pwc

NATIONAL PREPAREDNESS COMMISSION

Connecting for continuity in a crisis

Joining forces to strengthen UK resilience

Foreword

In a turbulent and increasingly interconnected world, where geopolitical instability is increasing and longer-term threats such as climate change are amplifying these dangers, crises are no longer isolated events. They interact, overlap and cascade.

It is no longer enough for individual businesses to focus solely on their own preparedness and resilience. Nor does it work for the government to approach these risks in isolation.

That is why the National Preparedness Commission asked PwC to prepare this report. It provides a clear message to organisations on how they should approach risks and what is needed to deliver a 'minimum viable company'. And it is grounded in the real-world experience of the corporate leaders who fed into the work. It also has important implications for government who need to provide the guiding principles and incentives to enable organisations to respond.

Indeed, government must harness its convening power to agree collective objectives. The first step is to be clear on current levels of preparedness against the threats in the National Risk Register and the nation's resilience against the systemic challenges set out in the Chronic Risks Analysis. Only with such a baseline assessment will it be possible to set out minimum resilience expectations and the preparedness needed in various scenarios to deliver a 'minimum viable UK'.

To support this, government must improve the flow of information – timely data to enable organisations to respond to a rapidly changing environment and for businesses to inform government of their experience of the threats they face and what is needed to combat them. This two-way exchange is vital for building real-time situational awareness and enabling a genuinely whole-of-society approach. Both government and private enterprises must 'dare to share' without compromising our nation's security.

Of course, most organisations have a sense of national duty, but the tension between this and the pressure of commercial realities needs to be recognised by government. However, everyone gains with greater visibility of the likely impact of threats and how best to build resilience against them.

But government needs to frame its expectations in commercial terms, showing why the necessary resilience and preparedness posture is consistent with and contributes to the needs of the businesses concerned. Sometimes regulation may be needed, or financial incentives will be required, but the first recourse should be to build on the work that is already underway and remove any barriers that make resilience and preparedness more difficult.

Government itself must move beyond departmental silos. A coordinated whole-of-government approach is required with strong central leadership to manage the interdependencies and trade-offs between sectors.

Systemic risks need a systemic approach. In a turbulent world, this must be the central mission of government and society. And it needs to be pursued at pace.

- Lord Toby Harris, Chair, National Preparedness Commission

Contents

Introduction 5

Rising to the resilience challenge 7

Shaping a unified system approach 12

Setting our sights on a minimum viable UK 15

Putting public-private collaboration at the heart of national resilience 19

Stakeholder reflections on the whole-system approach 21

Building strong foundations for success 26

Case study: Lessons from financial services 36

Appendices 41

Introduction

The UK's critical national infrastructure (CNI) must materially shift its preparedness for the challenges ahead. While the institutions that make up the UK's CNI have sustained the nation's critical functions through extreme difficulties in the past – COVID-19 being the obvious example – we need new capabilities to face future threats head-on.

More extreme concurrent crises are now a distinct possibility at a time when CNI is arguably less resilient than ever. In an age of proliferating risks – from hostile states to tech failures, climate change to civil unrest – taking action is a matter of urgency.

UK prosperity rests on our infrastructure being prepared. We have willing and capable leaders across government, regulatory bodies, and CNI who are ready to step up. But CNI resilience is built around individual organisations, rather than the ability to deliver system-wide outcomes under extreme strain. Thus, the UK is structurally underprepared.

Addressing this has been much discussed, and legislation is progressing through policies such as the Cyber Security and Resilience (Network and Information Systems) Bill. But far more must be done. To implement resilience at pace, the National Preparedness Commission asked PwC to identify practical steps to build the minimum level of resilience to keep the UK running and the lights on in a crisis.

A systemic challenge requires a systemic solution – one that acknowledges the interdependencies between CNI's component parts and its dependencies.

The only way to achieve this is to build a whole system resilience model that protects society's critical national functions from intolerable harm during a crisis. And we must build this fast.

What we set out to achieve

We wanted to understand the structural barriers to CNI resilience and what must change to overcome them, so that resilience is addressed as a true system-of-systems challenge. While many businesses are embedding resilience within their organisations, a centrally coordinated mechanism is essential to scale these efforts across interconnected CNI. Without this, whole-system resilience is likely to fall short.

We tested this thinking in research interviews with CNI leaders from private enterprise, the public sector, government departments, and industry bodies. From the findings, we shaped recommendations aimed at building a truly systemic approach to safeguarding the critical national functions that underpin the fundamentals of our society. One that reflects the deeply interdependent nature of the CNI.

These recommendations do not represent the full solution to the UK's resilience challenges. We recognise that future legislation and additional investment may be required. But without a strong foundational systems approach, future efforts risk being ineffective.

By design, we are not seeking to prescribe where significant investment should be directed, particularly in light of the current fiscal environment and resource constraints. Instead, we aim to make a cost-effective contribution to strengthening resilience by improving understanding of each organisation's role within the wider ecosystem. Our focus is at the strategic level rather than on day-to-day operations. Likewise, we do not intend to judge the specific infrastructure needed to make the UK fully resilient, or any shortcomings that may exist. Rather, our aim is to strengthen resilience – through better mutual understanding of interdependencies, recovery standards, and requirements – across the entirety of the existing CNI ecosystem.

What's our definition of resilience?
PwC defines resilience as the ability to absorb shocks, continue operating, recover and adapt during and after disruption. Our recommendations aim to engender this across CNI.

Rising to the resilience challenge

1

Where are we now and what needs to be done?

