FUTURE RESILIENCE AND COMPETITIVENESS

A PUBLIC-PRIVATE MODEL FOR THE UK IN A NEW WORLD ORDER

AUTHORS
Professor Paolo Taticchi, OMRI
Catrina Daly

REVISION
October 2025

UCL SCHOOL OF MANAGEMENT

POOL Re
REINSURING TERRORISM RISK

Future Resilience
FORUM

FOREWORD

The UK and the wider world face a period of profound uncertainty. Crises in one domain now spill into others, crossing borders and sectors, testing both national preparedness and economic competitiveness. These challenges are systemic, interconnected, and unpredictable. No government, business, or institution can meet them alone. They demand new forms of collaboration rooted in trust, reciprocity, and shared purpose.

Pool Re's mission is to ensure every business in Great Britain can access affordable and comprehensive terrorism insurance, fostering confidence in the economy and insulating taxpayers from catastrophic losses. Since 1993, this unique public–private partnership has paid more than £635 million in claims and today covers UK assets worth £2.2 trillion, from local traders and shopping centres to airports, power grids, and sectors including real estate, retail, transport, construction, and energy. Over three decades, Pool Re has become a global leader in terrorism risk financing, proving that collective strength is built through partnerships bridging government, business, and society.

This is why the Future Resilience Forum (FRF) has partnered with Pool Re: to explore systemic risks that cut across sectors and to build a model capable of generating forward-looking insights for both business and government. FRF is more than an international security conference. It is a call for collective action across geopolitical, technological, and economic domains. Its mission is to build resilience in democracies by identifying long-term geopolitical and geoeconomic threats while also highlighting opportunities that must be seized now to secure global stability and prosperity.

FRF brings together diverse industries with government and security communities to address shared challenges. Its purpose is to create partnerships and dialogue that endure, building trust across borders and sectors. These relationships are designed to withstand disagreement, adapt to disruption, and grow stronger through collaboration.

This white paper reflects that alignment. Just as Pool Re has shown the value of a trusted public–private model in terrorism risk financing, and just as FRF seeks to demonstrate globally, long-term security and competitiveness depend on collaboration around shared challenges and common values.

As co-authors of this Foreword, we are proud to support this work and commend it to policymakers, businesses, and researchers. The proposals here are pragmatic, timely, and rooted in a simple but powerful idea: competitiveness and security are inseparable, and both depend on partnerships that endure.

Fiona Hill CBE
Founder, Future Resilience Forum

Tom Clementi
CEO, Pool Reinsurance Company Limited

EXECUTIVE SUMMARY

The UK faces a period of accelerating systemic risk. The pandemic, cyber disruption, climate volatility, and geopolitical instability have each shown how shocks cascade rapidly across sectors, undermining both resilience and competitiveness.

Recent government analysis underlines the scale of exposure. The Government's *Chronic Risks Analysis* (2025) highlighted interdependencies across energy, climate, and health, while the CMA's *State of UK Competition* (2024) found that business dynamism has declined sharply over the past 25 years. Trade now represents around 70% of UK GDP, up from 43% in 1970, reflecting deep reliance on global supply chains. While this interdependence has reduced costs and expanded access to goods, it has also created systemic vulnerabilities: shocks such as the COVID-19 pandemic and the war in Ukraine disrupted flows of food, fuel, and commodities, with energy price volatility further magnifying these pressures across households and supply chains.

Government cannot anticipate or manage these challenges alone. Businesses, too, encounter limits when preparing for risks in isolation. The findings presented in this paper highlight a practical solution: structured collaboration, in which the public and private sectors share foresight, data, and analysis to strengthen national resilience.

This study draws on research with fifteen senior leaders from finance, infrastructure, health, technology, and security, supplemented by international comparisons. The findings reveal that the UK has untapped reservoirs of business insight that could materially enhance foresight and planning if shared securely with clear mutual value.

Three consistent lessons emerge. First, trust and confidentiality are prerequisites: firms will not share sensitive perspectives without legal clarity, controlled readership, and assurances against misuse. Second, collaboration must be reciprocal: too often, data has flowed into government without visible benefit in return. Sustained engagement requires outputs that are actionable for companies as well as policymakers. Third, any framework must reflect the diversity of the UK economy: multinationals, SMEs, and critical infrastructure providers all hold distinct perspectives that are not interchangeable; inclusivity is essential for credibility.

Findings from the research suggest a phased pathway for the UK. A pilot initiative, anchored in the Cabinet Office, should begin with a small, representative cohort of firms. This initiative would test mechanisms for secure data exchange and reciprocal outputs, such as quarterly risk reports, targeted briefings, and structured access to decision-makers. Crucially, participation would be supported by robust legal protections and confidentiality frameworks, ensuring obligations are mutual and enforceable.

The long-term objective is the creation of a UK Competitiveness and Resilience Partnership Model: a standing, co-chaired mechanism that embeds business–government collaboration on systemic risks. Such a model would not only strengthen national preparedness for shocks but also reinforce the UK's competitive standing in a volatile global economy. The research is clear: businesses are willing to contribute insight to the national interest, but only within a framework that protects independence, demonstrates reciprocity, and provides tangible value. By beginning with a carefully scoped pilot, the UK can move beyond fragmented engagement, keep pace with international competitors, and establish the foundations for a trusted, enduring partnership.

