we4u Insights

April 2026

Resilience in Telecom: Navigating Complexity in Uncertain Times

Resilience in telecom has always meant that services work reliably across networks, IT systems, and operations.

What has changed is not the expectation, but the conditions under which this reliability must be delivered.

Today, resilience depends on how operators manage:

- continuous system change
- growing dependencies across partners and platforms
- increasing operational complexity

This shifts the main source of incidents: failures are less about isolated faults and more about how systems interact during change and across dependencies.

Resilience becomes visible when systems are stressed and when organisations have to respond.

> *"Resilience most often breaks at interfaces... not through cyberattacks, but through faulty updates, vendor software issues, and cascading effects."*
> *Alois Schrems, Senior Advisor – Resilience*

IN THIS ISSUE

Resilience has become a board-level priority but remains difficult to manage in practice.

In this issue, we explore:

- how cost pressure, operating models, and regulation reshape resilience
- where and how resilience actually breaks in practice
- what recent incidents reveal about real-world failure patterns
- and how operators can strengthen resilience beyond concepts and compliance

The focus is not on theory, but on where resilience actually holds or fails and what this means for decision-making.

Executive Summary

Resilience as a Strategic Management Priority

Telecom networks are increasingly defined by continuous change, growing dependencies, and regulatory pressure (e.g. NIS2). In this environment, resilience is no longer an implicit outcome of engineering. It has become a board-level topic that requires active management of trade-offs.

Key Insights for Decision-Makers:

- **Resilience is determined in execution, not design**
  Stability is not a static feature of system architecture; true resilience is demonstrated in how an organization handles change and operates under real-world pressure.
- **Failures occur at interfaces**
  Disruptions are rarely caused by isolated faults. They emerge during software updates, legacy-to-modern transitions, and across vendor and partner boundaries.
- **Resilience shifts from control to coordination**
  With asset-light and partner-based models, resilience becomes an ecosystem challenge. Success depends on how effectively organisations act across multiple parties.
- **Resilience is the ability to recover and adapt**
  It is not the absence of failure, but the capability to respond, recover, and continue operations under stress.
- **Cost and resilience are in tension**
  Efficiency measures often remove buffers and fallback options. Resilience must be explicitly governed to avoid increasing systemic fragility.

Bottom line:
Resilience is not built in. It is managed. Organisations that treat it as an execution capability are better prepared for real-world disruptions.

Introduction

Resilience is becoming an explicit management topic in telecom.

Across operators, it is increasingly defined through KPIs, governance frameworks, business continuity processes, and regulatory requirements.

At the same time, the conditions under which resilience must be delivered have fundamentally changed.

Operators are managing:

- continuous system change across IT and networks
- increasing dependency on vendors, partners, and shared infrastructure
- growing regulatory pressure
- sustained cost and efficiency programmes

These dynamics create a new reality:

Resilience is not determined in system design.
It is determined in how systems and organisations perform under real operating conditions.

This raises a critical question:

Where does resilience actually hold — and where does it break — in practice?

What We See In The Market

Resilience is no longer implicit. It is negotiated under constraints.

Today, resilience is embedded in governance while operators face competing pressures:

- cost reduction programmes
- large-scale transformation
- increased partner dependency
- stricter regulation

This creates a fundamental shift:

Resilience is now in direct competition with other priorities. It becomes a decision topic shaped by trade-offs.

This is visible in everyday decisions:

- IT simplification reduces complexity but removes fallback options
- asset-light models improve efficiency but increase dependency
- cost reduction increases efficiency but reduces execution capacity

Operators integrate resilience into broader programmes, but this changes its nature:

Resilience is no longer assumed. It is considered and negotiated case by case.

We see several key aspects that impact this negotiation.