The reactive methods of the past are now inadequate. The March 2025 Heathrow substation fire saw over 1,300 flights cancelled.[1] Future incidents could be far worse. Severing undersea cables could wipe out the system's excess energy supply margin.[2] Multiple simultaneous pressures on CNI could be devastating.

While some parts of UK CNI are building more resilience, this doesn't apply across the board. Some stakeholders even expressed difficulty being recognised as CNI. Despite government attention, there's no centralised CNI resilience leadership or urgency to drive this across the entire CNI ecosystem. Let's explore the reasons why and what to do about it.

The UK's 13 government recognised CNI sectors

- Chemicals
- Civil nuclear
- Communications
- Defence
- Emergency services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

1. According to reporting by Reuters – 21 March 2025
2. Undersea cables transfer approximately 10% of the UK's peak power demand. NESO aims to hold a 10% margin.

How CNI resilience is managed

Systemic resilience oversight of the CNI mirrors the way the government manages crises.

The COBR Directorate
The central Cabinet Office Briefing Rooms (COBR) function is responsible for systemic resilience and the acute response to a systemic risk.

Lead Government Departments (LGDs)
LGDs have day-to-day oversight of their respective CNI areas (i.e. the Department for Transport oversees railways, etc.). They own planning, preparedness, response coordination, and resilience policy development.

Local Resilience Forums
These bring together Category 1 frontline responders like the police, fire, local authorities, and NHS bodies, along with Category 2 operators, including utilities and transport, to improve cooperation, information sharing, and joint local crisis planning.

Strategic Coordination Groups
These are established when local multi-agency coordination is required in a crisis.

Many government initiatives sit behind these functions. They range from cross-government frameworks like the **UK Government Resilience Action Plan**, to strategic risk-specific plans like the **Government Cyber Security Strategy**, government department plans, multi-agency plans, and local resilience plans. LGDs – for example, the Department for Transport and Department for Energy Security and Net Zero – are preparing to deliver strategies that flesh out sector resilience. See Appendix B for a summary of key current initiatives.

Our engagement with stakeholders, including LGD planning leads, points to major gaps, disparate resilience planning, limited visibility into others' preparedness, siloed thinking, and reactive coordination that coalesces only once a crisis emerges.

As a result, there's been little urgency to drive preparedness across the CNI ecosystem, leaving system-wide requirements unaddressed.

Stakeholders raised examples of what this means in practice.

- Interdependency mapping between component parts of CNI exists in the Cabinet Office *CNI Knowledge Base* but can't be accessed by many CNI operators. This mapping is key to identifying vulnerabilities.
- LGDs exchange limited resilience-building communication between each other, which is compounded by wider cross-departmental data-sharing challenges.
- Information sharing between the public and private sectors is problematic in both directions.
- Recovery timelines vary by sector and organisation, but interdependent parts of CNI don't have visibility of this.
- Resilience mandates vary by sector. For example, financial services is heavily regulated while food distribution has little to no direction.

Without a robust system-thinking approach, preparations will remain disjointed, uncoordinated, and even counterproductive. How CNI's component parts will respond to disruption remains unclear. The EU is already implementing the Critical Entities Resilience Directive. In our view, the UK government should be on a similar track.

Building on existing thinking to identify what's most urgent.

Our stakeholder engagement focused on identifying practical steps to keep the UK running in a crisis.

What needs to be done	What's required to make it happen
Adopt a whole-of-society approach	Combining government leadership with private sector and local execution, reflecting the UK's shared-responsibility model for CNI.
Move from silos to systems	Better information exchange, flexible decision-making, and the use of specialist expertise to manage complex interdependencies.
Prepare now for emerging long-term threats	Preparing for a wide range of plausible future scenarios, not only the most familiar or likely risks.
Strengthen resilience culture	Clarifying government's coordination role and empowering operators to make informed local decisions.
Realise value through resilience	Recognising that resilient organisations benefit from protecting their value during a crisis.
Deliver on government's duty of care	Designing and delivering infrastructure that offers equality of protection to vulnerable groups and underserved regions.

See Appendix C for an expanded version of this.

Shaping a unified system approach

2

Enabling resilience through collaboration

There was universal agreement among stakeholders on the need for a unified system approach. However, with government having devolved CNI resilience to LGDs, making this work will require widespread collaboration. This will take a whole-system or system-of-systems approach.

By pooling technical expertise, innovation capacity, resources, and operational readiness from private operators with strategic government oversight, a unified system can overcome fragmentation. As the central convener, government can delegate and share accountability, authority, and responsibility while CNI operators and societal stakeholders gather round to collaborate.

Five key aims of a systemic resilience approach

01

Support whole-of-society resilience

Bridging private-sector and government perspectives to foster joint planning and a collaborative response.

02

Prevent cascading failures

Improving understanding of the interdependencies within and between systems to prevent single points of failure from escalating.

03

Enable targeted resilience

Helping CNI ecosystem organisations prioritise limited resources in emergencies by distinguishing what's essential versus optional.

04

Accelerate recovery

Helping to identify which capabilities must be maintained or restored first to enable a faster, more coordinated recovery.

05

Achieve complete dependency mapping with cross-sector visibility

Mapping the interdependencies and common foundational infrastructure and services that all parts of CNI rely on, acknowledging the need for necessary controls at an appropriate level.

Setting our sights on a minimum viable UK

Embedding system thinking across CNI

To make whole-system thinking a reality, we must shift our view to see CNI not as a series of discrete, independent organisations, but as a single, interdependent system.

