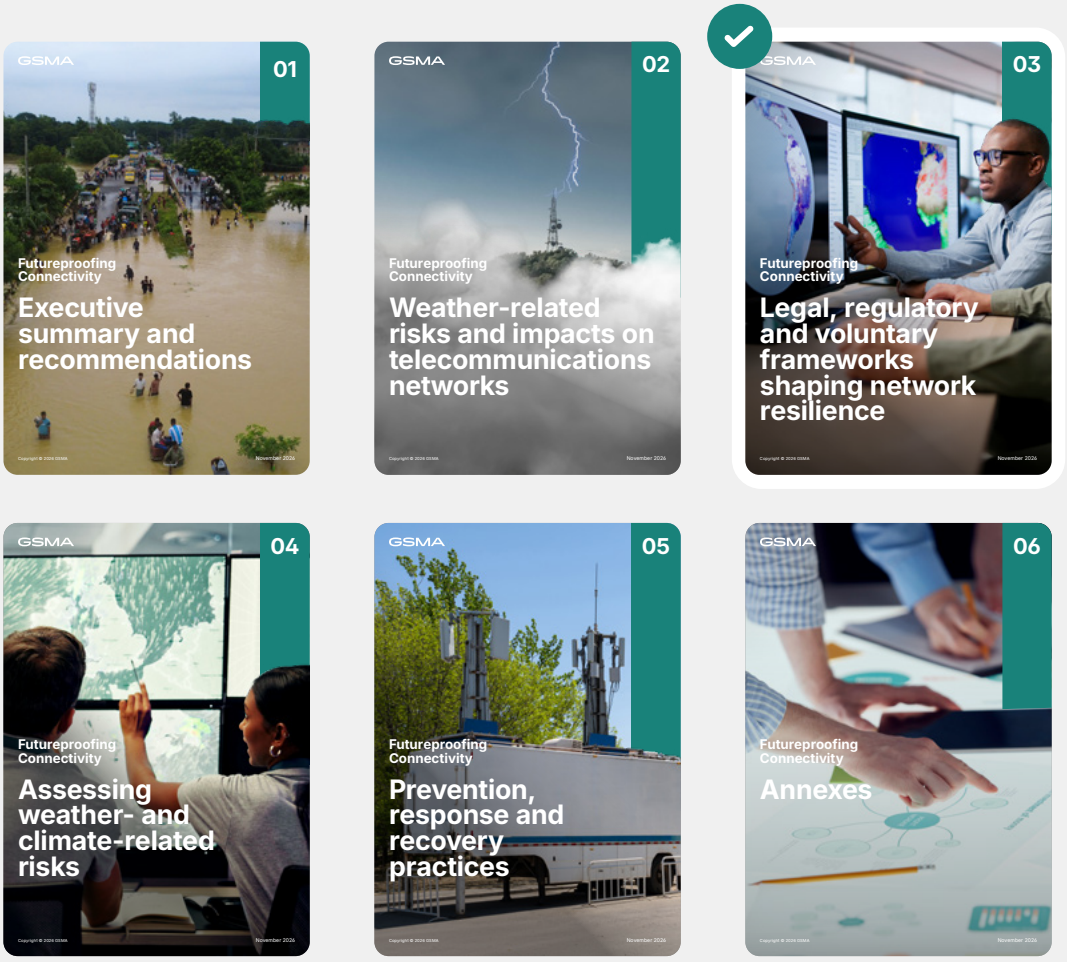
Antitrust notice

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

Futureproofing Connectivity

This is the third 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.



Frameworks for mobile network resilience

Telecommunications operators are subject to a range of legal, regulatory and voluntary frameworks that shape how they prepare for, respond to and recover from disruptions, including those caused by weather-related hazards. These frameworks play different roles with some focusing on continuity of service, public safety and emergency response, while others focus on longer-term climate risks, financial exposure, governance and disclosure.

