

UK Critical National Infrastructure Pressure Map & Resilience Framework



By Mark Conway,

Copyright Oak Consult, April 2026



Contents

Leadership Summary	3
Section 1- Opening — The Shift Has Already Happened	5
Section 2 - How to Use This Document	7
Section 3. The Model — Understanding the Framework	8
Section 4. The CNI Pressure Heatmap	9
Section 5. Sector Deep Dives — Where Pressure Becomes Real.....	10
5.1 Energy — The System Under Pressure	11
5.2 Communications — The System That Connects Everything	14
5.3 Transport — The System That Moves Everything	18
5.4 Water — The System That Sustains Everything	21
5.5 Health — Where System Failure Becomes Human Impact	24
5.6 SaaS / Digital Operating Layer — The System That Runs the Organisation	27
Section 6 - How Pressure Moves — Interdependency in Practice	31
6.1 Core System Relationships	31
6.2 Interdependency Matrix (High-Level)	32
6.3 Dependency Tolerance (Critical Concept)	32
6.4 Scenario Chains — How Failure Travels	33
6.5 What This Means for Leaders	34
Section 7 - Scenario Testing — Turning Insight into Action	35
7.1 How to Use Scenario Testing	35
7.2 Scenario 1 — Energy Constraint (Power Rationing)	36
7.3 Scenario 2 — Communications Degradation	37
7.4 Scenario 3 — Transport Constraint (Fuel / Movement Disruption)	38
7.5 Scenario 4 — SaaS / Digital Operating Layer Disruption	39
7.6 What Scenario Testing Reveals	40
7.7 What Good Looks Like	40
Section 8 – The Infrastructure Resilience Test.....	41
8.1 The Structure of the Test	41
8.2 The 10 Questions Every Leadership Team Should Answer	42
8.3 The Resilience Snapshot	43
8.4 Sector-Specific Prompts (Applied Layer)	44
8.5 How to Use This in Practice.....	44
Section 9 - The 30–60–90 Day Reset — Moving from Awareness to Action	45
9.1 First 30 Days — Clarity	45
9.2 Next 60 Days — Decisions	46
9.3 By 90 Days — Alignment	46
9.4 What This Reset Does Not Do	47
9.5 What Good Looks Like After 90 Days	47
Section 10 - Final Leadership View — What This Means Now.....	48



Leadership Summary

In 2026, access and continuity have replaced efficiency as the primary strategic constraint.

Most organisations still operate as if infrastructure is stable and available. It is no longer.

Scope and Focus

This document does not attempt to cover every UK Critical National Infrastructure sector in equal depth.

The UK's CNI landscape includes additional sectors such as Defence, Emergency Services, Finance, Government, Space, Chemicals, and Civil Nuclear, all of which are strategically important and carry their own resilience considerations.

However, this framework deliberately focuses on a smaller set of core systems:

- Energy
- Communications
- Transport
- Water
- Health
- SaaS / Digital Operating Layer

These have been selected not because they are more important in isolation, but because they represent the **primary pressure transmission layers** within the system.

They are the points at which constraint is most likely to:

- originate
- propagate across sectors
- and be experienced directly by organisations, customers, and employees

Other sectors, including Defence, Finance, Government, and Emergency Services, are highly dependent on these underlying systems and are therefore incorporated implicitly through interdependency rather than treated as separate analytical layers.

This is a deliberate focus.

The objective is not to catalogue risk, but to concentrate leadership attention on the systems that determine whether the organisation can continue to operate when pressure builds.

Where Pressure Is Concentrated

- **Energy** — cost volatility, access constraints, system-wide dependency
- **Communications** — coordination risk, cloud concentration, degraded performance
- **Transport** — fuel exposure, workforce mobility, logistics fragility
- **SaaS / Digital Layer** — operational control, vendor concentration, access risk

These are not isolated risks. They are **interdependent pressures that move through the system**. They will not present themselves one at a time.

What This Means

- Disruption is rarely binary
 - Systems degrade before they fail, often without clear visibility
 - Impact is experienced first through customers and employees, not dashboards
 - Under constraint, the quality of decisions matters more than the quality of plans
-

Three Questions Every Leadership Team Should Answer Now

1. If access to a critical dependency was constrained, **what fails first?**
 2. Do we know **where we sit in the priority queue** under disruption?
 3. Have we already decided **what we protect vs what we let go?**
-

What To Do Next

- Run the Infrastructure Resilience Test
- Identify your top 3 dependencies
- Test one real scenario within 30 days





Section 1- Opening — The Shift Has Already Happened

For many years, infrastructure sat quietly in the background of most organisations. It was assumed to be stable, dependable, and largely outside the scope of day-to-day leadership attention, only really surfacing when something went wrong or when a major investment decision was required.

That assumption no longer holds.

Infrastructure is no longer a supporting layer that enables the organisation to operate efficiently. It has become a primary determinant of whether the organisation can operate at all, and under what conditions it can continue to do so when pressure begins to build.

This shift has not been driven by a single event or a sudden change in direction. It is the cumulative effect of multiple pressures converging at once.

Energy is no longer a stable input. It has become a source of volatility in both cost and access, shaped increasingly by global dynamics rather than local control. The UK felt this acutely following the Russia–Ukraine conflict, where wholesale gas prices surged and translated directly into operational cost pressure across sectors. Even as prices stabilised, the underlying exposure remains. Energy is now a strategic dependency, not a background utility.

Communications infrastructure is also changing in character. It is no longer neutral. The UK's reliance on a small number of hyperscale cloud providers, combined with the removal of Huawei from 5G networks and ongoing concern around subsea cable resilience, has introduced a new layer of concentration and security risk. Organisations are more connected than ever, but also more dependent on infrastructure they do not control.

Transport systems are under sustained strain. Fuel cost volatility, driver shortages following Brexit and COVID, and ongoing pressure on logistics networks have exposed how little slack exists in the system. The HGV driver shortage in 2021, which led to fuel distribution disruption and visible shortages at petrol stations, was a clear demonstration of how quickly transport constraints can translate into public and operational impact.

At the same time, the software platforms through which organisations actually function have become more centralised and more critical. The global Microsoft outage in July 2024, triggered by a CrowdStrike update, disrupted airlines, healthcare services, financial systems, and public services across the UK. Systems did not fail in isolation. Entire operating environments became unavailable simultaneously, exposing how dependent organisations have become on a small number of interconnected digital platforms.

Individually, each of these pressures can be managed. Taken together, they change the nature of the operating environment in a more fundamental way.

Individually, each of these pressures can be managed. Taken together, they change the nature of the operating environment in a more fundamental way.

The challenge is not that systems fail more often. It is that they behave differently under pressure. Rather than stopping completely, they degrade. Performance becomes inconsistent, coordination becomes harder, and visibility reduces at the exact point where clarity is most needed. Under those conditions, organisations rarely come to a halt. Instead, they continue to operate, but with slower responses, poorer decisions, and increasing strain across both customers and employees. That is where value is quietly lost.

Many organisations are still operating as if infrastructure is stable and available. They continue to optimise for efficiency, cost, and utilisation, assuming that availability will hold. In the current environment, that assumption creates exposure. When access to a critical dependency becomes constrained, efficiency does not protect the organisation. It amplifies the impact of that constraint.

At the centre of this shift is interdependency. Energy powers communications, communications coordinate transport, transport enables delivery, and digital systems sit across all of them, shaping how organisations function day to day. When any one of these is placed under strain, the effects do not remain contained. They move through the system, often quickly and not always in ways that are immediately visible.

For leaders, this changes the nature of resilience. It can no longer be treated as a set of controls, a documented plan, or a function that sits alongside the business. It becomes a characteristic of how the organisation thinks and decides under pressure. In practice, that means understanding dependencies, recognising where constraint will be felt first, and making deliberate choices about what will be protected and what will not.

This is where most organisations are not yet ready. The issue is rarely a lack of awareness. Risks are generally understood, and dependencies are often known at a high level. The gap sits between understanding and decision-making. Trade-offs have not been fully confronted, priorities have not been explicitly agreed, and in many cases, the organisation has not decided how it will respond when multiple constraints emerge at the same time.