We propose achieving this with a twin-track approach.

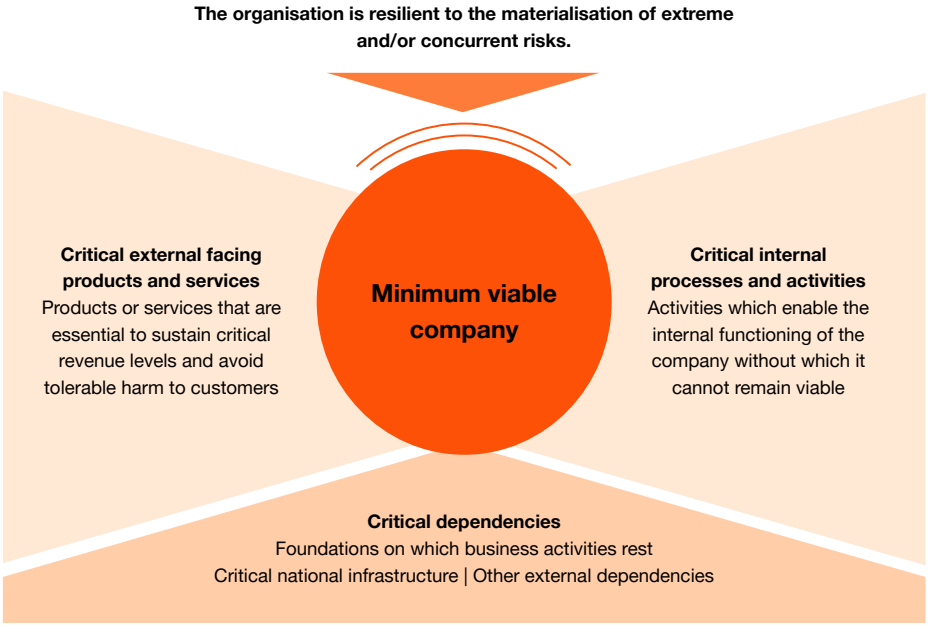
1. Embracing a minimum viable company model for individual CNI organisations.
2. Scaling this to a whole-system model for the entire CNI to build a minimum viable UK.

Borrowing from the start-up world, minimum viability is a concept to specify precisely what's needed to drive resilience. Without it, crisis decision-making will remain improvised and fragmented, prolonging recovery and negative long-term impacts.

Success will depend on nurturing a system-thinking culture across CNI. Organisations should not define their minimum viable company without an understanding of their role within the whole system and the dependency other CNI operators have on them.

Introducing the minimum viable company

As our starting block, the minimum viable company (MVC) combines the critical services, processes, and functions that must remain operational to stay financially, operationally, and strategically viable during a crisis, giving sufficient time to recover. It's intended only to keep the business running through the acute crisis phase and may include temporary scaling down of non-essential processes. By identifying the essentials, you can prioritise investments, streamline recovery plans, and sustain trust among customers, regulators, and stakeholders. And it's scalable for small businesses and multinationals alike.

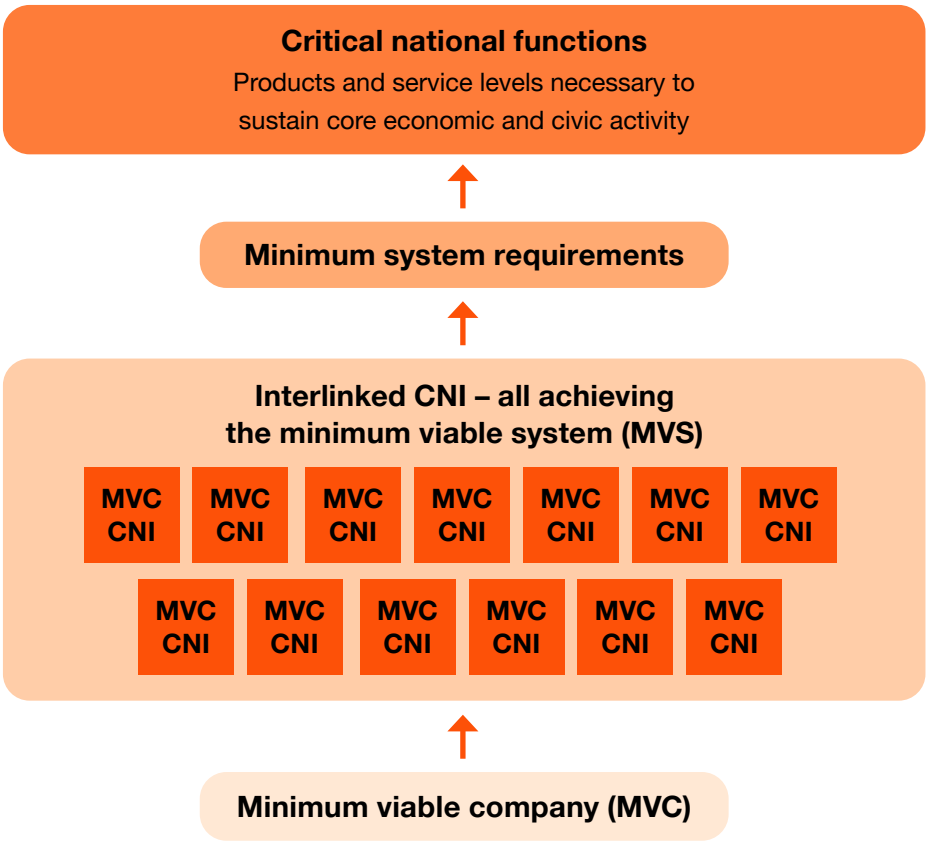


The minimum viable company brings together the top-down operational resilience view of the organisation (critical business services) with the bottom-up systems and technology services view. It encompasses all required operating licenses, health, safety, and reputation considerations, plus critical supporting functions for safe and legal operation.