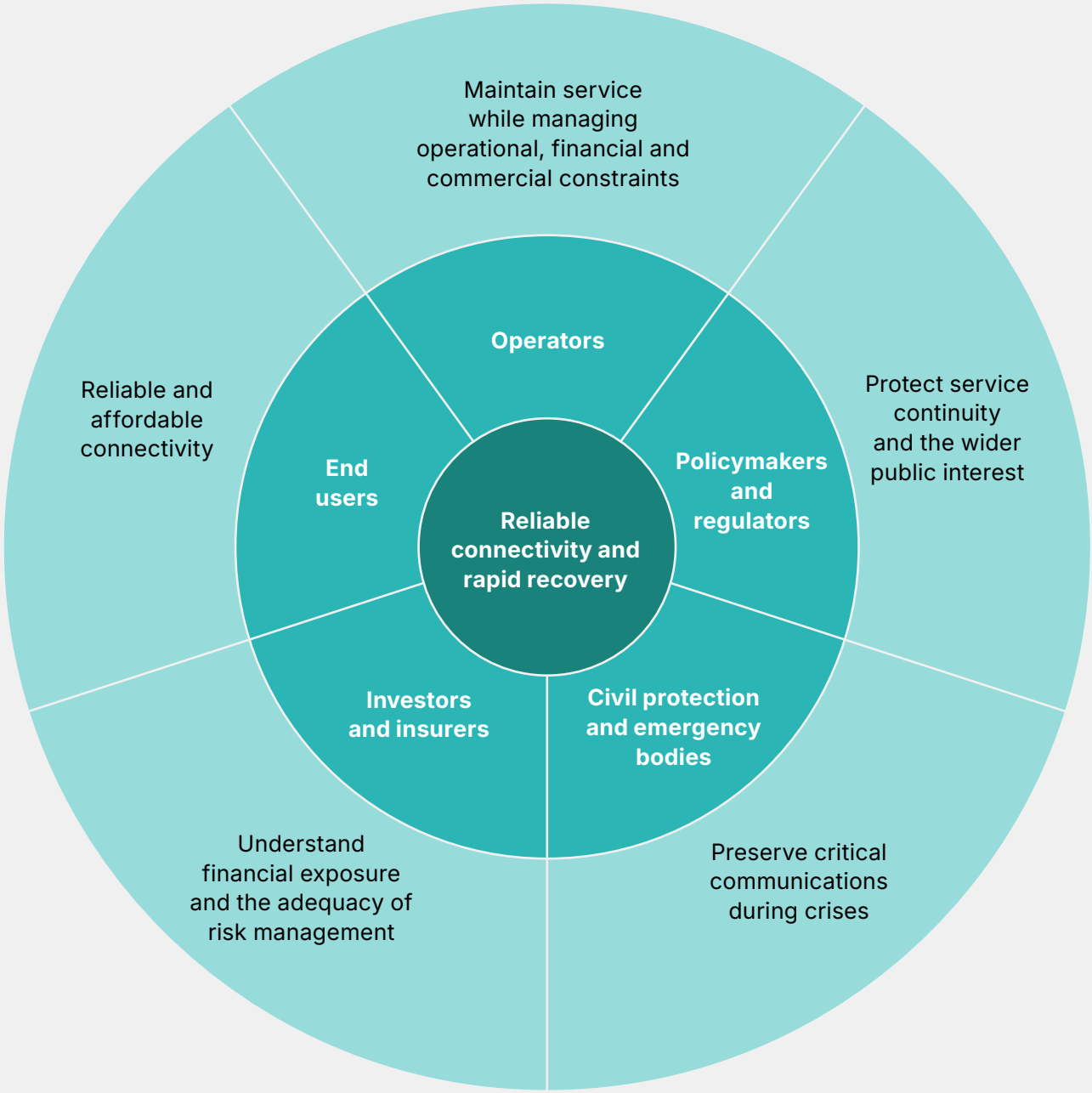
The main challenge is not a lack of frameworks, but ensuring they are aligned, proportionate to the risks being addressed, and sufficiently flexible to support effective resilience decisions without unnecessary duplication.

This report examines the priorities of different stakeholders and the five main frameworks affecting telecommunications operators. It then considers what makes these frameworks effective in practice, including how requirements change following major incidents, the consistency of resilience and adaptation reporting, their implications for operator costs and incentives and how regulatory rules can constrain resilience efforts.