TABLE OF CONTENTS

Foreword 2

Executive Summary 3

Table of Contents 4

1. Introduction 5

2. The Case for Action: Business Insight in National Decision-Making 7

2.1 Finance and Insurance 7
2.2 Energy and Infrastructure 7
2.3 Technology and Data 8
2.4 Health and Life Sciences 9
2.5 Practical Use Cases 10
2.6 The Case for Urgency 10

3. Case Studies and Examples 11

3.1 United States – OSAC 11
3.2 France – State–Industry Links 11
3.3 Singapore – Committees on Competitiveness 11
3.4 Sweden – Commercial Insight in Intelligence 11
3.5 United Kingdom – Existing Models 12
3.6 Observations for the UK 12

4. Conditions for Collaboration: Findings from the Research 13

4.1 Trust and Confidentiality 13
4.2 Purpose and Reciprocity 13
4.3 Practicality and Proportionality 13
4.4 Fragmentation and Silos 14
4.5 Technology and Data Handling 14
4.6 Longevity and Governance 14
4.7 Inclusivity and Representation 14

5. Design Options for a UK Model 15

5.1 Formal, Regulated Framework 15
5.2 Informal, Trust-Based Exchange 15
5.3 Pilot-Based Approach 15
5.4 Roundtable Forum Model 16
5.5 Criteria for Assessment 16
5.6 Comparative Reflections 16

6. Pilot Pathway 17
6.1 Criteria for Selecting Pilots 17
6.2 Structure and Governance 17
6.3 Participation and Representation 18
6.4 Incentives and Outputs 18
6.5 Trust-Building Mechanisms 18
6.6 Scaling and Evolution 19

7. Recommendations 20

8. Conclusion 21

Appendix: Stakeholder Engagement and Sources 22

Authors 23

1. INTRODUCTION

The Future Resilience Forum has commissioned this white paper, in collaboration with the UCL Centre for Sustainable Business and Pool Re, to examine how business and government can work together more effectively to anticipate and manage systemic risks. It responds to a growing recognition that resilience is not solely the responsibility of the state but is shaped by the ways in which public and private actors exchange insight, align incentives, and prepare for uncertainty.

The scope of the paper is to explore the value of creating a standing framework through which business perspectives and insights can be brought into national resilience planning. This involves mapping both the threats and opportunities where collaboration could have the greatest impact. Cyber disruption, health emergencies, energy volatility, climate pressures, the rapid deployment of artificial intelligence, and geopolitical shocks all carry consequences that reverberate across supply chains, financial systems, and public trust. At the same time, opportunities exist to harness business insight for long-term competitiveness, from monitoring shifts in global investment patterns to identifying vulnerabilities in critical infrastructure and supply chains before they crystallise into crises.

Corporations with an international presence sit on valuable information that could significantly enhance and enrich government understanding of geographies and emerging risks. Senior executives of energy companies, financial institutions, health multinationals, and technology firms often enjoy access and perspective that official agencies cannot replicate, sometimes closer to political leadership abroad than UK ambassadors themselves. In an era of systemic shocks and contested global influence, such insight is not peripheral but central to national resilience and competitiveness.

Research findings highlight that a collaborative framework could transform this untapped asset into a mutually beneficial exchange: government gaining foresight and situational awareness; business gaining proximity to decision-making, enhanced overseas influence, and more resilient market access. Comparable models already exist abroad, where firms systematically report into their governments, bolstering state awareness and corporate positioning. While the UK will not emulate such systems, the lesson is clear: countries that integrate corporate perspectives into national intelligence are not disadvantaged in global competition. For the UK, a tailored, secure, and voluntary partnership could both strengthen resilience and support companies seeking to expand overseas.

A wide range of sectors will be essential to any national model. Multinational corporations hold unique perspectives from overseas operations. Energy and infrastructure providers manage assets that underpin national life. Financial institutions have visibility over transaction flows that can indicate instability. Technology firms collect and analyse data at scale, often detecting trends before they are recognised elsewhere. Health companies carry expertise that is vital to anticipating and responding to future pandemics. Each of these perspectives is partial but taken together they provide a broader and richer picture of systemic risk.

International practice demonstrates that collaboration of this kind is possible. In some countries, business and government work side by side in permanent structures; in others, cooperation is organised around competitiveness and growth. While these models cannot be replicated wholesale, they show that effective frameworks can be designed when mutual benefit and trust are established.

This paper therefore maps the landscape of risks and opportunities, drawing on research with senior leaders across finance, energy, technology, health, infrastructure, and security. It identifies where business insight could most usefully complement national risk processes, outlines international lessons, and develops options for how the United Kingdom might design a collaborative framework of its own. The focus is on evidence and pathways, rather than prescribing a fixed model — setting the stage for later sections that evaluate design choices and propose a phased approach.

2. THE CASE FOR ACTION: BUSINESS INSIGHT IN NATIONAL DECISION-MAKING

The challenge facing the United Kingdom is not a lack of data, but a lack of structures through which valuable insight can be shared and applied across institutional boundaries. Businesses already generate intelligence of direct relevance to national resilience, yet this remains fragmented and under-utilised. The argument for structured collaboration is therefore not abstract but grounded in practical opportunities to strengthen foresight in key sectors.

Many large firms already contribute to international foresight exercises such as the World Economic Forum's Global Risks Report, which maps interconnected risks across geopolitics, technology, health, and the environment. Yet while UK businesses feed into global frameworks, there is no equivalent domestic structure to integrate their insight into the UK's own resilience planning. The National Security Risk Assessment (NSRA) and the National Risk Register (NRR) provide the government's official assessment of the most serious risks facing the UK. Both are regularly updated, with the NRR recently reformed to operate on a dynamic model refreshed several times a year. These frameworks could be complemented by structured business insights, adding depth and inclusivity. Overseas operations can flag geopolitical and supply chain vulnerabilities earlier, financial institutions can provide data on market stress, and infrastructure operators can highlight interdependencies not always visible to government.