Scaling the minimum viable company to the minimum viable UK

The same minimum viable principle can be scaled for CNI nationally. A minimum viable UK allows operators within the system to identify the critical enablers of economic and civic activity and smallest group of essential assets and dependencies to keep critical national functions running. It enables government, industries, and communities to coordinate cross-sector resilience, when multiple systems are under stress.

What is the minimum viable UK?
The set of critical national functions that must be sustained during a crisis to support the fundamentals of society for sufficient time to begin recovery.



The minimum viable UK model provides a practical, scalable way to define the CNI's minimum system requirements and align essential public and private action. Its four layers are essential to sustaining essential national activity.

Putting public-private collaboration at the heart of national resilience

Aligning on direction, standards, and incentives

Our engagements revealed broad support for the minimum viable UK concept as an effective framework for whole-system resilience. But they were also clear that success depends on the following:

- A single shared system picture – currently mapping is fragmented, terminology is inconsistent, government direction isn't always aligned, and there's no universal definition of criticality.
- A single set of mutually reinforcing incentives.
- Agreed cross-CNI minimum resilience standards.

CNI operators want these to be driven by a single centralised authority, but without terms being dictated to them. In other words, a collaborative private-public sector approach. The minimum viable UK model is designed to bridge these gaps with the government at the centre of – rather than adjacent to – the CNI's resilience system.

It's an approach designed to spread responsibility, prevent overburdening the centre, and minimise gaps. So, while government develops the umbrella and environment for the system to develop organically, the private sector must unite beneath it and actively participate to make it work.

Stakeholder reflections on the whole-system approach

Breaking down barriers to implementation

Establishing an effective minimum viable UK system requires an urgent focus on defining:

01

Agreed minimum essential service levels – what must never fail?

02

Criticality thresholds – what constitutes intolerable harm?

03

Time-bound tolerances – how long can the system absorb the disruption?

04

Sovereign capacity thresholds – what must be held nationally?

There was clear consensus among stakeholders on the need to break down barriers relating to the following core themes.

System-wide framing is accepted but siloed thinking remains widespread

Treating UK CNI as one interconnected system is overdue. Government mapping is incomplete, shared inconsistently, and not embedded in assurance. Government must consistently 'speak with one voice'. And governance is fragmented across departments with variable sector engagement.

"Criticalities, without doubt need a map."

There's no universally accepted definition of 'critical' in CNI

With so much variation between sectors, agreeing what is meant by 'critical' is essential to set priorities and determine minimum tolerance capacity. Criticality may need clear sovereign capacity thresholds, sector-specific tolerances, and cascading harm alignment across dependencies.

"Criteria to determine critical is the hardest part."

Information is not easily shared throughout the system

An entirely new approach to cross-CNI information exchange is essential. Legal constraints, security, commercial sensitivities, lack of channels, and regulatory structures disincentivise sharing during crises – when visibility matters most. Solutions include mandated crisis-time sharing, greater visibility of government continuity planning, and business incentives.

"Information sharing is still the biggest challenge."

There are no government-defined minimum resilience outcomes

Systemic resilience needs more than voluntary approaches. Government must articulate a minimum expectation and resilience target to help make it a priority. But this needs to be balanced and not overly prescriptive. Some public sector respondents want stronger regulation. And some want credible timescales to add legitimacy.

"We need regulations to drive it forward."

There's no capability to convene cross-sector resilience planning with senior representation present

Cross-sector public-private forums have been effective for coordinating multi-party situations in other fields – but senior representation is vital. They work well when responsibilities are clearly defined, government articulates what it will provide, expectations are explicit, and government acts collaboratively rather than directing from above.

"[Cross-sector forums] work really well and there is an appetite [in government] to replicate them."

Resilience isn't being framed in commercial terms

Boards don't generally respond to abstract resilience theories or sense of national duty. They're more motivated by a tangible financial, strategic, and reputational impact. Without aligning systemic resilience to fiduciary duty and remuneration incentives, resilience will lose out to short-term commercial pressures. The resilience drive must be framed in this reality.

"What if the thing that makes you money turns off?"

A cross-sector agreement on maximum allowable time to recovery against an array of scenarios doesn't exist

The model must include time thresholds, address compound risks, and be sufficiently robust for any scenario – even if it reveals uncomfortable truths. The UK must also prepare for large concurrent crises by driving relevant scenario development.

"We need to focus on severe but plausible scenarios, not just the most likely."

Stakeholder recommendations to reinforce the whole-system model.

Coordination and leadership

Stakeholders want stronger centre-led CNI coordination, with clear accountability, more robust cross-system governance, and leadership that can resolve cross-departmental trade-offs. They also want a defined hierarchy of resilience objectives. Without these, government departments could continue to pursue competing objectives without aligning to a unified mission.

"More of a cabinet office-led approach would be helpful."

Funding and incentives

Building resilience is costly, there are big incentive gaps, and structural factors deterring investment. There's huge variation between sectors and no mechanism to cooperate in a crisis. Suggestions include defining resilience investment for special tax treatment, sovereign capability subsidies, using regulatory CNI designation for critical third parties, and aligning remuneration and fiduciary duty with resilience.