This document has been designed to address that gap.

It does not attempt to catalogue every possible risk or predict specific outcomes. Instead, it provides a structured way to understand where pressure is concentrating, how it moves through the system, and what that means for organisations operating within those conditions. More importantly, it is intended to change the nature of the discussion, shifting it away from abstract questions about what might happen and towards practical decisions about how the organisation will respond when it does.

If it does not change a decision, it has not done its job.





Section 2 - How to Use This Document

This document is not intended to be read from start to finish in a single sitting, nor is it designed as a linear argument that builds to a single conclusion. It has been structured so that leaders can move through it in different ways, depending on the question they are trying to answer or the discussion they are trying to have.

At its core, it is a tool to support board-level thinking, scenario exploration, and more grounded decision-making in an environment that is becoming harder to interpret through traditional lenses.

A useful starting point for most readers is the heatmap. This provides a quick view of where pressure is currently concentrated across the core infrastructure sectors and helps to focus attention on the areas that are most likely to affect the organisation. From there, it becomes easier to move into the sector sections that are most relevant, using them to build a clearer picture of dependencies, risks, and how disruption might manifest in practice.

The board-level questions within each section are deliberately direct. They are not intended to be theoretical prompts, but to be used in real discussions, where assumptions can be challenged and gaps can be exposed. In many cases, the value comes less from the answers themselves and more from the conversation they force.

The scenario sections then provide a way of stepping out of abstract discussion and into more concrete thinking. By exploring how disruption might unfold, how quickly it might be felt, and how the organisation would respond, they help to bridge the gap between understanding and action.

Finally, the Infrastructure Resilience Test offers a simple way of pulling those insights together. It is not designed to produce a definitive score, but to give a clear sense of where the organisation stands, where confidence is justified, and where it is not.

Used well, this document should not sit on a shelf. It should be returned to, challenged, and applied to real situations as they emerge. Its value lies not just in what it contains, but in how it is used to shape thinking and decisions over time.



Section 3. The Model — Understanding the Framework

The framework that underpins this document is intentionally simple, but it has been designed to bring consistency and structure to what can otherwise become a fragmented and subjective discussion.

Its purpose is not to produce precise measurements, but to provide a shared way of thinking about where pressure exists, how it behaves, and what it is likely to mean in practice.

Each sector is considered across five core dimensions.

1. **Likelihood** reflects the probability that meaningful disruption or constraint will occur within the operating environment. This is not about rare or extreme events, but about credible conditions that organisations may reasonably expect to encounter.
2. **Impact** considers the severity of the consequences if disruption does occur, including operational, commercial, and, where relevant, societal effects. Some sectors may experience frequent issues with limited impact, while others may face less frequent disruption but with far more serious consequences.
3. **Interdependency** captures the extent to which disruption in one area affects others. In a tightly connected system, this becomes one of the most important dimensions, as it determines how quickly and widely pressure can propagate.
4. **Visibility** reflects how easily emerging issues can be detected and understood in advance. Low visibility increases risk, not necessarily because the underlying issue is more severe, but because it reduces the time available to respond effectively.
5. **Resilience** considers the current ability of the system to absorb disruption, drawing on factors such as redundancy, preparedness, and the capacity to adapt under pressure.

Alongside these dimensions, the model applies a set of overlay lenses that translate system-level risk into real-world consequences. The **Customer Spectacles** lens focuses on how disruption is experienced externally, through service, reliability, and trust. The **Employee** lens looks at how pressure affects the workforce, including the ability to operate, cost pressures, and day-to-day strain. The **Social and Workforce Stability** lens considers broader behavioural effects, particularly where disruption may influence availability, coordination, or public response. The **SaaS or Digital Operating Layer** lens reflects the reality that most organisations now operate through software platforms that introduce their own forms of dependency and control.

Taken together, these elements create a model that is less about predicting specific outcomes and more about improving the quality of discussion. It provides a consistent structure within which leaders can explore scenarios, compare areas of risk, and, most importantly, make better decisions in conditions that are unlikely to be stable or predictable.



Section 4. The CNI Pressure Heatmap

This is the entry point.

Relative assessment of systemic pressure across key sectors

SECTOR	LIKELIHOOD (Relative)	IMPACT (Relative)	INTERDEPENDENCY (Relative)	VISIBILITY (Relative)	RESILIENCE (Relative)	SCORE (Max 25)	RAG	KEY PRESSURE
ENERGY	High	High	High	Medium	Medium	22	●	Fuel volatility, global supply exposure
COMMUNICATIONS	High	High	Very High	Low	Medium	23	●	Subsea, cloud concentration, cyber
TRANSPORT	High	High	Very High	Medium	Medium-Low	22	●	Fuel, workforce, logistics fragility
WATER	Medium	High	High	Medium	Medium	19	●	Energy dependency, infrastructure age
HEALTH	Medium	High	High	Medium	Medium	19	●	Capacity strain, system dependency
SAAS / DIGITAL	High	High	Very High	Low	Medium	23	●	Cloud control, vendor concentration

SCORE GUIDE (Max 25)



21 – 25
Extreme Pressure



16 – 20
High Pressure



11 – 15
Moderate Pressure



0 – 10
Lower Pressure

Scoring: Likelihood + Impact + Interdependency (moderated by Visibility and Resilience)

Points to Note:

1. Score derived from combined assessment of Likelihood, Impact, and Interdependency, moderated by Visibility and current Resilience. Designed to indicate relative system pressure rather than precise measurement for your organisation.
2. Finance, Defence, Government, and Emergency Services are treated in this model as dependent layers within the system, rather than primary sources of pressure.



Section 5. Sector Deep Dives — Where Pressure Becomes Real

The heatmap provides a high-level view of where pressure is concentrated. What it does not show is how that pressure behaves in practice. This section breaks the system down into its core components, examining each sector in more detail to understand:

- where it is under strain
- how it connects to other sectors
- and how disruption is likely to manifest

These sections are not designed to be read in isolation, but to be used selectively, depending on where the organisation is most exposed. Some readers will focus on one or two sectors that are directly relevant. Others will move across multiple sections to understand how dependencies interact.

Each section follows a consistent structure:

- current pressure
- key signals
- interdependencies
- real-world impact
- leadership questions

The intention is not to provide a complete technical analysis. It is to translate system-level pressure into something that can be understood, discussed, and acted upon at a leadership level.



5.1 Energy — The System Under Pressure

Energy is not simply another infrastructure sector. It is the **foundational dependency across all others**.

When energy is stable, disruption elsewhere can often be absorbed, but when energy is constrained, disruption **propagates rapidly** across the system.

In 2026, the nature of energy risk has shifted. It is no longer defined purely by supply failure, but by:

- **cost volatility**
- **access constraints**
- **geopolitical exposure**
- **transition complexity**

The result is not always immediate failure. More often, it is **progressive constraint**.

Current Pressure Summary

RAG Status: High Pressure

Energy sits at the centre of the UK's infrastructure risk landscape due to:

- global supply chain exposure
- fuel price volatility
- interdependency across all CNI sectors
- increasing system complexity driven by transition

Key Signals

- Global energy flows remain exposed to geopolitical disruption and routing constraints
- Fuel price volatility is transmitting rapidly into operational and workforce costs
- UK energy resilience is now an explicit policy priority, not an assumption
- Transition to renewable and distributed energy is increasing system complexity
- Backup and contingency systems (generators, fuel supply) are themselves dependent on constrained inputs

Interdependencies (Where Energy Flows Next)

Energy is a **critical upstream dependency** for:

- **Communications** → telecoms, mobile networks, data centres
- **Transport** → fuel distribution, logistics, workforce mobility
- **Water** → pumping, treatment, distribution
- **Health** → hospitals, life-critical equipment, digital systems
- **SaaS / Digital** → data centre operation and cooling

Key Insight

Energy disruption rarely appears as a single point of failure. It appears as simultaneous constraint across multiple systems.