2.1 FINANCE AND INSURANCE

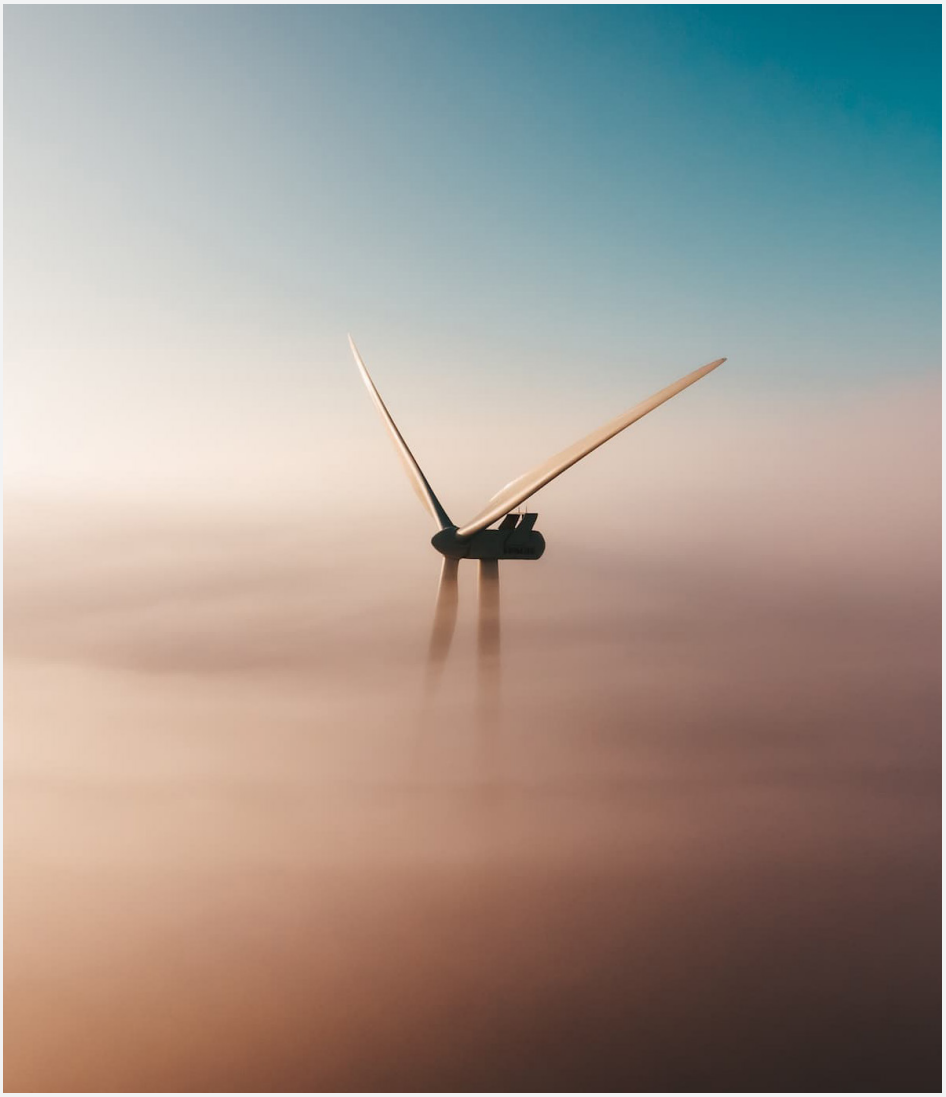
Financial institutions are acutely sensitive to geopolitical shocks, commodity volatility, and emerging patterns of instability. They track capital flows daily, model exposures across markets, and maintain visibility over transactions that may indicate unusual behaviour. One of the most persistent risks in this space is cyber-facilitated fraud, which remains widespread across UK firms. Aggregate insights from banks and insurers could provide early warning of systemic criminal exploitation while informing regulatory and law-enforcement responses.

Payment networks also provide unique visibility across economies. Aggregated spending data from companies such as Visa and Mastercard has already been used by HM Treasury. Unlike official statistics, which are published with a delay, these datasets can offer leading indicators of shifts in economic activity. Insurers hold equally valuable foresight: their catastrophe models quantify the potential impacts of natural disasters, terrorism, or pandemics, often at a level of granularity beyond national risk registers. Because these models underpin underwriting, they are continuously updated and tested against real-world losses. If selected outputs were shared securely, government would gain a richer picture of systemic risk, while firms would benefit from alignment with national assessments.

The insurance market also holds detailed intelligence that underpins risk modelling — including data not otherwise available to government. This demonstrates how structured public–private models can address systemic threats. A similar approach could be applied to cyber risk, where private markets alone lack the capacity to absorb large-scale events. Cyber has the potential to be systemic in nature, particularly with the expansion of attack surfaces through AI-enabled tools and increasingly complex IT supply chains.

2.2 ENERGY AND INFRASTRUCTURE

Companies in the energy sector operate across global supply chains and geopolitical landscapes that are often more volatile than official reporting suggests. They manage production, transport and refining networks that are vulnerable to disruption from sanctions, conflict or environmental hazards. Infrastructure providers hold equally critical data, monitoring the resilience of transport, utilities and communications systems. Insights from these companies can reveal where vulnerabilities are forming long before they become public crises. For example, firms reported that they often receive signals of political shifts or regulatory changes through direct interaction