"We can't rely on the market incentives."

Assurance and exercising

Firms need to know when legal or regulatory requirements can be paused to preserve critical functions. Without this flexibility, they may be conflicted. There was also strong support for a national personal resilience campaign to reduce pressure on CNI in a crisis. Minimum viability will require an exercising regime, maturity assessment tools, and transparent progress indicators to improve cross-sector visibility.

"Plans aren't capability. Capability is what you can demonstrate through exercising."

Timelines

Building the minimum viable UK will take staged implementation. A process that must accommodate for legislative adaptation, constraints on engineering, skills availability, and emerging technologies. Immediate agreement on baseline definitions should be followed by medium-term strengthening, with a long-term target for full system resilience between five and 25 years.

Building strong foundations for success

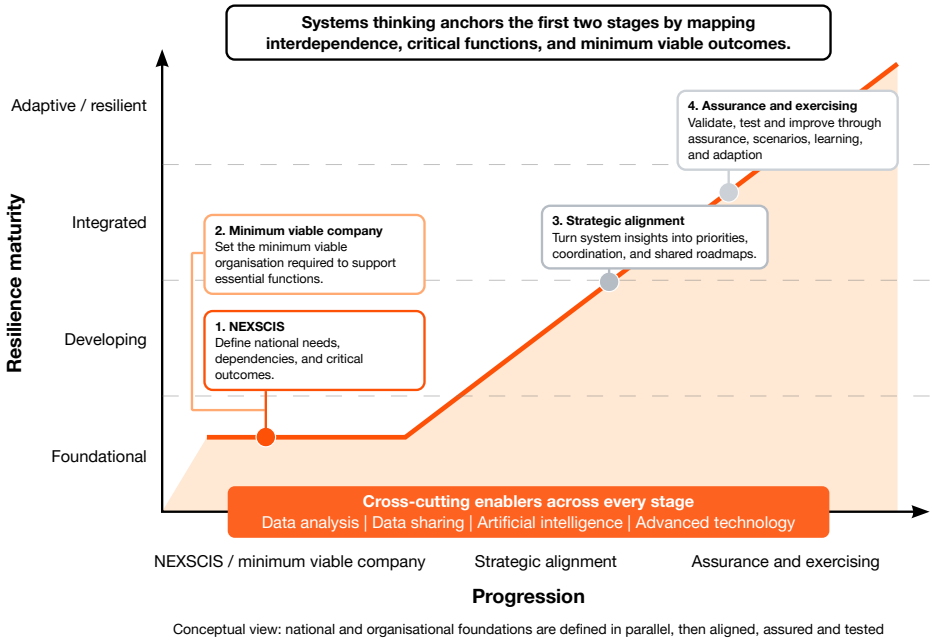
6

Practical steps towards systemic resilience

Building whole-system resilience will take a twin-track approach. First, we'll show how a national cross-sector group can form the foundation for a mature system-of-systems.

Second, we'll set out the practical steps organisations need to take now to establish their own resilience foundations as part of the wider system. Building systemic national resilience and organisational resilience must happen concurrently to establish a minimum viable UK.

A structured path to resilience maturity



Conceptual view: national and organisational foundations are defined in parallel, then aligned, assured and tested

Building the National Exchange for Sustaining Critical Infrastructure Services (NEXSCIS)

Central to our recommendations is establishing the National Exchange for Sustaining Critical Infrastructure Services (NEXSCIS). Inspired by a model from the UK financial services sector, it would expand on similar principles to build a robust capability for CNI.

As a cost-effective, cross-sector forum, NEXSCIS would strengthen resilience while maximising benefits. It's premised on government setting a clear north star for CNI operators to follow. By taking the lead, government can be the focal point, set parameters, and drive cross-sector resilience by convening top-level attendance. NEXSCIS is used here illustratively. Any organisation can be created or mandated to fulfil the same functions; the important thing is that a central coordinating body is needed.

"UK businesses recognise the need to strengthen resilience, especially across critical national infrastructure. This report makes a compelling case for moving beyond fragmented approaches towards a coordinated, system-wide model. Stronger collaboration between government and industry, combined with embedding resilience at every level, will be key to protecting essential services and sustaining long-term economic stability and competitiveness."

- John Foster, Chief Policy and Campaigns Officer, CBI

Building the National Exchange for Sustaining Critical Infrastructure Services (NEXSCIS)

Key NEXSCIS responsibilities	Headed by a government or quasi-non-government entity distinct from the Cabinet Office, NEXSCIS can draw on UN definitions of resilience for infrastructure. Its main role can be to: • Convey levels of intolerable harm to critical national functions. • Define CNI's minimum essential service levels. • Drive maximum system recovery timelines. • Define accountability distribution between government and CNI operators. • Own responsibility for national resilience outcomes. • Chair sub-groups for focused exploration of specific resilience issues. • Explore the use of technology, including AI, to build systemic resilience.
Internally agree a crisis threshold to pause competition	• To encourage cooperation between market competitors.
Leverage trade bodies for systemic risk insights	• Utilise established relationships between trade bodies and government. • Private firms, regulators, and government departments often view trade bodies as trusted conveners. • They reduce the risk of individual organisations raising questions that may imply non-compliance or inadequate risk mitigation. • They can be a single point to help government agencies disseminate information regularly.
NEXSCIS could learn from similar models in Europe	• In the Netherlands The Leading Group convenes senior CNI representatives to explore the systemic impacts of different scenarios. • Finland's Security Committee is rooted in a whole-of-society approach. It convenes representatives from government ministries, authorities, and the private sector – including organisations that operate CNI – to coordinate preparedness, share information, and explore crisis scenarios as part of a comprehensive security model.