Customer Spectacles

Customers do not experience “energy pressure”. They experience:

- increased pricing
- delayed service delivery
- reduced availability
- inconsistent reliability

Even where supply is maintained, **confidence erodes** as performance becomes less predictable.

Employee Impact

Energy pressure reaches organisations through their workforce before it reaches their systems.

Key effects:

- rising cost of commuting (fuel exposure)
- pressure on shift-based and field roles
- reduced workforce flexibility
- increasing reliance on remote working as a cost and resilience lever

Workforce viability becomes an energy issue.

Social & Workforce Stability

Energy is one of the few sectors with:

- direct household impact
- visible price signals
- historical precedent for disruption

Under sustained pressure, this creates plausible scenarios such as:

- fuel distribution disruption
- localised access constraints
- increased workforce absence or resistance

Leadership Reality

Energy pressure does not need to escalate into crisis to disrupt operations. Sustained constraint is sufficient.

What This Looks Like in Practice

Energy disruption typically manifests as:

- rising operating costs
- reduced operational flexibility
- pressure on workforce and logistics
- increasing need for prioritisation

Not immediate system failure, but **progressive loss of efficiency, then effectiveness.**

Board-Level Questions

1. Access & Priority

- What rights do we have to energy access under constrained conditions?
- Are we considered a critical or priority organisation?
- Do we support sectors that would be prioritised (NHS, emergency services, public sector)?
- If supply is rationed, where do we sit in the queue?

2. Operational Continuity

- What happens to our operations if energy availability or affordability is reduced?
- Which parts of the business fail first?
- Do we have defined minimum operating levels?

3. Fuel Strategy

- Should we hold strategic fuel reserves?
- Do we have guaranteed supply agreements in place?
- Have we explored priority access arrangements with suppliers?
- What is our exposure to spot pricing versus contracted supply?

4. Workforce Viability

- Can our workforce sustain current commuting costs?
- Which roles are most exposed to fuel dependency?
- What flexibility (WFH, shift redesign) can we introduce quickly?
- What early indicators would signal workforce strain?

5. Logistics & Field Operations

- How dependent are we on fuel for service delivery?
- Can we reduce unnecessary travel without damaging outcomes?
- Where are we dependent on third-party logistics providers?

6. Customer Impact

- What will customers experience first under energy constraint?
- How will service levels change?
- How will this affect trust and retention?

7. Scenario Readiness

- Do we have pre-agreed responses to energy disruption scenarios?
- Who makes decisions under pressure?
- How quickly can those decisions be enacted?

Common Failure Points

Across organisations, energy risk is often mismanaged through:

- assuming availability equals access (**A — Access**)
- removing buffers in pursuit of efficiency (**B — Buffers**)
- underestimating workforce exposure (**W — Workforce**)
- relying on pricing mechanisms rather than operational planning (**H — Hedging**)

Final Insight - Energy disruption is not defined by whether power remains on. It is defined by whether organisations can continue to operate effectively under constraint.



5.2 Communications — The System That Connects Everything

Communications is no longer just a supporting infrastructure. It is the **operating backbone of modern organisations**.

Every sector relies on it:

- to connect systems
- to coordinate operations
- to deliver services
- to access data

In 2026, the risk profile of communications has shifted. It is no longer defined by uptime alone. It is defined by:

- dependency concentration
- external control
- degraded performance scenarios
- and increasing exposure to hybrid threats

The most important change is this:

Communications failure is rarely binary. It degrades before it breaks.

Current Pressure Summary

RAG Status: High Pressure

Communications sits alongside Energy and Transport as one of the most critical and exposed sectors due to:

- reliance on subsea and physical infrastructure
- concentration of data centre capacity
- dependency on hyperscale cloud providers
- systemic importance across all other sectors

Key Signals

- Increasing global focus on subsea cable vulnerability and physical infrastructure exposure
- High concentration of UK data centre capacity in specific geographic regions
- Growing reliance on a small number of hyperscale cloud providers
- Increasing alignment of communications infrastructure with national security concerns
- Expansion of hybrid threat models combining cyber, physical, and systemic disruption

Interdependencies (Where Communications Flows Next)

Communications is a **core dependency layer** for:

- **Energy** → grid management, monitoring, and control systems
- **Transport** → signalling, logistics coordination, traffic systems
- **Health** → patient systems, telecare, diagnostics, coordination
- **Water** → monitoring, control, and distribution systems
- **SaaS / Digital Operating Layer** → access to all core business systems

Key Insight

Communications does not simply support other sectors; it enables them to function. Loss of communications does not stop systems immediately; it removes the ability to coordinate them effectively.

SaaS / Digital Operating Layer (Critical Overlay)

Modern organisations do not operate directly on infrastructure. They operate through software layers delivered over it. This includes:

- ERP platforms
- CRM and customer service systems
- Office productivity suites
- email and marketing platforms
- finance systems (invoicing, payroll, collections)
- middleware and integration layers

Key Insight

Most organisations believe they run on infrastructure. In reality, they run on services they do not control.

Risk Characteristics

- Access can be constrained without full outage
- Performance degradation can impact operations significantly
- Vendor concentration introduces systemic exposure
- Jurisdictional control creates uncertainty over long-term access

Customer Spectacles

Customers do not experience “communications disruption.” They experience:

- inability to access services
- failed transactions
- inability to contact organisations
- degraded or inconsistent performance

The impact is immediate and visible. Unlike energy or transport, there is little buffering. The effect is direct.

Employee Impact

Communications is central to how modern work is performed. Disruption results in:

- inability to access core systems
- breakdown in internal coordination
- failure of remote working
- reduced productivity and increased error rates

Where systems degrade rather than fail, the effect is often confusion, duplication of effort and operational slowdown.

Social & Workforce Stability

Communications plays a stabilising role in modern society. When it degrades:

- visibility reduces
- coordination becomes more difficult
- uncertainty increases

In combination with pressure in other sectors, this can amplify:

- operational disruption
- customer dissatisfaction
- workforce stress

What This Looks Like in Practice

Communications disruption typically manifests as:

- slower systems
- intermittent failures
- delayed data
- unreliable connections

Rather than total outage. This creates a more complex challenge. The organisation continues to operate, but less effectively.

Board-Level Questions

1. Dependency Awareness

- Which of our operations depend on continuous connectivity?
- What happens if connectivity is degraded, not lost?

2. Control vs Exposure

- Which parts of our communications stack do we control?
- Where are we fully dependent on third-party providers?

3. Concentration Risk

- Are we dependent on a small number of providers or locations?
- What happens if a key data centre region becomes unavailable?

4. SaaS Dependency

- Which critical processes rely entirely on SaaS platforms?
- Do we have any fallback capability outside cloud-based systems?

5. Sovereignty & Control

- Do we understand the jurisdictional exposure of our systems?
- Is our dependency on external providers a conscious decision?

6. Operational Continuity

- Can we operate effectively with reduced connectivity?
- Do we have defined degraded-mode operating procedures?

Board-Level Questions Continued

7. Workforce Impact

- What happens to productivity if systems become unreliable?
- Can teams operate without real-time access to systems?

8. Customer Impact

- What fails first from a customer perspective?
- How quickly would customers notice?
- How do we communicate during communications disruption?

9. Scenario Readiness

- Have we tested communications degradation scenarios?
- Who makes decisions when systems are partially functional but unreliable?

Common Failure Points

Organisations typically underestimate communications risk by:

- equating uptime with resilience
- failing to map dependency on specific providers and regions
- assuming SaaS platforms are inherently resilient
- ignoring degradation scenarios
- underestimating the impact of concentration risk

Final Insight

Communications disruption is not defined by loss of connectivity. It is defined by loss of coordination. Organisations rarely fail because systems stop. They fail because they can no longer operate effectively through them.