The value of resilience for different stakeholders

The resilience of telecommunications networks matters to operators, end users, governments and regulators, civil protection organisations and wider society. While all stakeholders value and depend on resilience to climate- and weather-related threats, they tend to emphasise different dimensions of resilience (see Figure 1). These different objectives help explain why the resilience landscape is shaped by multiple frameworks.

Figure 1 The value of resilience for different stakeholders



Source: Frontier Economics

The five frameworks shaping operator decisions

There are five types of frameworks that can impose obligations or responsibilities on operators to build resilience to climate and weather-related hazards or to support them in building this resilience.

Table 1 Mandatory and voluntary frameworks serve different purposes

Type of framework	Purpose and application to weather resilience
Telecoms-specific legal and regulatory instruments	These instruments focus directly on network availability and continuity of service. They typically require operators to manage operational and security risks, identify dependencies and single points of failure, maintain incident preparedness arrangements and notify authorities of significant incidents or outages. This category includes telecoms licences and codes or ad hoc decisions from telecoms regulators.
Mandatory climate and sustainability disclosure frameworks	These frameworks require companies to identify, assess and disclose material physical climate risks and the actions taken to manage them. They are generally forward-looking and cover governance, scenario analysis, materiality, anticipated financial impacts and adaptation measures over the short, medium and long term. They provide a common structure for assessing weather-related risks but are less concerned with real-time incident management or restoration. Examples include the EU Corporate Sustainability Reporting Directive (CSRD) and European Sustainability Reporting Standards (ESRS) or jurisdictional application of IFR.
Corporate governance and risk management frameworks	These frameworks embed weather and climate risks within internal decision-making. They address board oversight, internal controls, risk appetite, escalation routes and the allocation of responsibility across the business. In practice, they can translate identified risks into investment plans, supplier arrangements, operational triggers, testing programmes and business continuity and recovery processes. These frameworks include a mix of international standards and enterprise risk management (ERM) frameworks, which are then implemented into operator-specific plans (ISO 37000 – Governance of organisations; ISO 22301 – Business continuity, management systems; ISO 31000 – Risk management or COSO ERM).
Critical infrastructure and civil protection frameworks	These frameworks take an “all hazards” approach to maintaining essential services. They focus on emergency preparedness, cooperation with public authorities, cross-sector dependencies, restoration priorities and crisis coordination. They may impose both ex-ante planning requirements and ex-post notification or reporting obligations for service outages. These frameworks do not necessarily apply to the entire telecommunications sector – they typically only impose obligations on operators, services or assets that have been formally designated as critical.
Voluntary or market-led disclosure frameworks and expectations	These frameworks provide common methods for assessing and communicating climate risks outside formal regulatory requirements. Although not legally binding, they can create incentives for operators to improve their practices through investor scrutiny, benchmarking and stakeholder pressure. They can also help operators compare practices, identify gaps and demonstrate that their approach is aligned with emerging good practice. These include, in particular, the CDP (Carbon Disclosure Project) disclosure platform.



Characteristics of effective resilience frameworks

The five types of assessment and reporting frameworks described here can benefit governments, insurers, investors and other stakeholders by improving the visibility of operators' risk profiles. They can also benefit operators by establishing ownership within the organisation for assessing and reporting climate and weather-related risks, creating a common terminology, set of tools and data sources and bringing together teams that previously considered climate risk separately.

Case Study

Voluntary frameworks can help operators prepare for mandatory disclosure requirements and provide a consistent approach to assessing risk

A European towerco began analysing and disclosing climate risks voluntarily in around 2017, initially in response to investor and sustainability index expectations. It then built on these efforts to comply with the introduction of CSRD and ESRS requirements.[1] The company reported that these frameworks helped it prepare for more formal obligations.

A European operator similarly described CDP and other voluntary frameworks as useful methodological tools. In the absence of a standardised approach to adaptation, these frameworks help operators select scenarios and data sources and decide how to assess and report adaptation measures.

1 Harmonised mandatory framework introduced in 2015 in the EU for large public interest entities through the Non-Financial Reporting Directive, later expanded through the Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS).