2.3 TECHNOLOGY AND DATA

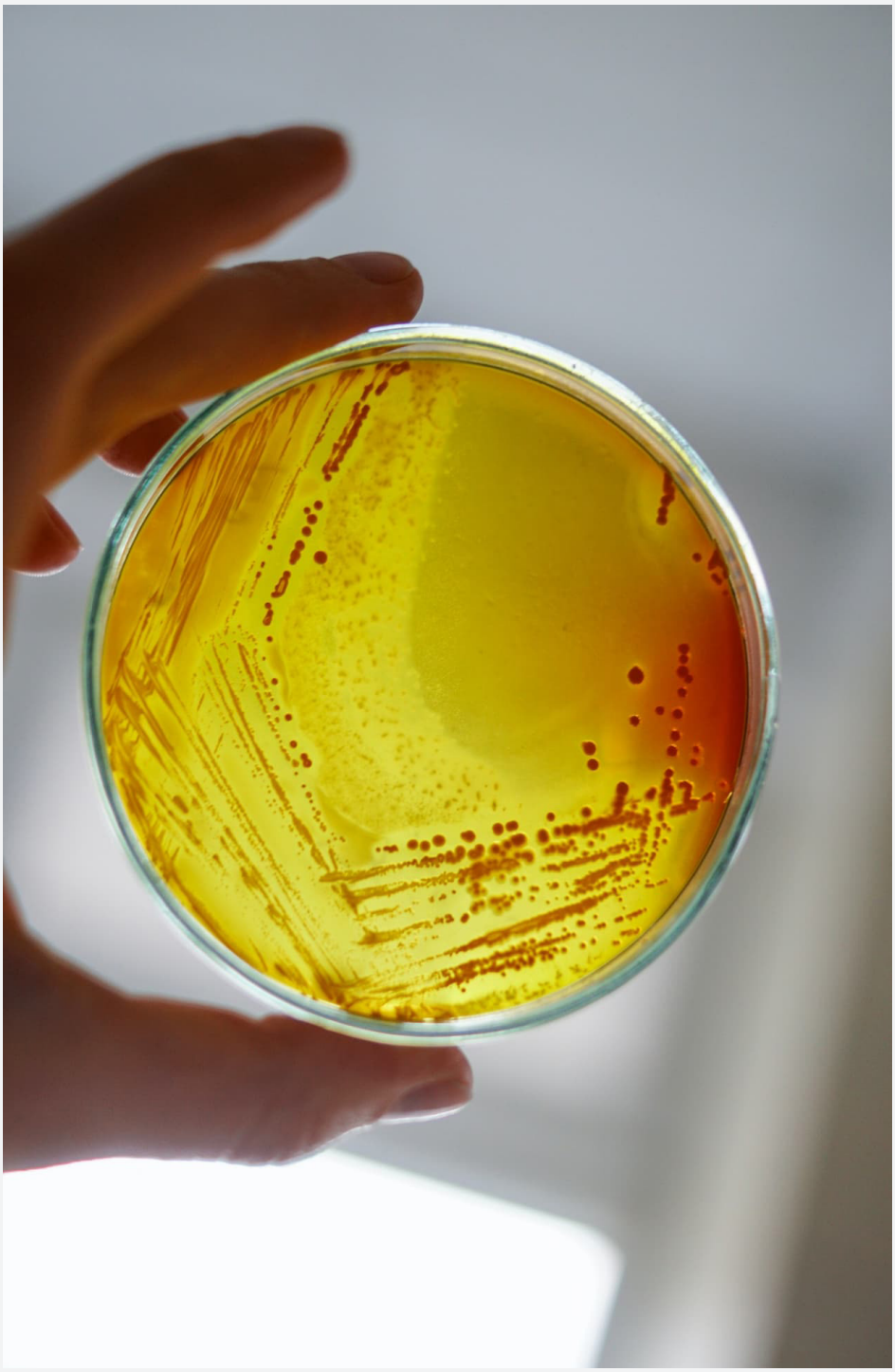
The Cyber Security Breaches Survey 2025, the research study on UK cyber resilience, found that an estimated 3% of all businesses and 1% of charities experienced fraud resulting from a cyber breach or attack in the past 12 months — equivalent to around 40,000 businesses and 2,000 charities, with an estimated 72,000 incidents in total. These figures underline how cyber-facilitated fraud is now a systemic risk alongside espionage, ransomware, and data exfiltration.

Technology companies, particularly those working with advanced analytics, artificial intelligence, and cyber defence, hold datasets of extraordinary scale and richness. These include records of attempted intrusions, patterns of malicious cyber activity, and early indicators of systemic vulnerabilities in software and hardware. The challenge is not only technical but also organisational. Businesses emphasised the need for privacy-enhancing technologies that allow for federated analysis, where each organisation retains control of its raw data but contributes aggregated outputs to a collective model. Such approaches would allow cyberattack patterns — including fraud and espionage campaigns — to be identified across multiple companies without exposing internal systems.

The same model could apply beyond cyber to domains such as environmental monitoring, where aggregated corporate data on emissions or supply chain risks would strengthen national sustainability and resilience strategies.

2.4 HEALTH AND LIFE SCIENCES

Companies in the pharmaceutical and healthcare sectors hold foresight that proved critical during the COVID-19 pandemic. They monitor the spread of disease, track disruptions in clinical trials and navigate regulatory frameworks across multiple jurisdictions. These insights were invaluable for understanding supply chain resilience, vaccine development and the capacity of health systems to respond. Looking forward, businesses have highlighted the importance of antimicrobial resistance, pandemic preparedness and regulatory harmonisation as areas where organised information exchange with government could save lives as well as costs. One practical proposal was a system for confidentially reporting aggregate data on workforce illness, giving government early signals of outbreaks by geography or sector while protecting commercially sensitive details.



2.5 PRACTICAL USE CASES

The research underlined that abstract calls for information sharing are insufficient. What matters are practical, issue-led use cases that show clear mutual value:

- **Economic and financial indicators.** Aggregated spending data from payment networks provides near real-time insight into consumer demand and economic shifts.
- **Labour market signals.** Recruitment platforms such as Adzuna provide live vacancy data, already used in official labour market statistics.
  Declines in postings for certain roles, such as administrative staff, have historically acted as early warning of downturns.
- **Public health monitoring.** Aggregated, anonymised reporting of workforce illness could provide government with early warnings of outbreaks while offering businesses visibility over sectoral resilience.
- **Cybersecurity.** Firms could share indicators of malicious activity without revealing internal network details, strengthening national defences and improving private sector benchmarking.
- **Supply chain resilience.** Logistics and construction companies already use tools that integrate trade, shipping and aviation data to map dependencies across multiple tiers. Shared selectively, this would strengthen the National Risk Register and resilience planning.
- **Border operations.** Companies involved in logistics hold real-time data on border delays and chokepoints, providing government with an operational perspective not always captured in official statistics.

Across these examples, two principles stand out. Governments benefit most from lead indicators which are real-time signals of change, rather than lagging statistics. And businesses will only participate if information is shared through secure, trusted mechanisms, with reciprocal value such as aggregated analysis, early warnings or closer alignment with national planning.

2.6 THE CASE FOR URGENCY

The costs of inaction are becoming clear. Without formalised cooperation, government risks missing signals that businesses already hold, while businesses are deprived of official perspectives that could guide investment and planning. Both sides lose when insight remains fragmented. By contrast, a structured model for collaboration would expand situational awareness, enable the detection of early signals in the noise, and align the United Kingdom's economic competitiveness with its national resilience.

3. CASE STUDIES AND EXAMPLES

Examining international practice is important because it shows how other governments have structured cooperation with the private sector. Studying these examples helps clarify what works, what does not, and what principles might guide a UK framework. The purpose here is not to replicate foreign systems but to understand the different ways collaboration has been organised, and what lessons may be relevant in shaping a UK approach.