5.3 Transport — The System That Moves Everything

Transport is not just a supporting function. It is the physical delivery mechanism of the entire system. It enables:

- movement of people
- distribution of goods
- delivery of services
- maintenance of infrastructure

In 2026, transport risk is no longer defined by capacity or efficiency. It is defined by:

- fuel dependency
- workforce viability
- network fragility
- and cost-driven constraint

Unlike other sectors, transport is where disruption becomes **visible first**.

Current Pressure Summary

RAG Status: High Pressure

Transport sits at the centre of operational risk due to:

- direct dependency on fuel and energy
- reliance on a distributed and exposed workforce
- tight coupling to supply chains
- limited buffering in most systems

Key Signals

- Sustained fuel price volatility directly impacting logistics and field operations
- Increasing cost pressure on transport-heavy industries
- Continued reliance on just-in-time supply chains with limited buffers
- Workforce pressures across driving, logistics, and operational roles
- Critical dependence on a small number of major nodes (ports, routes, hubs)

Interdependencies (Where Transport Connects)

Transport acts as the **linking layer** between sectors:

- **Energy** → distribution of fuel and infrastructure maintenance
- **Communications** → access for installation, repair, and field operations
- **Water** → movement of materials, maintenance teams
- **Health** → staff, patients, supplies, emergency response
- **SaaS / Digital Operating Layer** → indirectly through logistics coordination

Key Insight

Transport does not just connect systems. It enables them to function physically. When transport degrades, systems do not stop immediately. They become progressively harder to sustain.

Customer Spectacles

Customers do not experience “transport disruption”. They experience:

- delays
- missed appointments
- reduced availability
- rising costs

Transport is one of the most visible forms of infrastructure failure. It is where disruption becomes real.

Employee Impact

Transport is directly linked to workforce viability. Key effects include:

- increased cost of commuting
- reduced accessibility to workplaces
- pressure on shift-based roles
- increased fatigue and reduced flexibility

For many roles, especially field-based or operational, transport disruption equals **inability to work**.

Social & Workforce Stability

Transport is often the point at which pressure becomes visible at scale.

Under sustained stress, it creates plausible scenarios such as:

- localised disruption or blockades
- reduced workforce participation
- supply chain interruptions
- increased public frustration and behavioural change

Leadership Reality

Transport does not need to fail completely to disrupt operations.

Reduced reliability is sufficient.

What This Looks Like in Practice

Transport disruption typically manifests as:

- slower delivery times
- reduced service reliability
- increased operational cost
- growing dependency on prioritisation

Not:

- total system shutdown

But:

A gradual loss of efficiency followed by loss of effectiveness.

Board-Level Questions

1. Access & Movement

- What happens if we cannot move people or goods reliably?
- Which parts of our operation fail first under constrained movement?

2. Fuel Dependency

- How exposed are we to fuel cost and availability?
- What happens if fuel access is constrained, not just expensive?

3. Workforce Mobility

- Can our workforce physically get to work under current conditions?
- Which roles are most exposed to transport disruption?

4. Supply Chain Continuity

- Where are we dependent on just-in-time delivery?
- What buffers actually exist in practice?

5. Operational Flexibility

- Can we reduce movement without damaging outcomes?
- What activity can be localised or decentralised?

6. Third-Party Dependency

- Where do we rely on external logistics providers?
- What happens if those providers are constrained?

7. Customer Impact

- What will customers experience first under transport disruption?
- How will delays or availability changes affect trust?

8. Scenario Readiness

- Have we tested transport disruption scenarios?
- Do we know how long we can operate under reduced movement?

Common Failure Points

Transport risk is often underestimated due to:

- assuming availability equals access
- over-optimising for efficiency at the expense of resilience
- removing buffers from supply chains
- underestimating workforce dependency
- failing to identify critical routes and nodes

Final Insight

Transport disruption is not defined by whether movement stops.

It is defined by whether movement becomes unreliable.

Organisations rarely fail because transport disappears.

They fail because they can no longer depend on it.



5.4 Water — The System That Sustains Everything

Water is one of the most fundamental infrastructure systems. It underpins:

- public health
- sanitation
- industrial activity
- environmental stability

Unlike other sectors, water is often assumed to be stable.

In reality, it is highly dependent on:

- energy
- ageing infrastructure
- environmental conditions
- and operational continuity

In 2026, water risk is not defined by immediate scarcity alone.

It is defined by:

- system fragility
- energy dependency
- and the consequences of failure

Current Pressure Summary

RAG Status: Moderate to High Pressure

Water is less exposed to sudden disruption than energy or communications, but:

- consequences of failure are severe
- recovery is often slow
- dependency on energy is critical

Key Signals

- Increasing focus on infrastructure resilience and long-term investment requirements
- Ageing UK water infrastructure in many regions
- Growing environmental pressure (drought risk, flooding variability)
- Strong dependency on continuous energy supply for pumping and treatment
- High regulatory and public scrutiny

Interdependencies (Where Water Connects)

Water is both a dependent and enabling system:

- **Energy** → required for pumping, treatment, distribution
- **Transport** → required for maintenance, materials, and operational response
- **Communications** → monitoring, control systems, network management
- **Health** → sanitation, infection control, clinical operations
- **SaaS / Digital Operating Layer** → monitoring, billing, control platforms

Key Insight

Water is not an isolated system. It is a **continuous process** dependent on multiple other sectors.

Customer Spectacles

Customers rarely think about water until it fails. When it does, they experience:

- loss of supply
- water quality concerns
- service disruption
- immediate loss of trust

Unlike other sectors, tolerance for failure is extremely low.

Employee Impact

Water operations rely on field engineers, maintenance teams and also control system operators.

Key impacts include:

- reliance on transport for response and repair
- dependency on energy for operational continuity
- requirement for rapid response under pressure

Workforce effectiveness is critical to maintaining continuity.

Social & Workforce Stability

Water has a direct link to public health and wellbeing.

Disruption can lead to:

- immediate public concern
- rapid escalation of media and regulatory attention
- increased pressure on public services

Leadership Reality

Water issues escalate quickly from operational to public concern.

What This Looks Like in Practice

Water disruption typically manifests as:

- reduced pressure or supply interruptions
- water quality warnings
- localised outages

Not always widespread system failure, but:

- **high-impact local disruption**

Board-Level Questions

1. Energy Dependency

- How dependent are we on continuous energy supply for water-related operations?
- What happens to water services under power disruption?

2. Infrastructure Resilience

- How resilient is the underlying infrastructure?
- Where are the weakest points in the network?

3. Operational Continuity

- How quickly can we respond to failures or disruptions?
- Do we have sufficient redundancy in critical systems?

4. Monitoring & Control

- How dependent are we on communications and digital systems for monitoring?
- What happens if those systems degrade?

5. Customer Impact

- What would customers experience first under water disruption?
- How do we communicate effectively during outages or quality issues?

6. Workforce Readiness

- Can our teams respond effectively under constrained conditions?
- Are we dependent on specific skills or roles that could become unavailable?

7. Scenario Readiness

- Have we tested water disruption scenarios alongside energy and communications failure?
- Do we understand how quickly issues escalate?

Common Failure Points

Water risk is often underestimated due to:

- assumption of continuous availability
- underinvestment in infrastructure resilience
- lack of visibility into system dependencies
- reliance on stable operating conditions
- underestimating energy dependency

Final Insight

Water disruption is not defined by frequency.

It is defined by consequence.

Organisations do not experience water issues often.

But when they do, the impact is immediate, visible, and difficult to contain.



5.5 Health — Where System Failure Becomes Human Impact

The health sector is the point at which infrastructure risk becomes personal. It depends on:

- energy
- communications
- transport
- water
- digital systems

Unlike other sectors, health has:

- extremely low tolerance for disruption
- immediate consequences when systems degrade
- limited ability to defer demand

In 2026, health risk is not defined by isolated system failure. It is defined by **compound dependency risk**.