Some operators stated that the combined requirements of multiple frameworks imposed an unnecessary compliance burden. A European telecommunications infrastructure company pointed to the duplication of mandatory requirements, such as CSRD and ESRS, and multiple information requests by sustainability indices and other frameworks, describing the reporting landscape as fragmented and burdensome. An operator headquartered in Sub Saharan Africa also identified duplication in one of their markets, where the communications authority and environmental authority request some of the same climate-related information. It also highlighted potential tensions between communications quality requirements, which can require network densification and higher power levels, and environmental requirements affecting site power and generator use. This may suggest that the compliance burden could be minimised by ensuring alignment between definitions, metrics, reporting formats and information requests.



Countries differ both in how prescriptive their requirements are and which aspects of resilience they prioritise, reflecting differences in hazard exposure, geography, network structure and institutional arrangements. Some regulatory regimes set detailed technical requirements for critical infrastructure while others rely more heavily on outcomes-based continuity obligations and others use operator-led risk management.

- **Chile** has a comparatively prescriptive regime, combining different requirements for critical sites with specified backup power, route diversity, rapid outage reporting, emergency roaming and active regulatory monitoring.
- The **United States** places greater emphasis on objective outage thresholds, daily disaster reporting, mutual aid and specific 911 reliability duties, while leaving ordinary commercial mobile site backup largely to operator practice and certain state rules.
- **The Bahamas**, given its location in the “hurricane belt”, focuses on hurricane and disaster preparedness through a structured cycle of resilience planning, outage reporting, restoration and post-event mitigation – reflecting the needs of a small and geographically dispersed island market.
- **Bangladesh, Kenya and South Africa** rely more on broad continuity and emergency management duties, regulatory powers and coordination arrangements. Requirements are generally less prescriptive for quantified measures such as backup duration, fuel reserves, restoration times and minimum degraded mode service.

Stronger requirements needed for major outages

Several operators reported that resilience rules and technical standards have been strengthened after major failures exposed weaknesses in existing arrangements. Event-led regulation can close genuine gaps and draw on observed operational evidence.

Major incidents can expose systemic design weaknesses

Examples from The Bahamas and Canada illustrate a common pattern: major failures can reveal weaknesses not apparent under normal operating conditions.

In The Bahamas, Hurricane Dorian and Category 5 storms have contributed to a shift from tower standards designed for winds of around 135 mph to ones designed for approximately 200 mph. This will progressively strengthen the resilience of the wider network, helping the sector prepare for a future in which high-intensity cyclones may occur more frequently and with greater intensity.

In Canada, the Canadian Radio-television and Telecommunications Commission (CRTC) commissioned an independent assessment after a service outage in July 2022 affecting more than 12 million customers and critical services. This led operators to implement measures including a separate management network, backup connectivity, improved change and incident management and planned separation of wireless and wireline IP cores.



However, designing appropriate and proportionate regulation requires appropriate stakeholder consultation and engagement.

Backup power rules require consultation and proportionality

Consultation played an important role in designing proportionate regulations for power resilience in Chile. Following an April 2025 electricity blackout, authorities in Spain proposed new backup power requirements for larger telecommunications operators. The initial proposal would have required eight hours of autonomy while maintaining mobile coverage for 85% of the population. It was only after consultation that the requirements were reduced to a more proportionate level: four hours and 75% coverage by 2030.

Standardisation in resilience, adaptation and mitigation reporting

Several operators distinguished between reporting greenhouse gas (GHG) mitigation and reporting resilience or adaptation. They noted that mitigation reporting benefits from established accounting boundaries, the internationally recognised GHG Protocol and relatively standardised emissions metrics. In contrast, physical risk assessment and adaptation reporting allow much greater discretion over climate scenarios, time horizons, hazard data, geographical granularity, asset vulnerability, financial impacts and the classification of adaptation expenditure. This reduces comparability across operators and makes assessments harder to translate into operational decisions.



Impact of framework design on implementation costs and operator incentives

Operators generally favour frameworks that focus on the outcome rather than how they should achieve that outcome. This is because output-based frameworks allow operators to determine the most efficient combination of engineering, operational and restoration measures for their own networks.