A more detailed list of NEXSCIS responsibilities can be found in Appendix A.

Immediate steps to get your organisation resilience ready

Stakeholders painted a picture of varying levels of resilience maturity across different organisations and different sectors. This must change fast.

Start by implementing these low or no-cost measures within your organisation and your critical dependencies. And be mindful that developing resilience through a systems lens will mean bilaterally engaging across different sectors to gain a true understanding of your dependencies and test planning assumptions.

"In an age of constant polycrisis, adaptability is essential. Resilience needs whole-of-society collaboration, systems thinking, and strong communities. We must exercise together across sectors to break silos before crises hit. Learning from international partners and public–private collaboration can strengthen our shared resilience without waiting for perfect conditions."

- Rosehanna Chowdhury, CEO, UK Resilience Academy

Immediate steps to get your organisation resilience ready

Define your minimum viable company with minimum viable UK principles	• Define what matters most to your organisation. If everything is critical, then nothing is critical. • Identify which critical dependencies and parts of CNI your organisation relies on. • Assess which other parts of CNI rely on your functions.	• Identify critical systems. • Calculate the minimum revenue to meet existing financial obligations. • Determine the minimum time to recover from a crisis.
Diversify non-executive directors	• Bring in non-executive directors with experience of resilience failures to guide planning and challenge risk assumptions.	
Designate a competent board-level person with accountability for resilience	• This individual should be your consistent NEXSCIS representative.	
Leverage new technologies and data	• Enable end-to-end visibility to map and manage business services, assets, and dependencies in one unified system of record. • Automate testing and scenario planning to simulate disruptions and stress-test operations against impact tolerances. • Integrate data models to connect risk, continuity, IT operations, and third-party data for unified decision-making.	• Embed real-time monitoring for proactive issue detection and rapid response. • Enable intelligent workflows to automate selective response, communication, escalation procedures, and business-as-usual activities such as refreshing BIAs. • Adopt analytics and reporting to deliver real-time resilience dashboards for executives and boards.

Strategic alignment

Treat resilience as a core strategic capability to assess the risk of operational failures to your business. For CNI organisations, resilience is the lynchpin that underpins public trust, national stability, and long-term commercial success. Safeguarding it could not be more important.

Strategic alignment

Identify how a resilience failure will impact your business in terms of:	• Reputation • Market positioning • Resource allocation • Strategic vision
Incentivise long-term resilience throughout your organisation	Embed resilience into reward structures – including repurposing existing incentives. Shift focus from short-term gains to sustained performance to reinforce long-term value and competitiveness. • **Board and C-suite:** Include resilience KPIs (reliability, availability, security) on executive scorecards and link annual and long-term incentives to performance against them. • **Middle and upper management:** Use bonus pools and performance reviews to reward proactive risk reduction – e.g. in testing, automation, backlog reduction – not just low incident counts. • **Frontline teams:** Use small, frequent rewards and recognition for improvements. Run simple suggestion schemes with rapid feedback and monthly impact reporting on downtime, recovery time, etc., while screening for quality to avoid low-value volume. • **Measurement and enablers:** Standardise transparent reporting of reliability KPIs by business area. Embed resilience expectations into hiring, onboarding, and performance management.

Assurance and exercising

Assurance and exercising

Conduct scenario testing and maturity scoring	• Rigorously test plans to build an evidence-based view of maturity, exercising across complex, cross-sector scenarios to expose interdependencies, challenge assumptions, and identify vulnerabilities.	• Capture insights to feed into continuous improvement and wider UK resilience planning, strengthening a coherent minimum viable UK system.
Pursue a mature understanding of acceptable resilience	• Reframe government resilience standards as the minimum rather than optimal level, as they were conceived before today's heightened threat landscape.	• With mature resilience practices and flexibility to move fast, you can work towards better outcomes aligned to what good looks like.
Stress test cross-CNI communications	• Give extra attention to stress-testing cross-CNI crisis communications.	• Exercise the impacts of failed communications networks to identify robust contingencies.
Engage with the UK's National Resilience Academy (UKRA)	• The UKRA is set to expand its reach, mirroring the Finnish model where resilience education is provided to the broader economy.	• This reflects Cabinet Office recognition that firms need more information on resilience.

Case study: Lessons from financial services

7

Lessons to guide CNI implementation

NEXSCIS will need to be properly implemented and its mandates enforced. It can adopt the foundations and principles from the model used by the UK financial services industry. Co-chaired by the Bank of England and UK Finance, the Cross Market Operational Resilience Group (CMORG) coordinates collaboration in areas like cyber threat, incident, and continuity planning to protect the financial system and consumers. Understanding what has worked well can inform the CNI sector as it establishes its own version.

Existing regulatory frameworks for identifying critical service delivery and maximum tolerable harm could be adapted for CNI. Under the guidelines, firms must identify important business services (IBS) and set impact tolerances (IToLs). These must be clear, measurable, and approved by the board. Firms must map supporting resources, conduct scenario testing, remediate vulnerabilities, and stay within their impact tolerances. Striking the right balance is key to business viability while strengthening system resilience.

Equally, we can learn from what has not worked so well. For example, accountability for systemic resilience remains somewhat unclear, largely unenforced, and there's a tension in how it is incentivised. These are all lessons that can guide the way forward for CNI.