3.1 UNITED STATES – OVERSEAS SECURITY ADVISORY COUNCIL

OSAC, created in 1985 by the US Department of State, has become one of the most durable examples of structured public–private cooperation. It connects thousands of organisations worldwide and provides regular briefings on overseas threats, travel advisories, and country-level risks. Its value lies in reciprocity: companies contribute perspectives from their operations abroad, while government provides consolidated analysis in return. The US model demonstrates that collaboration can endure over decades when participation is voluntary, confidentiality is respected, and outputs are consistently useful. The strength of OSAC lies in its dual appeal — US firms see clear benefit from receiving information, while government benefits equally from private-sector feedback.

3.2 FRANCE – STATE–INDUSTRY LINKS IN STRATEGIC

Stakeholders also highlighted the French tradition of close collaboration between the state and large firms in strategic areas such as aerospace, energy, and defence. One example raised was the role of private business-intelligence firms with established ties to national security services, which multinationals sometimes rely on for due diligence and strategic advice. This reflects a model where coherence between state and corporate priorities can reinforce national strategy. One example raised was the role of the Direction Générale de la Sécurité Extérieure (DGSE), which has historically maintained close links with large national companies. However, stakeholders stressed that any UK model would need to carefully preserve independence and confidentiality, avoiding arrangements that could compromise trust.

3.3 SINGAPORE – COMMITTEES ON COMPETITIVENESS

Singapore offers a structured, committee-based model in which government, business, and academia convene to align around long-term national priorities. Its 2025 Economic Strategy Review, for example, included a Committee on Global Competitiveness that brought together multinational corporations alongside domestic firms to chart growth opportunities and strengthen economic resilience. This approach demonstrates the value of embedding competitiveness and resilience in the same agenda, ensuring that private-sector contributions are purposeful and directly linked to national outcomes.

3.4 SWEDEN – INCORPORATING COMMERCIAL INSIGHT INTO INTELLIGENCE

Sweden's recent reforms in the intelligence sphere have emphasised that partnerships with commercial actors can create new opportunities to strengthen analysis. Proposals have suggested that a new agency could be tasked with producing a comprehensive national intelligence assessment in cooperation with other government bodies, explicitly including input from commercial perspectives. This reflects recognition that industry often holds data and foresight that government alone cannot generate, and that collaboration is needed to produce a more comprehensive threat picture.

3.5 THE UNITED KINGDOM – EXISTING MODELS

The UK does not currently have a directly comparable mechanism to OSAC in the United States or Singapore's competitiveness committees. Existing forums, such as business networks, provide valuable dialogue but do not function as structured intelligence-sharing mechanisms.
Where the UK has made tangible progress is in specific domains, particularly cybersecurity. The National Cyber Security Centre (NCSC) has built trusted channels with businesses for sharing threat intelligence, conducting joint exercises, and providing tailored guidance. This demonstrates that when the scope is clearly defined and supported institutionally, government and industry can collaborate effectively.

The challenge is whether such trusted models can be extended beyond cyber to cover a broader spectrum of systemic risks, from supply chain resilience to health and climate. This remains the central opportunity for the UK.

3.6 OBSERVATIONS FOR THE UNITED KINGDOM

Taken together, these cases suggest several considerations for the UK debate:

- **Defined remit.** OSAC illustrates the value of a tightly scoped mission with consistent outputs; Singapore shows how competitiveness can provide a unifying objective.
- **Balanced participation.** Successful models engage different scales of business, ensuring perspectives extend beyond a narrow group of incumbents.
- **Mutual value.** Collaboration endures only where companies see clear benefit — whether through early warning, aggregated analysis, or structured access to government.

Examining allies and competitors alike demonstrates that structured collaboration is feasible and increasingly common. The UK already has pockets of strength, particularly in cybersecurity, but lacks an overarching model for harnessing corporate insights across sectors. Designing such a framework will require building on existing good practice, protecting independence and ensuring confidentiality.

4. CONDITIONS FOR COLLABORATION: FINDINGS FROM THE RESEARCH

The research revealed both a strong appetite for closer collaboration and significant reservations about how it is structured. Businesses recognised the potential benefits of formal frameworks but highlighted persistent barriers that have limited engagement in the past. These include the lack of feedback loops, a tendency for government to request exhaustive datasets rather than targeted indicators, and fragmentation across government. Concerns around reputational risk, confidentiality, and unclear purpose were also consistent. The sections that follow synthesise these findings.

4.1 TRUST AND CONFIDENTIALITY

Trust emerged as the most consistent prerequisite. Companies emphasised that sharing sensitive operational data carries both reputational and commercial risk, and that participation depends on credible safeguards. Several noted that while government sometimes proposes its own confidentiality agreements, businesses are often more comfortable using their own contractual frameworks, ensuring obligations are enforceable on both sides.

The risk of misuse — whether through leaks or inadequate handling — was a recurring concern. Findings suggest that any framework must be underpinned by enforceable MoUs or contractual agreements. Companies also stressed that their preference is for NDAs that are binding on government as well as themselves.

4.2 PURPOSE AND RECIPROCITY

Equally important was clarity of purpose. Businesses want to understand why information is being requested, how it will be used, and what value they will gain in return. Without this, data sharing risks being seen as administrative burden rather than strategic contribution.

Companies distinguished between issues where they are willing to contribute for collective benefit, such as pandemic preparedness or systemic cyber resilience, and areas where competitive advantage is at stake, where caution is greater. In the latter, reciprocity must be explicit and tangible.

Several practical examples show how this can work. The UK Vaccine Taskforce and the European Exit Relationship Group were cited as successful models of purpose-driven collaboration, where government, industry, the NHS, and academia worked together in structured, co-chaired forums. Elsewhere, global payments companies have provided aggregate spending data to HM Treasury, while labour-market platforms such as Adzuna have generated early indicators of downturns. These insights, collected for commercial purposes, acquired public value when shared in aggregate. In return, businesses expect actionable outputs: timely alerts, structured analysis, and risk reports that demonstrate how their contributions shape decisions.