Operators stressed that the effectiveness of a requirement depends on whether the measure taken is available and operational during an actual disruption, given local hazards, theft or vandalism, access constraints, supplier capability and cost. They also stressed that different measures may achieve the same resilience outcome and that requirements need periodic review against observed performance.

Case Study

Resilience requirements may be undermined by the local operating environment

An operator from Latin America explained that battery backup may satisfy a formal power backup requirement when it is installed, yet fail to provide resilience in practice when batteries are stolen or vandalised. In such cases, the regulatory measure is hindered by local operating conditions and may generate repeated replacement costs without improving service continuity. In a public security roundtable, it was noted that battery theft from cell sites was a significant concern in parts of Chile. It was reported that in 2025 and the first five months of 2026, nearly 3,000 vandalism events and 8,739 stolen batteries were recorded.[2]

2 Subsecretaría de Telecomunicaciones de Chile. (13 July 2026). "Biobío es la segunda región con más robos de baterías de telecomunicaciones: Subtel realiza la primera Mesa de Conectividad y Seguridad Pública en la region".

Mandatory requirements can establish a consistent and enforceable baseline where risks to public safety, critical services or wider economic externalities are material. However, overly prescriptive requirements may limit operators' ability to select the measures best suited to their networks and local operating conditions, and may also limit their ability to compete.

Case Study

Operator-led initiatives are preferable

An authority in North America noted that operator-led voluntary arrangements may be preferable to mandatory requirements, as they can be introduced more quickly and applied more flexibly and cost-effectively. Mandatory frameworks, meanwhile, require more consultation, legal process, compliance monitoring and can take longer to make changes.

Case Study

Resilience can create competitive value

A European operator reported that its faster restoration of services following a cyclone was followed by a gain in market share. It regarded this as evidence that customers value an operator's ability to recover rapidly after a major event and that it is important to preserve incentives to invest in resilience, as it helps operators compete on reliability and recovery performance.

Operators view network resilience as an important part of service quality. Where regulatory resilience requirements establish minimum expectations, such as for battery autonomy, some operators may choose to exceed these minimum requirements to even better protect service continuity in their own networks.



Other regulatory rules affect the resilience measures available to operators

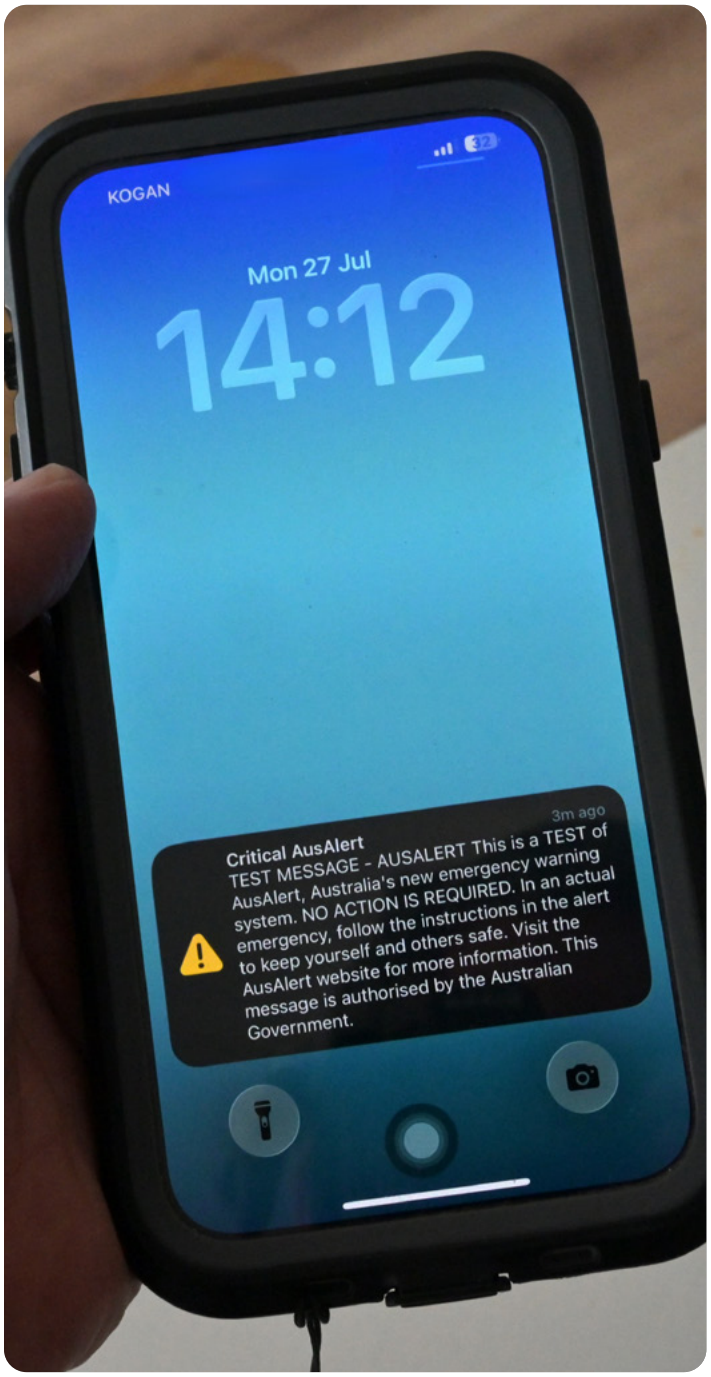
Operators also identified rules that were not designed primarily for climate resilience but can affect the measures available to them during disruption or the speed at which investments in resilience can be delivered.