Current Pressure Summary

RAG Status: Moderate to High Pressure

Health is not typically the source of disruption. It is where disruption is:

- absorbed
- amplified
- and ultimately exposed

Its risk profile is driven by:

- dependency on other sectors
- operational complexity
- workforce pressure
- and demand variability

Key Signals

- Increasing demand pressure on healthcare systems
- Continued reliance on digital systems for patient care and administration
- High dependency on stable energy, water, and communications infrastructure
- Workforce constraints across clinical and operational roles
- Limited tolerance for service degradation

Interdependencies (Where Health Depends)

Health is one of the most dependent sectors:

- **Energy** → life-critical equipment, hospital operations, digital systems
- **Communications** → patient records, coordination, telecare, diagnostics
- **Transport** → staff, patients, emergency response, supply chains
- **Water** → sanitation, infection control, clinical operations
- **SaaS / Digital Operating Layer** → patient systems, scheduling, records, diagnostics

Key Insight

Health does not fail in isolation. It fails when other systems fail to support it.

Customer (Patient) Spectacles

Patients do not experience “infrastructure disruption”. They experience:

- delayed or cancelled appointments
- reduced access to care
- longer response times
- perceived decline in quality of service

In critical scenarios, this leads to increased clinical risk and direct impact on wellbeing .

Key Reality

Tolerance for disruption in healthcare is extremely low.

Employee Impact

Healthcare is heavily workforce-dependent. Key pressures include:

- staffing shortages
- shift intensity and fatigue
- reliance on physical presence
- limited flexibility for remote working in many roles

Disruption in supporting infrastructure leads to:

- increased workload
- reduced efficiency
- higher stress levels

Social & Workforce Stability

Health is closely linked to public confidence. Disruption can lead to:

- rapid escalation of concern
- increased demand on emergency services
- heightened political and media scrutiny

Leadership Reality

Health is where infrastructure failure becomes visible at a societal level.

What This Looks Like in Practice

Health disruption rarely appears as a single failure. It manifests as:

- increased waiting times
- reduced service availability
- operational strain
- prioritisation of critical cases

Over time, this leads to system backlog, declining performance and increased risk.

Board-Level Questions

1. Dependency Awareness

- Do we fully understand our dependency on energy, communications, transport, and water?
- Which of these would impact us most immediately?

2. Continuity of Care

- What happens to patient care under infrastructure disruption?
- Which services are most vulnerable?

3. Workforce Sustainability

- Can our workforce sustain operations under increased pressure?
- What are the risks of fatigue, absence, or attrition?

4. Digital Dependency

- How dependent are we on digital systems for patient care?
- What happens if these systems degrade?

5. Emergency Response

- How resilient is our emergency response capability?
- What happens if multiple systems degrade simultaneously?

6. Patient Impact

- What will patients experience first?
- How will this affect confidence and behaviour?

7. Scenario Readiness

- Have we tested compound disruption scenarios?
- Do we understand how quickly issues escalate?

Common Failure Points

Health risk is often underestimated due to:

- assuming stability of supporting infrastructure
- underestimating compound dependency risk
- reliance on workforce resilience rather than system resilience
- limited contingency planning for multi-system disruption

Final Insight

Health disruption is not defined by system failure. It is defined by patient impact. When infrastructure degrades, healthcare does not stop ; it becomes harder, slower, and more fragile.



5.6 SaaS / Digital Operating Layer — The System That Runs the Organisation

Modern organisations do not operate directly on infrastructure. They operate through a layer of software delivered over it.

This includes:

- ERP systems
- CRM platforms
- Office productivity suites
- email and marketing systems
- finance platforms (invoicing, payroll, collections)
- customer service tools
- integration and middleware layers

This layer has become the **primary operating environment** for most organisations.

In 2026, the risk profile of this layer has shifted. It is no longer defined by functionality or uptime alone.

It is defined by:

- dependency concentration
- external control
- access constraints
- and performance degradation

Current Pressure Summary

RAG Status: High Pressure

The SaaS / Digital Operating Layer is a critical cross-sector dependency due to:

- reliance on a small number of hyperscale providers
- limited fallback capability
- increasing exposure to jurisdictional and control risk
- integration across all core business functions

Key Signals

- Widespread organisational reliance on SaaS platforms for core operations
- High concentration of services across a small number of cloud providers
- Growing focus on digital sovereignty and control of infrastructure
- Increasing complexity of integrated software ecosystems
- Limited operational capability outside cloud-based systems

Interdependencies (Where SaaS Connects)

The SaaS layer sits across all sectors:

- **Energy** → monitoring, billing, control systems
- **Communications** → delivery layer for SaaS access
- **Transport** → logistics coordination and tracking
- **Water** → operational systems, monitoring, billing
- **Health** → patient systems, scheduling, diagnostics
- **Government / Finance** → transactions, records, compliance

Key Insight

SaaS is not a supporting system. It is the **operational interface through which organisations function.**

Customer Spectacles

Customers interact with organisations through this layer. Disruption is experienced as:

- inability to transact
- delayed responses
- inconsistent service
- loss of access

Unlike other sectors, SaaS disruption is often:

- immediate
- visible
- and difficult to isolate

Employee Impact

The workforce is heavily dependent on this layer. Disruption results in:

- inability to access systems
- breakdown in workflows
- reduced productivity
- increased manual workarounds

In many organisations, if SaaS fails, work stops.

Social & Workforce Stability

The SaaS layer underpins:

- communication
- coordination
- decision-making

When degraded:

- visibility reduces
- coordination becomes slower
- operational confidence declines

In combination with pressure in other sectors, this amplifies:

- disruption
- inefficiency
- organisational stress

What This Looks Like in Practice

SaaS disruption rarely appears as a complete outage. It manifests as:

- slower systems
- intermittent failures
- delayed processing
- unreliable integrations

This creates a difficult operating environment. Work continues but becomes inefficient and error-prone

Control & Sovereignty Dimension (Critical)

This is the defining characteristic of the SaaS layer. Organisations do not own the infrastructure on which they operate. They depend on:

- external providers
- external jurisdictions
- external priorities

Key Insight

Availability does not equal control. Even if systems are running, access may be:

- constrained
- reprioritised
- or altered under external conditions

Board-Level Questions

1. Dependency Awareness

- Which core business processes rely entirely on SaaS platforms?
- What would stop if these systems became unavailable or unreliable?

2. Provider Concentration

- How dependent are we on a small number of providers?
- Where are we exposed to single points of failure?

3. Control & Sovereignty

- Do we understand the jurisdictional exposure of our systems?
- Under what conditions could access be restricted or altered?
- Is our current dependency a conscious decision?

4. Operational Continuity

- Can we operate effectively if SaaS systems degrade rather than fail?
- Do we have any fallback capability outside these platforms?

5. Integration Risk

- How dependent are we on interconnected systems and APIs?
- What happens if one component fails or slows down?

6. Workforce Impact

- What happens to productivity if systems become unreliable?
- Can teams function without real-time system access?

7. Customer Impact

- What would customers experience first under SaaS disruption?
- How would this affect trust and retention?

8. Scenario Readiness

- Have we tested SaaS degradation scenarios?
- Who makes decisions when systems are partially functional but unreliable?

Common Failure Points

Organisations typically mismanage SaaS risk by:

- treating SaaS as “just software”
- assuming uptime guarantees equal resilience
- underestimating integration complexity
- failing to plan for degraded performance scenarios

Final Insight

- SaaS disruption is not defined by system failure. It is defined by loss of operational control.
- Organisations do not fail because software stops. They fail because they can no longer access it.

Most Common Leadership Blind Spots

Across sectors, a consistent set of leadership blind spots emerges:

- Assuming availability equals access
- Removing buffers in pursuit of efficiency
- Underestimating workforce exposure to infrastructure pressure
- Treating SaaS and digital platforms as control rather than dependency
- Failing to plan for degradation scenarios, focusing only on failure
- Deferring decisions until pressure forces them

These patterns are not sector-specific. They reflect how organisations typically behave under stable conditions, and why they struggle when those conditions change.

What Section 5 Means for Leadership

Across these systems, a consistent pattern emerges. None of them fail cleanly, and none of them operate independently. Pressure builds unevenly, moves across boundaries, and is often felt far from its point of origin. What appears to be a transport issue may originate in energy. What looks like a digital failure may be rooted in communications dependency. What presents as a healthcare challenge is often the visible end of multiple upstream constraints. This is the shift.