4.3 PRACTICALITY AND PROPORTIONALITY

The research also highlighted frustration at government's tendency to request exhaustive datasets, which are resource-intensive and often arrive too late to inform decisions. Companies argued instead for timely, targeted indicators — such as payroll trends, transaction volumes, or cyberattack patterns — that provide early warning without unnecessary burden.

Examples such as HMRC's real-time payroll data show how concise, regularly updated indices can deliver significant insight. Others pointed to health datasets, where NHS records have enabled world-leading innovation but raised questions about access rights and fairness. The message was clear: government requests must be proportionate, carefully scoped, and designed for visible impact.

4.4 FRAGMENTATION AND GOVERNMENT SILOS

Even when businesses are willing to contribute, fragmentation in government reduces the value of engagement. Systemic risks cut across finance, health, infrastructure, and supply chains, yet departments remain siloed. Inputs offered to one department often fail to reach others who could benefit. Research participants argued for a single, joined-up channel for structured engagement, ideally located in the Cabinet Office or with a neutral convenor, to ensure inputs are aggregated, protected, and shared across government.

4.5 TECHNOLOGY AND DATA HANDLING

Technical design is also central to trust. Findings suggest that any platform must combine strong security with tiered access: aggregated outputs available widely, restricted reports for vetted participants, and highly confidential briefings for a small circle of cleared actors. Privacy-preserving technologies such as federated analysis — where raw data remains within companies' systems but contributes to collective models — were seen as adaptable from existing uses in cyber security and health research. A trusted environment for sharing indexed rather than raw data would go a long way toward enabling participation.

4.6 LONGEVITY AND GOVERNANCE

Any framework must be designed to endure. Past efforts have faltered when government priorities shifted, or elections intervened. For credibility, new structures should be embedded in formal governance, ideally reporting into a standing Cabinet committee. Pilot initiatives should be explicitly linked to longer-term institutionalisation, so that early experiments build momentum rather than fade. Businesses will only invest if they are confident that arrangements are durable, purposeful, and embedded in national strategy.

4.7 INCLUSIVITY AND REPRESENTATION

Finally, inclusivity was a consistent concern. If collaboration is dominated by large incumbent firms, it risks skewing priorities and overlooking wider perspectives. Smaller firms and start-ups often hold valuable frontline information but lack resources to engage directly. While trade bodies and sector associations play an important role, relying on them exclusively may dilute signals. Findings therefore suggest that credibility requires balanced participation: established multinationals and SMEs all need a seat at the table. Inclusivity is not only a fairness issue but essential to capturing the full spectrum of insight across the economy.

5. DESIGN OPTIONS FOR A UK MODEL

The conditions identified in the research point to a central dilemma: government and business both recognise the value of closer collaboration, but trust, proportionality, and durability remain unresolved. Any framework must therefore balance three tensions: confidentiality versus utility, inclusivity versus efficiency, and flexibility versus continuity. Against this backdrop, three broad design options emerge for how the UK might structure a model for business–government collaboration.

5.1 FORMAL, REGULATED FRAMEWORK

A first option is the creation of a formal, regulated mechanism, overseen by government and underpinned by confidentiality agreements. This could resemble the NCSC's existing arrangements, where threat intelligence is exchanged within a secure environment, supported by technical standards, non-disclosure agreements, and statutory protections. Such a model offers clarity: participants would know precisely what data is sought, how it will be used, and what safeguards are in place. It would also provide government with reliable channels for early warning and structured insight. For businesses, the appeal lies in predictability, clear rules, and access to reciprocal information.

The risks are twofold. First, over-centralisation may deter participation if firms perceive the framework as government-dominated or bureaucratic. Second, regulation can stifle adaptability; systemic risks evolve quickly, and a rigid legal structure may not keep pace. Stakeholders noted that while formal frameworks build trust, they must avoid becoming "box-ticking" exercises.

5.2 INFORMAL, TRUST-BASED EXCHANGE

At the opposite end of the spectrum is an informal, networked model built on trust and personal relationships. The advantage is agility. Insights can be shared rapidly, without the delays of formal reporting cycles, and sensitive information can be tested in small circles before being scaled. Informal models also reduce barriers to entry for smaller firms, which may lack the resources to participate in highly structured processes. However, without formal governance, there is little guarantee of a mutual benefit or follow-up. Informal exchanges are valuable for horizon scanning, but they cannot substitute for structured arrangements where accountability and impact are visible.

5.3 PILOT-BASED APPROACH

The third pathway is a pilot-based approach centred on a secure information channel, operating alongside existing government risk architecture as a structured mechanism for business–government collaboration.

To ensure focus and alignment with national priorities, participation should be framed around themes drawn from the NSRA and the public-facing NRR. This would help business input complement existing risk processes while avoiding duplication.

The pilot could be co-chaired by government and industry, supported by an MoU that sets out clear terms of engagement: the scope of data-sharing, safeguards for confidentiality, and obligations for feedback. MoUs offer a practical balance between flexibility and assurance, allowing both sides to define expectations without the rigidity of statutory regulation.

By starting small, the pilot would avoid over-engineering while creating a controlled space to test privacy-preserving technologies, explore secure briefing formats, and evaluate governance structures. Success would be measured not by the volume of information exchanged but by whether participants gain tangible benefits such as improved foresight, stronger risk modelling, and closer alignment with national assessments.

5.4 ROUNDTABLE FORUM MODEL

A fourth option is a roundtable forum model, in which a small group of trusted companies (typically 6-12) meet regularly under Chatham House–style rules. These closed discussions foster candour, build confidence, and reduce the need for complex legal frameworks. Similar arrangements, such as quarterly Whitehall roundtables on Africa, have historically proved effective at surfacing first-hand commercial knowledge. Exclusivity can itself be an incentive: participants gain privileged access to decision-makers and peers, while the forum's credibility and reputation attract further interest, creating the potential to expand over time.