Core transferable tenets that could be adopted by CNI	• Identifying risks and developing solutions to improve whole sector resilience. • Sub-groups for knowledge-sharing initiatives, e.g. publishing practical guidance.	• Practical focus on improving system-level resilience and sector exercising. • Simulation exercises to test collective response to severe disruption scenarios.
Building on the senior management and certification concept	• Clarifying senior manager function (SMF24[3]) accountability and responsibilities.	• Whole-organisation approach with a senior manager driving the process.
Information sharing and trust models	• Adapt the Financial Sector Cyber Collaboration Centre trust-tiered sharing model to manage sensitive information. • Enable access without vetting, instead relying on trust to determine information access.	• Disseminate cross-sector information from industry to government departments and regulators.

3. The Chief Operations Function (usually a Chief Operating Officer), which holds direct, personal accountability to the board for the resilience and functioning of internal operations.

Conclusion

No organisation wants to be the weakest link in a crisis, especially when it comes to keeping the critical national functions that underpin our society running. As reflected in the views of the stakeholders we spoke to, accelerating the minimum viable UK approach will be a pragmatic way to strengthen national resilience at speed and scale.

From a big picture perspective, we're at the early stages of our whole-system journey. While the goal is not perfection, we urgently need to seize this moment and prepare for a fast-changing threat landscape. By joining forces to build a more connected CNI, the UK will be better able to withstand shocks and recover fast. That's how we can collectively safeguard what matters most to protect our people and our society. And enable continuity in a crisis – whatever lies ahead.

Are you ready to connect for continuity?

Contact

Bobbie Ramsden-Knowles
Partner, Crisis & Resilience, PwC UK

Rachel Taylor
Partner, Head of Government and Health Industries, PwC UK

Chris Scudamore
Partner, UK Leader for Central Government, Capital Projects & Infrastructure, PwC UK

Sean Withington
Senior Manager, Geopolitical Risk, PwC UK

Acknowledgements

This research was carried out by PwC from December 2025 to March 2026. It was conducted through a series of round-table discussions and interviews with CNI leaders from private sector businesses, public sector organisations, and government departments.

About PwC UK

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum.
Find out more at **www.pwc.com**

About the National Preparedness Commission

The National Preparedness Commission is an independent, not-for-profit body, whose mission is to promote policies and other activities that lead to a better-prepared UK. See more at **www.nationalpreparednesscommission.uk**

Appendices

Appendix A: Key responsibilities of the National Exchange for Sustaining Critical Infrastructure Services (NEXSCIS)

1. Consistent senior representation will be pivotal to success.
Attendance should include members of:
a) Government – COBR, NCSC, and relevant departments.
b) CNI boards.
c) Local Resilience Forums.
d) Industry associations.
e) Subject matter experts, including systems thinkers to design stress testing.

2. It should communicate:
a) Critical mutual dependencies
Generate cross-CNI visibility of mutual dependencies. A unified system needs a complete view of its dependencies. This is essential to understand the practical challenges and avoid false assumptions about the availability of critical dependencies in a crisis.
b) Minimum recovery times across infrastructure and dependencies
Ensure each CNI operator's recovery timeline is governed by minimum viable system requirements rather than individual organisational priorities. For example: Transport for London's (TfL) minimum recovery time for transportation is currently 24 hours. But there's no visibility if other parts of the system need swifter recovery. Unified, systemic thinking may require TfL's recovery timeline to be expedited to enable other CNI operatorsreliant on transport to remain sufficiently resilient.
c) Regulatory hurdles to resilience and recovery
Enable government to maintain an understanding of how market conditions, regulation, and policy create incentives or disincentives for resilience investment.
d) Practical barriers to regulatory implementation
Provide government with regular industry insights into the practical challenges of implementing resilience measures, informing expectations of progress towards whole-of-society resilience.

3. It should agree:
a) A single, cross-sector definition of CNI resilience.
b) A single cross-sector resilience lexicon and vocabulary.
This is essential to build a common understanding of the risk and resilience landscape across all CNI.
c) A process for deciding when competition can be suspended and cooperation adopted to sustain critical national functions.

4. It should share best practice for building resilience:
This can include efficient implementation, optimum resilience levels, and a cross-CNI standard.

5. It should drive the creation of an information-sharing model:
One example for adaptation could be the Financial Sector Cyber Collaboration Centre's (FSCCC) trust-tiered sharing model – a sector-wide information sharing methodology to manage sensitive information based on trust. Implementation will allow access to sensitive information without formal vetting.

Appendix B: Current government resilience initiatives

Cross-government resilience frameworks

- UK Government Resilience Action Plan: Overall resilience blueprint setting whole-of-government actions to increase UK resilience to systemic and acute risks. Published July 2025.

- The UK Government Resilience Framework: Foundational strategy outlining systems, principles, and capabilities to support national resilience.
  - Resilience Framework Implementation Updates: 2023 reports, detailing progress against the framework's commitments and cross-government resilience actions.

- Resilience Guidance and Doctrine (COBR Directorate guidance): Cabinet Office guidance to support consistent resilience planning and doctrine across government and responders.

Risk assessment publications

- National Risk Register for Civil Emergencies: Government publication identifying and categorising major risks and hazards to the UK.

National security community / Risk-specific strategic plans

National security and strategic planning

- **National Security Strategy 2025: Security for the British People in a Dangerous World:** Government's main national security strategy integrating resilience as a core component of 'security at home'.
  - Includes cross-cutting elements such as cyber resilience, infrastructure resilience, biological risk preparedness, and supply chain considerations.
- **Strategic Defence Review 2025 (linked to NSS 2025):** Defence domain strategy with resilience implications for homeland and critical infrastructure security (this is embedded in the NSS 2025 framework).