Infrastructure can no longer be understood, or managed, as a set of individual domains. It is a connected operating environment where resilience is determined not by the strength of any single system, but by how those systems interact under pressure. That has two immediate implications for leadership:

1. Visibility is inherently partial. No dashboard, report, or operational view will fully capture how pressure is building across the system. Decisions are therefore made with incomplete information.
2. Optimisation at a system level often requires compromise at a local level. Improving efficiency in one area may increase fragility in another. Reducing cost in one system may increase dependency elsewhere. The trade-offs are not always visible until they are tested.

This is why resilience is no longer a technical or operational concern. It is a leadership responsibility. The organisations that adapt will not be those with the most robust individual systems, but those that understand how pressure moves between them, and act accordingly.



Section 6 - How Pressure Moves — Interdependency in Practice

Understanding that systems are connected is only the starting point. The real challenge for leadership is not recognising interdependency in principle, but understanding how it behaves in practice. Pressure does not move evenly, and it does not always follow the most obvious path. It travels through points of weakness, across hidden dependencies, and often accelerates as it moves between systems. In many cases, the first visible issue is not the origin of the problem, but its consequence.

A disruption in energy supply may initially appear as a cost issue, before surfacing as a transport constraint, a service delay, or a capacity challenge elsewhere in the organisation. A communications outage may present as a system failure, but quickly becomes an operational and customer issue. A digital platform disruption may begin as a technical event, but rapidly affects decision-making, coordination, and delivery across multiple functions. This is the nature of modern infrastructure. Cause and effect are no longer linear. They are distributed.

For leadership teams, this creates a fundamental shift in how resilience must be understood. It is no longer sufficient to assess risk within individual domains. The focus must move to how disruption propagates across the system, and how quickly it can escalate beyond its point of origin. The question is not simply - *What could go wrong?* It is - *Where will it show up first, and where will it go next?*

6.1 Core System Relationships

The UK infrastructure system can be understood as a set of interconnected layers:

- **Energy** — powers all systems
- **Communications** — connects and coordinates systems
- **Transport** — enables physical movement and delivery
- **Water** — sustains health and operations
- **Health** — absorbs and reflects system failure
- **SaaS / Digital Operating Layer** — enables organisations to function

Each of these sectors is both dependent on others and a source of dependency.

Key Insight

Interdependency is not symmetrical. Some sectors act as:

- upstream dependencies (e.g. Energy)
- downstream impact points (e.g. Health)
- cross-cutting layers (e.g. SaaS)

6.2 Interdependency Matrix (High-Level)

The table illustrates the relative strength of dependency between infrastructure sectors.

PROVIDES DEPENDENCY ↓	DEPENDS ON →					
	ENERGY	COMMUNICATIONS	TRANSPORT	WATER	HEALTH	SAAS / DIGITAL
ENERGY	–	HIGH	HIGH	HIGH	HIGH	HIGH
COMMUNICATIONS	MEDIUM	–	HIGH	HIGH	HIGH	CRITICAL
TRANSPORT	MEDIUM	MEDIUM	–	MEDIUM	HIGH	LOW
WATER	LOW	LOW	LOW	–	HIGH	LOW
HEALTH	HIGH	HIGH	HIGH	HIGH	–	HIGH
SAAS / DIGITAL	MEDIUM	CRITICAL	MEDIUM	MEDIUM	HIGH	–

HIGH Critical to operation	MEDIUM Important but tolerable for a period	LOW Limited dependency	CRITICAL Essential for operation – loss has immediate system-wide impact	– Self
--------------------------------------	---	----------------------------------	--	-----------

KEY INSIGHT

The system is not a network of equal nodes. It is a stack of dependencies, where:

- ⚡ **ENERGY** enables
- 📶 **COMMUNICATIONS** coordinates
- 🚆 **TRANSPORT** delivers
- ☁️ **SAAS / DIGITAL** operates
- ❤️ **HEALTH** absorbs

ENERGY – Upstream Dependency

- Energy disruption propagates rapidly across the entire system.

COMMUNICATIONS – Coordination Layer

- Loss of communications reduces the ability to coordinate operations even where systems remain active.

TRANSPORT – Physical Enabler

- Transport disruption slows response, delivery, and recovery.

WATER – Sustaining System

- Water has fewer outward dependencies but very high consequence where it matters.

HEALTH – Impact Layer

- Health has low direct dependency on other sectors.
- Other sectors have high dependency on health.

SAAS / DIGITAL – Operating Layer

- SaaS does not power systems physically.
- It enables organisations to operate through them.

Key Insight

The system is not a network of equal nodes. It is a **stack of dependencies**, where:

- Energy enables
- Communications coordinates
- Transport delivers
- SaaS operates
- Health absorbs

6.3 Dependency Tolerance (Critical Concept)

Not all dependencies fail at the same speed. Each has a tolerance window:

- Immediate
- Hours
- One day
- Several days

Examples

- Communications without power → hours (depending on backup)
- Health without communications → immediate degradation
- Water without power → hours to days depending on system
- SaaS without communications → immediate operational impact

Key Insight

Understanding dependency is not enough. Leaders must understand **how long the system can tolerate disruption before failure occurs**

6.4 Scenario Chains — How Failure Travels

To understand interdependency, we apply real-world scenarios.

Scenario 1 — Power Rationing (Energy Constraint)

Trigger

Planned or unplanned electricity rationing across regions.

First-order impact

- Communications infrastructure switches to backup systems
- Water pumping and treatment capacity reduces
- Health facilities move to backup power
- Transport systems begin to degrade

Second-order impact

- Communications become unreliable or constrained
- SaaS access becomes inconsistent
- Remote working capability reduces
- Logistics coordination becomes more difficult
- Telecare and remote health monitoring degrade

Third-order impact

- Service delivery slows across sectors
- Workforce coordination becomes inefficient
- Customer experience deteriorates
- Health services experience increased pressure

Customer experience

- delayed services
- reduced availability
- failed transactions or communications

Employee impact

- inability to work effectively
- increased workload
- reduced coordination
- rising stress

Key Insight

Energy disruption does not stop systems immediately.

It removes the conditions required for them to operate effectively.

Scenario 2 — Communications Degradation

Trigger

Reduced connectivity or performance across networks.

First-order impact

- SaaS platforms become slower or unreliable
- Communication channels degrade
- Monitoring and control systems lose visibility

Second-order impact

- operational coordination breaks down
- remote working becomes ineffective
- customer service channels fail

Third-order impact

- service delivery slows or stops
- customer trust declines
- workforce productivity drops

Key Insight

Communications failure is often silent at first. Its impact becomes visible through operational inefficiency.

Scenario 3 — Fuel Distribution Constraint (Transport + Energy)

Trigger

Restricted fuel availability or distribution.

First-order impact

- transport capacity reduces
- field operations slow
- workforce mobility declines

Second-order impact

- supply chains become unreliable
- maintenance and response times increase
- service delivery becomes inconsistent

Third-order impact

- customer experience deteriorates
- operational backlog builds
- organisational performance declines

Key Insight

Transport disruption turns system pressure into visible operational failure.

6.5 What This Means for Leaders

Leaders do not need to understand every dependency. They need to understand:

- where their organisation sits within the system
- which dependencies matter most
- how quickly disruption will affect them
- and what decisions must be made under pressure

Final Insight

Infrastructure resilience is not about preventing failure. It is about understanding:

- how failure moves
- how quickly it escalates
- and how the organisation responds



Section 7 - Scenario Testing — Turning Insight into Action

Understanding how the system behaves is necessary, but it is not sufficient.

Leaders need to go one step further and test how their organisation would perform under realistic conditions of constraint.

This is where scenario testing becomes valuable.

It provides a structured way of moving from abstract understanding to practical decision-making, allowing leadership teams to explore how disruption might unfold and how effectively they could respond.

The purpose is not to predict specific events.