Cost discipline directly shapes resilience decisions	Cost reduction and simplification continue to shape telecom operating models. Cost is a filter that actively shapes which resilience measures are implemented and which are deferred.
Asset-light models turn resilience into a coordination problem	Infrastructure sharing and outsourcing shift resilience from ownership to coordination. Operators such as Vodafone and Deutsche Telekom illustrate different approaches, but the underlying dynamic is the same: resilience increasingly depends on how effectively multiple parties act together. This becomes visible in outage resolution, investment decisions, and rollout flexibility; areas where responsibilities are distributed but outcomes remain shared.
Resilience is becoming a compliance and audit topic	With NIS2 and similar frameworks, resilience becomes enforceable. Operators must: implement risk management, define governance, report incidents and demonstrate recovery capabilities. This increases transparency and accountability, but also shifts resilience towards governance and documentation. This then also bears the risk that formal compliance outpaces actual operational capability.
Physical infrastructure remains a dominant resilience risk	Despite the focus on cyber and IT, many incidents still originate from the physical layer. ENISA identifies cable damage as the most frequent technical cause of incidents and reports a sharp increase in incidents linked to natural phenomena, with significant service impact.

Resilience is gaining importance, but so is the pressure on systems and organisations. The real test is not in planning, but in where and how things break in practice.

Insight Spotlight

Where Resilience Actually Breaks

Change is the most fragile moment in otherwise stable systems

Several recent disruptions show that resilience issues are often triggered not by external attacks, but by internal changes.

In Spain, a Telefónica network update led to widespread disruption of fixed services and temporarily affected access to emergency number 112 in several regions. The issue was traced to a technical failure during update activities, requiring isolation of affected nodes and gradual recovery.

Similarly, Vodafone UK experienced a major outage affecting broadband and mobile services, caused not by a cyberattack, but by a non-malicious software issue at a vendor partner.

These are not isolated cases. ENISA data shows that software changes and updates are among the most significant contributors to service disruption in terms of impact.

Resilience is **not tested in stable conditions but during change**, where small errors can trigger large-scale effects.

Dependencies turn incidents into coordination problems

As operating models become more distributed, many resilience issues are no longer purely technical. They are coordination challenges across organisations.

ENISA reports a significant increase in incidents linked to third-party failures, reflecting growing dependency on vendors, partners, and shared infrastructure.

In practice, this becomes visible when:

- software issues originate at vendor level but affect operator services
- recovery depends on multiple parties with different responsibilities
- accountability is contractually defined but operationally fragmented

In practice, operators address this through SLAs, governance structures, and joint processes. But these mechanisms structure coordination. They do not eliminate dependency.

In multi-party environments, resilience depends less on redundancy and more on how quickly and clearly organisations can **act together under pressure**.

The physical layer remains a major and underestimated risk

The physical layer remains a key risk area with increasing impact from natural events. What makes this special is that these risks are inherently harder to control and often lie outside the direct influence of telecom operators.

They require coordination with external stakeholders (e.g. utilities, authorities) and investment in physical redundancy (e.g. routes or energy backups).

This shows that resilience is not only a digital challenge. It is also a physical and cross-sector one, often **outside the core focus of transformation programmes**.

Security measures themselves can reduce availability

Resilience is often framed as protection against cyber threats. In practice, the response to such threats can itself create service impact.

In a 2025 incident, Orange isolated affected systems following a cyberattack. While this contained the threat, it also led to disruptions in certain services and platforms.

This reflects a fundamental trade-off:

- “isolate aggressively” protects integrity, but reduces availability
- “keep systems running” maintains service, but risks further compromise

These decisions are not technical; they are **policy and governance decisions**, often taken under time pressure. Resilience is not about avoiding trade-offs. It is about **making them explicitly and consistently when it matters most**.

we4u Advisor Perspectives

To complement our analysis, we asked two of our resilience experts, Alois Schrems and Thomas Müller, for their perspective on where resilience actually breaks and what operators tend to underestimate in practice.

Alois Schrems

Senior Advisor – Resilience, Infrastructure & Crisis Management

Alois Schrems brings deep expertise in telecom infrastructure, resilience strategy, and crisis management. With a background spanning network operations, transformation, and standardisation, he focuses on how resilience is implemented and sustained under real-world conditions. His perspective combines technical depth with practical experience in managing complex, high-impact situations.