Biological and health resilience

- **UK Biological Security Strategy:** Sets out actions to protect the UK from biological risks (contained within the Resilience Framework 2023 Implementation Update).
- **Pandemic Preparedness Strategy:** Department of Health and Social Care publication outlining preparedness action for future pandemics.

Cyber and digital resilience

- **Government Cyber Security Strategy:** High-level cyber resilience strategy – continued iteration following 2016-21 strategy.
- **Cyber Security and Resilience Bill:** New legislation aimed at strengthening cyber resilience across critical services and infrastructure.
- **Cyber Resilience Strategy for Defence:** MOD strategy focused on ensuring the defence sector continues operations under cyber attack (feeds into broader cyber resilience).

Critical infrastructure and supply chain resilience

- **Supply Chains Resilience Framework** (part of the Resilience Framework): Cross-government guide to strengthening supply chain resilience.
- **Energy Security and Resilience Taskforce and Energy Resilience Strategy:** Cross-government initiative focusing on grid resilience and infrastructure robustness; full strategy planned for 2026 (announced Nov 2025).

Individual government department resilience plans and guidance

Cabinet Office

- **Organisational Resilience Guidance for UK Government Departments, Agencies and Arm's Length Bodies:** Departmental resilience planning guidance across government bodies.

Department of Health and Social Care

- **Pandemic Preparedness Framework (awaiting publication):** Another element of this plan will align physical health preparedness with broader resilience actions.

Local and multi-agency resilience structures

- **Local resilience forum plans:** Regionally tailored emergency and resilience plans (not a single national document but operationally critical and referenced across resilience planning).

Energy

Energy Resilience Strategy: Currently being drafted.

Please note that the list above is not exhaustive and is based on sources available at the time of publication.

Appendix C: Building on existing thinking to identify what's most urgent (expanded version)

Our background analysis found many good pre-existing ideas to start addressing the UK's resilience challenges. These have yielded consistent themes that we have built on and extrapolated to identify the deeper requirements for a resilient CNI system-of-systems.

What needs to be done	What's required to make this happen
Adopt a whole-of-society approach Resilience is everyone's business, not only the responsibility of government. Numerous studies advocate a whole-of-society approach, and every organisation must hold some accountability for it. Nowhere more so than across CNI.	**Systemic thinking** • Build resilience capacity throughout the CNI ecosystem and into wider society by combining government leadership with private sector execution on the ground. **Compliance with government guidance** • While UK CNI governance currently assigns accountability to government departments, the UK Government Resilience Framework increasingly emphasises shared responsibility with operators and local actors. This is exactly what a systemic approach enables.

What needs to be done	What's required to make this happen
Move from silos to systems No organisation is immune from a crisis. Proposed solutions consistently highlight the need to replace siloed thinking with systems thinking, both within individual organisations and across CNI.	**Effective information sharing** • Better cross-sector insights to pinpoint vulnerabilities across interdependencies. **Flexibility with scale** • A balance that allows individual CNI organisations the agility to act independently while also operating as part of a larger system. **Use of specialist expertise** • The ability to delegate authority to those with the right technical or domain expertise. • This could encourage better decisions on complex technical matters – e.g. to identify what is critical to the organisation and wider system.
Prepare now for emerging long-term threats We need to be realistic about looking beyond the short-term to prepare for far more serious threats that could plausibly materialise. This means taking seriously the more extreme risks from climate change, AI, major geopolitical conflict, and health crises. If we wait too long, it could be too late. The time for systemic, long-term thinking is now.	**Prepare for plausible scenarios** • We mustn't underestimate how much the world could change. • Preparing for plausible scenarios, not just the most familiar or probable ones, is what builds real resilience.

What needs to be done	What's required to make this happen
Strengthen resilience culture A strong resilience culture starts with clear accountability at the top. Improved governance, independent oversight, and better measurement and metrics are all needed to drive adoption.	**Empower CNI operators to make better decisions** • Inform operators and equip them to make better decisions closer to the point of action, where managers have better local knowledge. • Respond faster to customers, regulators, and market changes by reducing bottlenecks. **Distribute accountabilities and responsibilities effectively** • Shift government responsibility from managing to coordinating the whole system so that government has oversight while operators implement. • Enable local and organisational flexibility, rather than defining standards that constrain innovation and provide false comfort. **Realise cultural benefits** • Leaders should embed an enterprise-wide resilience culture across their organisations. • Encourage innovative approaches to drive resilience at all levels of the organisation. • Enhance motivation, engagement, and a shared commitment to resilience goals.

What needs to be done	What's required to make this happen
Realise value through resilience Getting on the front foot to drive resilience through crisis planning is more cost-effective than scrambling to react when disruption occurs.	**Avoid costly resilience requirements** • Resilient organisations benefit from protecting their value during a crisis; efforts to increase systemic resilience must recognise and respect this.
Deliver on government's duty of care There's also a moral imperative to drive CNI resilience in ways that balance regional and community disparities. Research demonstrates that underserved regions and vulnerable groups are disproportionately exposed to crisis impacts. Inaction puts them at greater risk of experiencing those impacts most strongly.	**Embody a whole-of-society approach** • Resilient infrastructure must be designed and delivered in ways that offer equality of protection to all, including vulnerable groups and underserved regions.

NATIONAL PREPAREDNESS COMMISSION

Connecting for continuity in a crisis

Joining forces to strengthen UK resilience