Case Study

Flexible traffic management rules and expedited approvals can strengthen resilience without weakening ordinary safeguards rules designed for normal operating conditions.

A Latin American operator reported that network neutrality rules can create uncertainty about whether an operator can prioritise traffic during a major disruption. It suggested that defined emergency flexibilities could allow voice, emergency calls, public warnings or low-bandwidth messaging to be prioritised, or high-bandwidth services to be temporarily reduced, if basic connectivity was preserved for more users for longer.

A European telecommunications infrastructure company and operators reported that planning and permitting processes can affect the timing and cost of relocating assets away from flood-prone areas, hardening sites, adding backup power, improving route diversity or deploying temporary infrastructure. Slow or uncertain approvals may therefore delay otherwise cost-effective resilience measures.



Conclusion

Legal, regulatory, corporate and voluntary frameworks play different roles in supporting resilient telecommunications:

- Telecoms-specific and critical infrastructure requirements are primarily aimed at protecting service continuity, public safety and emergency communications.
- Climate disclosure frameworks encourage operators to assess longer-term physical risks and their potential financial impacts.
- Corporate governance and enterprise risk frameworks provide the internal processes through which risks are assigned, escalated, funded and monitored.
- Voluntary frameworks allow operators the flexibility to develop innovative solutions and mechanisms most appropriate and effective for the risks they face in their markets, and they enable long-term targeted investment and planning.

However, these frameworks are not always aligned. Operators may be required to describe the same underlying risks using different definitions, thresholds, time horizons and metrics. Adaptation and resilience reporting also remains considerably less standardised than GHG reporting – reducing comparability and making reported information harder to translate into operational decisions.

Authorities should coordinate the design of resilience frameworks, and review existing ones to remove overlapping, conflicting or misaligned requirements. This includes using common information and defining clear service continuity and public safety outcomes, while giving operators the flexibility to select the most effective combination of engineering, operational and restoration measures for their networks. Operator-led frameworks can be implemented more quickly, are more flexible and risk based, and can be more cost-effective.

Policies and frameworks should recognise interdependencies and support coordinated planning before, during and after major incidents. Telecommunications networks are part of a wider ecosystem and rely on access to power, fuel, transportation, for example. While major incidents can reveal genuine gaps and provide a basis for stronger requirements, responses to incidents should be coordinated across authorities and developed closely with operators and other stakeholders to avoid inconsistencies.

Broader rules on planning, permitting and emergency traffic management should also enable timely investment in resilience and proportionate action during major disruptions.

Building on this research, the GSMA has published a set of policy principles to guide governments and regulators in designing frameworks which strengthen mobile network resilience.

Copyright © 2026 GSM Association