Thomas Müller

Senior Advisor – Risk, Governance & Operational Resilience

Thomas Müller specialises in governance, risk, and operational resilience in telecom and IT environments. His experience covers large-scale operations, transformation, and the integration of resilience into management systems and decision-making. He focuses on how organisations translate resilience requirements into executable processes and effective response capabilities.

Resilience is determined by how organisations manage change, coordination, and dependencies under pressure.

Both perspectives strongly reinforce a central observation of this issue: resilience is not determined in design but in execution.

In practice, this becomes critical when systems are changed, responsibilities are distributed, and dependencies must be actively managed.

Alois Schrems highlights the technical and systemic dimension:

> *"Resilience most often breaks at interfaces, in highly complex legacy environments, and through hidden dependencies... it is rarely zero-day cyberattacks, but faulty updates, vendor software issues, or cascading effects across layers."*

Thomas Müller describes the same pattern from an operational perspective:

> *"It most often breaks at the interfaces: during change, across legacy-to-modern transitions, and where operator, vendor, and partner responsibilities meet."*

Resilience is therefore not primarily a question of architecture. It is a question of how organisations manage systems under real operating conditions.

The underestimated trade-off: speed and efficiency vs resilience

Both advisors emphasise that resilience is not lost by accident. It is often the result of accumulated trade-offs.

Operators are simultaneously driving:

- faster time-to-market
- increased automation and outsourcing
- cloudification and virtualisation

Alois Schrems points to the hidden effect of this dynamic:

> *"Increasing complexity without matching investment in operational control erodes resilience… the hidden operational costs only become visible in crisis situations."*

Thomas Müller complements this from an efficiency perspective:

> *"Cost reduction, simplification, outsourcing, and automation improve performance, but they also remove buffers, local knowledge, and fallback options."*

Resilience is weakened not by single decisions but by the accumulation of optimisation decisions over time.

From engineering topic to governed capability

Both perspectives confirm a fundamental shift: resilience has moved beyond engineering.

Thomas Müller frames it clearly:

> *"Resilience has moved from an engineering topic to a board-level issue… requiring explicit governance, evidence, and accountability."*

At the same time, Alois Schrems highlights a structural change in risk patterns:

> *"The strict separation between IT and network operations has effectively disappeared… this cyber-physical convergence has become the dominant risk pattern."*

Resilience is no longer embedded in systems. It is actively governed across technology, organisation, and partners.

What improves resilience in practice

A consistent message from both advisors is that resilience does not improve through documentation alone but through execution.

This includes:

- strengthening change and release discipline
- making dependencies transparent
- enabling fast, decentralised decision-making
- and continuously testing systems under realistic conditions

Alois Schrems emphasises the importance of realism and culture:

> *"Operators need to move away from theoretical paper concepts toward continuous stress testing… and build a culture where trained teams can make fast decisions under pressure."*

Thomas Müller adds the operational perspective:

> *"Resilience improves when operators can execute change safely and coordinate quickly across internal and external parties."*

Resilience improves when organisations can act effectively under pressure, not when processes look complete on paper.

A common misconception: resilience is not about preventing failure

Both advisors challenge a persistent misconception.

Alois Schrems states:

> *"A common misconception is equating resilience with robustness… real resilience means accepting that systems will fail and being able to recover and adapt."*

Thomas Müller reinforces this view:

> *"Resilience is not mainly about redundancy. It is an operating capability: making sound decisions under stress and recovering fast."*

Resilience is about managing failure and recovering effectively, not about avoiding failure.

Takeaway

Across all examples, observations and perspectives, a consistent pattern emerges.

Resilience does not primarily fail at the level of design or strategy, and it is not a matter of IT nor is it fully controllable by operators.

It breaks where:

- systems are changed
- responsibilities are distributed
- dependencies are activated under stress

In these moments, resilience depends on:

- the quality of change and release processes
- clarity of ownership and decision-making
- readiness of coordination across internal and external parties
- and the ability to respond quickly to physical disruptions.