It is to expose:

- where the organisation is vulnerable
- how quickly pressure would be felt
- and whether decisions can be made with clarity under real conditions

7.1 How to Use Scenario Testing

Scenario testing should be used:

- in board and leadership discussions
- as part of operational planning
- to challenge assumptions about resilience

It is not a technical exercise. It is a **leadership exercise**.

Approach

For each scenario:

1. Define the trigger
2. Identify first-order impacts
3. Assess second-order consequences
4. Translate into customer and employee impact
5. Identify required decisions

Key Principle

The value is not in the scenario itself. It is in the **quality of the discussion it creates**.



7.2 Scenario 1 — Energy Constraint (Power Rationing)

Trigger - Planned or unplanned reduction in electricity availability across regions.

First-Order Impact

- Communications infrastructure moves to backup systems
- Water pumping and treatment capacity reduces
- Health services rely on backup power
- Transport systems begin to degrade

Second-Order Impact

- Connectivity becomes inconsistent
- SaaS systems become unreliable
- Remote working capability reduces
- Logistics coordination slows

Customer Impact

- delayed or inconsistent service
- reduced availability
- communication challenges

Employee Impact

- inability to work effectively
- increased workload
- reduced coordination

Leadership Questions

- What do we prioritise when energy is constrained?
- Which services must continue at all costs?
- What can be reduced or paused?
- How do we communicate with customers under constraint?

Decision Reality

Energy constraint forces **prioritisation decisions**. Not everything can be maintained.



7.3 Scenario 2 — Communications Degradation

Trigger - Reduced connectivity or performance across networks.

First-Order Impact

- SaaS systems become slower or unreliable
- communication channels degrade
- monitoring systems lose visibility

Second-Order Impact

- coordination breaks down
- customer service channels fail
- remote working becomes ineffective

Customer Impact

- inability to access services
- failed transactions
- delayed responses

Employee Impact

- reduced productivity
- confusion and duplication
- increased operational friction

Leadership Questions

- Can we operate effectively with degraded systems?
- What is our fallback mode of operation?
- Who makes decisions when information is incomplete?
- How do we maintain customer trust?

Decision Reality

Communications degradation creates **operational ambiguity**.

Leaders must act without full visibility.



7.4 Scenario 3 — Transport Constraint (Fuel / Movement Disruption)

Trigger - Reduced availability of fuel or disruption to transport networks.

First-Order Impact

- reduced workforce mobility
- slower logistics and delivery
- limited field operations

Second-Order Impact

- supply chains become unreliable
- service delivery becomes inconsistent
- response times increase

Customer Impact

- delays
- reduced availability
- increased cost

Employee Impact

- inability to travel
- increased fatigue and pressure
- reduced flexibility

Leadership Questions

- What activities can continue without movement?
- Which roles are most exposed to transport disruption?
- How do we prioritise limited capacity?
- What alternative arrangements can we implement quickly?

Decision Reality

Transport constraint forces **trade-offs between efficiency and continuity**.



7.5 Scenario 4 — SaaS / Digital Operating Layer Disruption

Trigger - Performance degradation or restricted access to core SaaS platforms.

First-Order Impact

- core business systems become unreliable
- workflows slow or fail
- integrations break down

Second-Order Impact

- operational coordination declines
- customer interactions degrade
- manual workarounds increase

Customer Impact

- failed transactions
- delayed responses
- inconsistent service

Employee Impact

- inability to complete tasks
- increased manual effort
- reduced confidence in systems

Leadership Questions

- Which processes stop if SaaS systems degrade?
- Do we have any fallback capability?
- How do we operate under reduced system performance?
- What is our tolerance for system unreliability?

Decision Reality

SaaS disruption challenges **operational control**.

7.6 What Scenario Testing Reveals

Across all scenarios, a consistent pattern emerges:

- organisations are stronger in awareness than readiness
 - dependencies are known but not fully mapped
 - decisions are not pre-agreed
 - trade-offs are not clearly defined
-

Key Insight

Most organisations do not fail because they lack understanding.

They fail because they have not converted understanding into decisions.

7.7 What Good Looks Like

Effective organisations:

- understand their critical dependencies
 - define minimum operating conditions
 - pre-agree prioritisation decisions
 - communicate clearly under pressure
-

Final Insight

Scenario testing is not about avoiding disruption.

It is about ensuring that when disruption occurs:

- decisions are clear
 - priorities are understood
 - and the organisation continues to function
-





Section 8 – The Infrastructure Resilience Test

A Board-Level Diagnostic

Most organisations believe they are prepared for disruption. They have risk registers, contingency plans, and documented scenarios that create a sense of coverage and control.

In practice, this often masks a different reality.

Understanding risk is not the same as being ready to respond to it, particularly when multiple systems are under pressure at the same time. In those conditions, organisations rarely fail because they lack awareness. They fail because they have not made the decisions that pressure forces upon them.

This test has been designed to expose that gap.

It does not measure how much you know.

It reveals how ready you are to act.

8.1 The Structure of the Test

The test is built around five areas:

- A. Dependency Clarity
- B. Control vs Exposure
- C. Customer Impact
- D. Commercial Reality
- E. Response Readiness

Each area contains two questions. Together, they provide a clear view of whether the organisation understands its position and, more importantly, whether it has translated that understanding into decisions.



8.2 The 10 Questions Every Leadership Team Should Answer

A. Dependency Clarity

Why this matters in 2026: Most organisations are exposed to dependencies they have never fully mapped, particularly across energy, communications, and digital platforms.

- What are the five infrastructure dependencies without which the business cannot operate?
- Where are the choke points within those dependencies, including providers, regions, routes, or platforms?

B. Control vs Exposure

Why this matters in 2026: Many of the systems that determine whether you can operate sit outside your control but inside your risk.

- Which of our critical dependencies do we directly control, and which are externally controlled?
- If access to one of these dependencies was restricted or reprioritised, how exposed are we in practice?

C. Customer Impact

Why this matters in 2026: Resilience is not experienced internally. It is experienced through broken promises.

- If a key dependency was constrained for 72 hours, what would our customers experience first?
- How quickly would our most important customers notice, and what would it do to their confidence and behaviour?

D. Commercial Reality

Why this matters in 2026: Resilience is now a commercial condition, not just an operational consideration.

- Would a major customer's procurement or risk function approve us as a strategic supplier today?
- Where could resilience concerns lead to exclusion before we are even considered?

E. Response Readiness

Why this matters in 2026: Under pressure, speed and clarity of decision-making matter more than the completeness of information.

- Do we have pre-agreed actions for major disruption scenarios, or would we be improvising?
- Who owns decision-making in a live disruption, and how quickly can those decisions be made and executed?



8.3 The Resilience Snapshot

This test is designed to produce a simple leadership view. Each category should be assessed as:

- Strong
- Partial
- Weak

The value is not in the label itself, but in the discussion required to agree it.

Indicative Interpretation

Dependency Clarity

- Strong: Dependencies are explicitly mapped and understood
- Partial: Key dependencies are known, but gaps remain
- Weak: Dependencies are assumed or incomplete

Control vs Exposure

- Strong: Clear ownership, alternatives identified, and tested
- Partial: Some control, but reliance on external providers remains high
- Weak: Critical dependencies sit fully outside control with no tested fallback

Customer Impact

- Strong: Customer impact is clearly defined and has been tested through scenarios
- Partial: Likely impact is understood but untested
- Weak: Customer impact is unclear or assumed

Commercial Reality

- Strong: Organisation would confidently pass a customer risk or procurement review
- Partial: Some exposure that could be challenged
- Weak: Material risk of exclusion or loss of confidence

Response Readiness

- Strong: Pre-agreed actions, clear ownership, rapid decision capability
- Partial: Some planning exists but gaps remain
- Weak: Response would rely on improvisation under pressure



8.4 Sector-Specific Prompts (Applied Layer)

The test becomes more powerful when applied through specific dependencies.