5.5 CRITERIA FOR ASSESSMENT

In assessing these four design options, the research applied three simple but robust criteria. First, impact: would the model materially strengthen national foresight and resilience? Second, ease of implementation: could it be established quickly without excessive bureaucracy or legal overhaul? Third, longevity: would participants remain engaged over time, with incentives aligned across government and business? These criteria were tested in discussion with participants, and the pilot-based approach emerged as the most balanced pathway: impactful, feasible to initiate, and able to evolve incrementally.

5.6 COMPARATIVE REFLECTIONS

The research suggests that the most credible pathway is sequenced rather than singular. Each design option brings strengths: formal frameworks provide clarity and assurance; informal networks allow agility; pilot models enable structured testing; and small, trust-based forums create the conditions for candour. On their own, each risks imbalance — too rigid, too fragile, too narrow, or too exclusive. Combined, they offer a progression.

A consistent message from participants was that collaboration must begin with trust. For some, this implied formal safeguards such as an MoU; for others, the emphasis was on forums where trusted companies (drawn from different sectors and not direct competitors) could speak openly without heavy legal scaffolding. Crucially, such forums are most effective when targeted around clearly defined risks or specific geographies. A roundtable on African market dynamics will yield very different insights from one on supply-chain cyber resilience, but both can provide government with foresight it cannot easily access on its own.

6. PILOT PATHWAY

The research findings consistently emphasised the importance of piloting before committing to a permanent framework. A single, well-structured pilot provides a pragmatic way to test ideas, demonstrate value, and build confidence without prematurely fixing an institutional design. It also addresses scepticism: many businesses will only engage once they see in practice that collaboration can be secure, reciprocal, and genuinely useful.

6.1 CRITERIA FOR SELECTING PILOTS

Pilots should be chosen with care, not least because early examples will shape perceptions of the entire initiative:

- **Systemic relevance.** A pilot should address risks that cut across multiple sectors, rather than narrow technical issues. Supply chain resilience, for example, matters simultaneously to manufacturers, retailers, logistics providers, and government planners, making it a natural candidate. By focusing on themes of broad consequence, the pilot demonstrates value beyond a single constituency.
- **Shared incentives**. Pilots should focus where government and corporate interests clearly overlap. Cyber resilience, for instance, is as vital to national security as it is to companies' commercial continuity. Focusing on these aligned spaces reduces friction and reassures participants that their input will not be used against their competitive interests.
- **Data maturity.** Success depends on starting where companies already collect information in a structured way. Hiring platforms, transaction networks, and logistics firms already generate datasets that can serve as forward indicators. Building on these existing streams avoids creating new reporting burdens and proves that collaboration can be efficient rather than extractive.
- **Representative participation.** A credible pilot must not only include major corporates but also smaller firms and trade associations. SMEs often provide the earliest signals of stress — for example, in export paperwork, supply chain costs, or credit conditions — but lack the resources for direct engagement. Including them ensures the pilot reflects the full economy rather than the vantage point of a few incumbents.

6.2 STRUCTURE AND GOVERNANCE

The Cabinet Office would be the most appropriate home for a pilot, given its cross-government remit and role in national resilience planning. As noted in Section 4.6 on longevity, continuity is essential if the model is to succeed. One way of securing this would be through the appointment of an external convenor. Frequent staff rotation in the civil service often undermines long-term initiatives, whereas an external convenor could provide stability, neutrality, and sustained focus. This figure should be a consensus appointment, chosen for relevant government and/or resilience experience, and could be appointed on a renewable fixed-term contract. By providing continuity and independence, the convenor would reinforce the longevity of the model while complementing official leadership within the Cabinet Office.

Staffing and budgetary considerations will inevitably arise, but these are practical issues that can be resolved if there is sufficient will and recognition of the value such a partnership can bring .

6.3 PARTICIPATION AND REPRESENTATION

A pilot should begin with a small group of 6 - 12 companies, carefully chosen from sectors with systemic importance such as finance, energy, technology, and life sciences. This keeps the group manageable while ensuring diversity of perspective. Representation must also extend beyond large corporates. Trade associations and chambers of commerce can channel perspectives from SMEs, ensuring their concerns are heard without imposing heavy resource burdens.

Alongside the formal pilot, a complementary forum-style model could be considered. Such forums can surface early signals and build personal trust more quickly than structured pilots. While they are limited in scale and rely heavily on individual participation, they can provide a valuable informal channel that runs in parallel with a pilot, ensuring that insights are not lost during the longer process of formalising collaboration.

6.4 INCENTIVES AND OUTPUTS

The credibility of any pilot rests on its outputs. Research findings indicated that companies will only invest if they see value returned in forms they can use. This might include:

- **Quarterly risk reports** developed by government, drawing on aggregated business input. These reports should not just catalogue risks but provide interpretation, demonstrating how corporate insight shapes national analysis.
- **Secure briefings** that give businesses early visibility of geopolitical, economic, or cyber trends identified by government. The reciprocal exchange — insight from business, analysis from government — is what sustains participation.
- **Access to decision-makers**, through structured dialogues with senior officials and ministers. For businesses, influence and proximity are incentives in themselves, provided they are linked to substantive outputs.
- **Insurance premium advantages**, with participation in structured data-sharing frameworks recognised by insurers as reducing uncertainty and systemic exposure. This could translate directly into lower premiums or preferential terms, creating a concrete financial return on engagement.

Each output is designed to reinforce reciprocity. They show businesses that engagement is not extractive but produces benefits they could not generate alone.

6.5 TRUST-BUILDING MECHANISMS

Trust will be the single most important determinant of success. To protect it, several mechanisms should be built into pilots from the outset:

- **Confidentiality agreements** that recognise companies' preference for their own NDAs or contractual frameworks. This ensures obligations are mutual and enforceable.
- **Tiered information handling**, distinguishing between general insights, restricted reports, and highly sensitive material. This reassures firms that contributions will not be overexposed.
- **Feedback loops**, so participants can see how their input influences government action. Absence of feedback was one of the strongest sources of frustration cited in interviews; pilots must correct this from the beginning.

Regular reviews, co-chaired by government and business, would allow processes to be adapted as confidence grows.