For operators, the key challenge is no longer to design resilient systems in isolation. **It is to ensure that resilience holds under real operating conditions**:

- during upgrades and migrations
- across vendor and partner ecosystems
- under cyber pressure and incident response
- and in the face of physical and environmental disruption

This shifts the focus of resilience from architecture to **execution capability**:

- safe change becomes as critical as stable design
- coordination becomes as important as control
- and physical infrastructure becomes as relevant as digital systems

Operators that recognise and address these dimensions explicitly tend to manage resilience.
Where they remain implicit, resilience issues tend to surface at exactly the moments where systems are under the most pressure.

Worth Your Attention

- ENISA – Telecom Security Incidents Report 2024
- BEREC – Network Resilience Workshop Report
- Vodafone, Deutsche Telekom, Orange, Telefónica, BT – Annual Reports
- EU Commission – NIS2 Directive and related initiatives

Updates from we4u

Business Resilience – from concept to execution

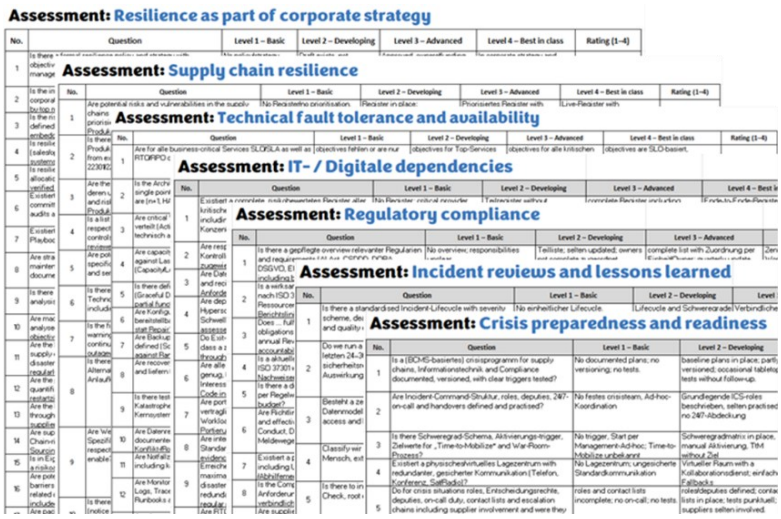
In line with the growing importance of resilience and the gap between design and execution we see the need for a more integrated and operational approach.

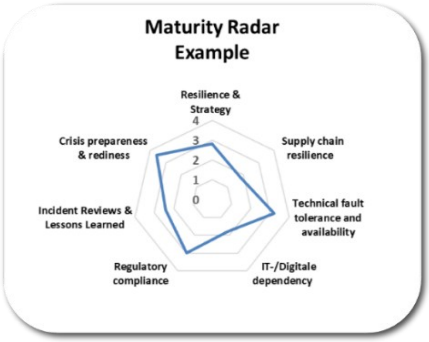
With the combined expertise of our Senior Advisors from operations, procurement, technology, risk management, regulation and resilience we have shaped a Business Resilience approach that focuses on:

- linking resilience to strategy and decisions
- making dependencies visible and manageable
- strengthening operational resilience through testing and readiness
- aligning compliance, risk, and execution

Based on real-life Tier-1 telco and hands-on crisis and transformation experience we support organisations from **quick assessment to implementation**.

Starting from analysis of the own company's resilience in critical dimensions of corporate strategy, supply chain, technical faults, IT-/Digital dependencies, regulation, lessons learned and crisis readiness we make weaknesses and vulnerabilities visible so that effective improvements can be found and realized.





We Endeavor for you

Ruediger Koester

Managing Director and Co-owner
Endeavor 4U GmbH
ruediger.koester@we4u.io

+43 676 8200 7700

www.we4u.io

Thomas Stuettgen

Managing Director and Co-owner
Endeavor 4U GmbH
thomas.stuettgen@we4u.io

+49 151 5235 7509

www.we4u.io