Energy

- What rights do we have to energy access under constrained conditions?
- Where would we sit in a prioritisation or rationing scenario?
- How would cost or availability constraints affect workforce and operations?

Communications

- Which operations fail if connectivity degrades rather than stops?
- Where are we dependent on specific providers, regions, or infrastructure?
- What is our degraded-mode operating capability?

Transport

- What happens if we cannot move people or goods reliably?
- Which roles or services fail first under constrained movement?
- What buffers actually exist within our supply chain?

SaaS / Digital Operating Layer

- Which core processes rely entirely on SaaS platforms?
- What happens if those systems degrade rather than fail?
- Do we have any meaningful fallback capability?

8.5 How to Use This in Practice

This test should be used in leadership discussions, not completed in isolation. It is most effective when:

- assumptions are challenged
- disagreements are surfaced
- and gaps are made explicit

The objective is not to produce perfect answers. It is to force clarity. If the discussion does not lead to decisions, the exercise has limited value.

Final Insight

Resilience is not built through documentation. It is built through decisions made before they are needed. The organisations that perform well under pressure are not those that understand risk best. They are those that have already decided what matters most, what they will protect and what they are prepared to let go.



Section 9 - The 30–60–90 Day Reset — Moving from Awareness to Action

For most organisations, the challenge is not recognising that infrastructure risk has increased. It is translating that awareness into a clear and practical starting point. Without that, the response tends to drift into either over-engineered transformation programmes or incremental adjustments that do not materially change resilience. This reset is designed to avoid both. The reset is built on three principles:

1. **Clarity before action**
2. **Decisions before investment**
3. **Alignment before optimisation**

9.1 First 30 Days — Clarity

Focus - Understand the organisation’s real dependencies and exposure.

Key Actions

- Run the Infrastructure Resilience Test with the leadership team
- Complete the Resilience Snapshot across all five areas
- Identify the top five infrastructure dependencies
- Map the key choke points within those dependencies
- Define what a 72-hour disruption would look like from a customer perspective
- Surface all assumptions that have not been tested

Leadership Behaviour

- challenge existing beliefs
- avoid premature solutions
- focus on visibility and honesty

Outcome

A clear, shared understanding of:

- where the organisation is exposed
- where assumptions exist
- and where resilience is weakest

Key Insight - At this stage, nothing is fixed. The goal is to **see clearly**.

9.2 Next 60 Days — Decisions

Focus

Confront trade-offs and define how the organisation will respond under pressure.

Key Actions

- Decide where redundancy is required versus where risk will be accepted
- Identify the two most critical disruption scenarios
- Define pre-agreed actions and triggers for each scenario
- Clarify ownership of decision-making in a live event
- Assess whether the organisation would pass a major customer risk review
- Identify gaps in operational capability

Leadership Behaviour

- confront uncomfortable trade-offs
- prioritise what matters most
- avoid deferring decisions

Outcome

- clear prioritisation of critical systems and services
- defined response actions for key scenarios
- agreed ownership and decision-making structure

Key Insight

Most organisations stall at this stage. Not because they lack options, but because they avoid decisions.

9.3 By 90 Days — Alignment

Focus

Embed resilience into how the organisation operates.

Key Actions

- Align the leadership team on key dependencies and exposure
- Integrate resilience considerations into operational and commercial decisions
- Define clear customer communication approaches for disruption scenarios
- Confirm workforce implications and required adjustments
- Re-run the Resilience Snapshot and assess progress
- Establish a cadence for ongoing review

Leadership Behaviour

- reinforce alignment
- ensure consistency of decision-making
- maintain focus on practical execution

Outcome

- shared understanding across leadership
- resilience embedded into decision-making
- visible progress from initial baseline

Key Insight

Resilience is not a document. It is reflected in how decisions are made.

9.4 What This Reset Does Not Do

This reset is not designed to:

- eliminate all risk
- create perfect resilience
- replace long-term transformation

It is designed to:

- move the organisation from passive awareness to active control

9.5 What Good Looks Like After 90 Days

Organisations that complete this reset will:

- understand their critical dependencies
- have made key prioritisation decisions
- be able to respond more quickly under pressure
- communicate more clearly with customers and employees

They will not be immune to disruption. But they will be:

more prepared, more aligned, and more decisive

Final Insight

Resilience is not built through activity. It is built through decisions.

The organisations that perform well under pressure are those that:

- know what matters most
- have already made the difficult choices
- and can act without hesitation





Section 10 - Final Leadership View — What This Means Now

Infrastructure has already changed. It is no longer a background utility that quietly supports the organisation. It has become a primary determinant of whether the organisation can operate at all. This shift is not coming. It is already underway. The real question is whether organisations recognise it in time to respond with intent rather than hindsight.

The Nature of the Shift

For many years, infrastructure was treated as stable, reliable, and largely invisible. Risk was considered something that could be isolated, managed, and, in most cases, contained within the organisation's own boundaries. That model no longer holds.

In 2026, infrastructure is interconnected in ways that are not always visible, dependencies are layered and increasingly complex, disruption does not follow predictable patterns, and control often sits outside the organisation rather than within it. The operating environment has shifted from one defined by efficiency and optimisation to one defined by access and continuity.

What Leaders Must Understand

This is not simply a technology issue, nor is it an operational one. It is a leadership issue. When infrastructure is constrained, not everything can be maintained. Trade-offs are unavoidable, and priorities must be made explicit. The organisations that perform well under pressure are not those that avoid disruption altogether, but those that understand their dependencies, make decisions in advance, and act with clarity when it matters.

The Emerging Pattern

Across sectors, a consistent pattern is becoming visible. Energy introduces constraint. Communications determines how effectively the organisation can coordinate. Transport governs access and movement. SaaS shapes control and operability. Health, ultimately, reveals the human consequences when the system comes under strain. These are not independent risks to be managed in isolation. They form a connected system in which pressure builds, moves, and compounds.

The Leadership Gap

Most organisations are not starting from zero. They understand their systems, their risks, and their dependencies to a reasonable degree. The gap lies elsewhere. It sits between understanding and decision-making. It is the space where known risks are not fully mapped, where dependencies are only partially understood, and where critical decisions have not been agreed in advance. This is the resilience gap. Organisations rarely fail because they lack awareness. They fail because they have not acted on what they already know.

What Will Differentiate Organisations

In this environment, advantage will not come from scale, efficiency, or optimisation alone. Those qualities still matter, but they are no longer sufficient.

What will differentiate organisations is their clarity of dependency, the speed and quality of their decision-making, and their ability to operate under constraint without losing control.

The organisations that succeed will be those that design for disruption rather than stability, prioritise access over cost when it matters, and align leadership around a small number of critical decisions.

A Different Way of Thinking

Resilience is often treated as a function, a plan, or a set of controls that can be documented and maintained.

In practice, it is something quite different. It is a way of thinking about the organisation, a way of making decisions under pressure, and a way of operating when conditions are no longer ideal.

Resilience is not something the organisation has. It is something the organisation does.

What This Document Enables

This document is not intended to provide a complete set of answers. It is designed to challenge assumptions, expose gaps, and prompt decisions that might otherwise be deferred.

It provides a structured view of system pressure, a clearer understanding of interdependencies, a set of realistic scenarios, and a practical diagnostic to test readiness.

What it does not do is remove the need for leadership judgement.

The Decision Facing Leaders

Every organisation now faces a set of simple but unavoidable questions.

What do we depend on most, and how well do we truly understand those dependencies?

What do we control, and where are we exposed to decisions made elsewhere?

What happens when those dependencies are constrained, not in theory but in practice?

What are we prepared to protect at all costs, and what are we prepared to let go?

These are not theoretical considerations. They are operational decisions that will determine how the organisation performs under pressure.

Final Statement

Resilience in 2026 is not defined by whether systems exist. It is defined by whether organisations can retain access to them when conditions tighten and priorities compete.

Closing Thought

Geopolitics is a board-level concern. A broken service is a customer experience.

If an organisation cannot bridge the gap between the two, it does not have a strategy. It has a hope. And in this environment, hope is not a hedge.