6.6 SCALING AND EVOLUTION

Pilots should not end as experiments but act as stepping stones to a durable framework. If successful, they could evolve into a standing UK Competitiveness and Resilience Committee. What matters is that pilots prove the concept: that business insight can be captured securely, analysed collectively, and translated into outputs that serve both government and industry.

If designed carefully, pilots will build the trust, credibility, and institutional memory required to make collaboration sustainable. They can show that structured partnership is not only possible but valuable, paving the way for a long-term framework embedded in national resilience and competitiveness strategy.

7. RECOMMENDATIONS

To move from principle to practice, the UK should launch a pilot initiative that demonstrates credibility, builds trust, and delivers measurable value. The following steps are proposed:

1. **Launch a Pilot Committee**
   Establish a UK Competitiveness and Resilience Committee (Pilot), co-chaired by government and industry, housed in the Cabinet Office. Begin with 6–12 trusted companies across critical sectors, alongside SME and academic representation.

2. **Set Legal and Confidentiality Safeguards**
   Participation should be governed by an MoU or contractual agreements that protect commercial interests, clarify confidentiality arrangements (for example, Chatham House rules), and define reciprocal obligations.

3. **Define Scope and Purpose**
   Agree early on the pilot's thematic focus — whether systemic risks (e.g., cyber resilience, supply chains), sector-specific vulnerabilities, or international insights — to ensure clarity of purpose and alignment with strategic priorities.

4. **Use Secure Technologies**
   Ensure outputs are accessible at different levels of sensitivity, from aggregate insights to restricted briefings.

5. **Embed Feedback and Outputs**
   Provide participants with regular, actionable outputs: quarterly reports, early-warning bulletins, and structured access to senior decision-makers.

6. **Secure Cabinet-Level Visibility**
   Route findings directly into Cabinet committees to avoid departmental silos and ensure business insights shape national strategy.

7. **Guarantee Inclusive Representation**
   Ensure participation reflects the full economy, balancing multinationals with SMEs and trade associations to capture diverse perspectives.

8. **Commit to Independent Review**
   Evaluate the pilot after 12 months against agreed criteria (participation, quality of insights, effectiveness of outputs, trust in governance). Use the results to inform scaling into a permanent national framework.

8. CONCLUSION

The UK is entering a period where systemic risks, from pandemics to cyber threats, from climate volatility to geopolitical shocks, will increasingly define national resilience and competitiveness. Government cannot manage these pressures alone, and businesses cannot prepare in isolation.

The research presented in this paper shows that a practical opportunity exists to turn corporate foresight into a shared national asset, through structured collaboration built on trust, reciprocity, and inclusivity. Other countries have already begun embedding business perspectives into resilience planning, and the UK must act if it is to remain competitive and prepared.

Launching a carefully scoped pilot will demonstrate that secure and reciprocal collaboration is both possible and valuable. From there, the UK can build a permanent framework that strengthens foresight, protects against cascading shocks, and ensures that national strategy reflects the insights of companies operating at the frontiers of global markets.

The case is clear. By moving beyond fragmented engagement, the UK can establish a trusted partnership between business and government that endures. Such a partnership will help safeguard resilience and reinforce competitiveness in a volatile global economy. The time to act is now.

APPENDIX: STAKEHOLDER ENGAGEMENT AND SOURCES

APPENDIX A. SECTORAL USE CASES (ILLUSTRATIVE)

SECTOR	POTENTIAL CONTRIBUTION	BENEFIT TO GOVERNMENT	BENEFIT TO BUSINESS
Finance & Insurance	Capital flow monitoring, catastrophe models	Real-time indicators of instability	Alignment with national assessments
Technology	Cyber intrusion data, federated analytics	Early warning of systemic vulnerabilities	Benchmarking & resilience planning
Health & Life Sciences	Outbreak monitoring, trial disruptions	Early detection of health risks	Policy clarity, supply chain resilience
Infrastructure	Border operations, supply chain chokepoints	Operational foresight	Policy predictability, risk reduction

B. METHODOLOGY

This paper is based on research conducted over four months, drawing on semi-structured interviews with senior representatives from finance, energy, infrastructure, life sciences, technology, construction, and media. To encourage candour, all contributions were anonymised. Insights were synthesised thematically and triangulated with published materials and international comparator models.

C. UK FRAMEWORKS AND DATA SOURCES

The analysis also drew on and referenced selected UK government documents and practice:

- **Chronic Risks Analysis** (Cabinet Office, 2025)
- **CMA State of UK Competition** (2024)
- **Cyber Security Breaches Survey** (DSIT & Home Office, 2025)

PAOLO TATICCHI

Paolo Taticchi is a Professor of Strategy and Sustainability and Deputy Director at UCL School of Management, where he co-directs the UCL Centre for Sustainable Business. A global expert in sustainability and strategy, he has trained thousands of Fortune 500 executives, taught at top business schools such as Imperial College London, and developed business projects across five continents.

His widely cited research includes over 50 publications and books such as How to Be Sustainable (2025) and Disruption(2023). In 2025, his research on impact investing was highly commended by the Financial Times for making a real difference. A sought-after speaker and advisor, he has delivered 250+ talks attended by more than 100,000 people and serves on several international advisory boards.

As an entrepreneur, he co-founded four companies and led major educational initiatives. His accolades include Poets & Quants “Top 40 Under 40 Business Professors in the World” (2018), being mentioned by Sole 24 Ore as the most influential Italian under 40 (2021-23), and inclusion in the Thinkers50 Radar List (2025).

E: p.taticchi@ucl.ac.uk
paolotaticchi.com

CATRINA DALY

Catrina Daly is Centre Manager at the UCL Centre for Sustainable Business, where she supports research and partnerships at the intersection of sustainability, competitiveness, and business strategy. Her work focuses on how corporate transformation and innovation can drive long-term value creation.

Before joining UCL, she advised global energy, infrastructure, and investment clients on investor relations and communications strategy, with experience spanning decarbonisation, regulatory engagement, and responsible business practices. Catrina holds an MA in Sustainability and Energy Management from Bocconi University and a BA (Hons) from Trinity College Dublin, and she speaks Italian and Spanish fluently.