



NATIONAL
PREPAREDNESS
COMMISSION

 MarshMcLennan

PARTNERING WITH PURPOSE

Strengthening national-level resilience
in the UK through more dynamic
public-private interactions

Marsh GuyCarpenter Mercer OliverWyman

EXECUTIVE SUMMARY

It's frequently acknowledged that preparedness for contingencies that threaten UK wellbeing and prosperity needs the participation of all sectors of society. The concerns are large, varied, complex, interconnected, and far-reaching. In turn, resilience efforts need to be multifaceted, adaptive, and widely owned.

The private sector can, should, and is keen to contribute in many ways. Companies have much to offer by way of finance, physical assets, workforce, capabilities, and innovation. Many corporate leaders recognise the value of both resilient business ecosystems and more general societal commitments. The right conditions can enable them to align commercial imperatives with larger national ambitions.

The experience of recent crises suggests that existing national resilience arrangements fall short of what is required for current and future shocks. Sustained supply-chain challenges, extreme weather events, large-scale cyber-attacks, energy crises of different kinds, and a still-evolving COVID-19 virus all argue for efforts to be increased and made more supple. Insufficient cohesion around mitigation measures and contingency plans, as well as the failure to anticipate possible cascading effects, impede the best use and co-ordination of different capabilities across public and private sectors.

Reframing the goals of national resilience and fostering debate about sectoral responsibilities would create a greater unity of purpose. A tripartite vision might focus on 1) reducing broadly defined societal vulnerabilities, 2) maintaining the reliability of critical ecosystems, and 3) securing the UK's long-term strategic imperatives. Against that backdrop and the risk outlook, government and the private sector should explore how far to go – separately and in collaboration – to enhance risk mitigation and crisis preparedness. Maximal resilience may not always be desirable.

Underpinning cross-sectoral interactions with the right 'terms and conditions' is fundamental to securing the best results. More creative, equitable approaches to risk sharing should be nurtured where changing risks severely compromise the commercial business case for investment and action. Regulatory regimes should look harder at systemically important sub-sectors, make resilience a more central tenet of their agenda, expand the use of stress testing, and tighten enforcement. New data-sharing provisions should reduce barriers to sharing (where appropriate) and support decision-making by better integrating open source, public, and private data. Government emergency measures that flex standard procedures should be deployed in ways that enable rather than inhibit private-sector contingency planning.

More generally, ensuring the private sector has a real seat at the table for resilience ideation and implementation would help reduce stovepiping tendencies within government and enhance traction for solutions across the economy.

The new national resilience strategy being prepared by government should stimulate and test new approaches that will position the UK well for the future. Numerous opportunities exist for public and private sectors to interact to greater effect, and much can be learned from initiatives in place already — in the UK and abroad. To take forward the selection identified in this report, government will need to play director, client, stimulator, facilitator, and cheerleader.

In ‘director’ mode, government could review the extent and deployment of existing legislative and regulatory powers. Key areas for examination include mandates for the production and stockpiling of critical goods prior to a crisis, requisition and production directives in a time of crisis, and enhanced powers of intervention to mitigate the potentially systemic impacts of large-scale cyber-attacks.

As ‘client’, government could further influence private-sector behaviour in line with new priorities. Key opportunities relate to adjusting contracting requirements to set resilience expectations of suppliers, creating a new suite of contingent contracts and procurement guidelines that could be drawn on in a crisis, and establishing a technology innovation fund focused on key resilience vulnerabilities.

As a ‘stimulator’ of markets, government could more strongly catalyse or expand novel solutions. Opportunities include cultivating an open research ecosystem where technology, innovation, and data can be combined in a pre-competitive environment; developing a multi-peril insurance scheme for catastrophes; building a cyber-risk pool that

might focus on infrastructure loss events and/or small and medium-sized enterprises; and expanding the deployment of resilience and adaptation bonds.

As a ‘facilitator’ of innovation, government could enhance the integration of data and analytical capabilities. In particular, it could clarify or adapt legal guidance on data sharing to alleviate uncertainties; provide researchers from all sectors with access to a data sandbox and complex analysis platform; ensure the flow of real-time data from diverse sources into the new National Situation Centre; enable the better stress testing of critical national infrastructure assets and supply chains against major contingencies; and encourage relevant private-sector businesses — particularly CNI operators — to participate in cross-sector crisis exercises.

In ‘cheerleading’ mode, government could help promote resilience initiatives developed within the private sector. Measures to be encouraged might include the inclusion of metrics on asset resilience and risk governance in outputs from rating agencies and investment data providers; the creation of industry-based crisis codes of conduct that would help establish expectations as to reasonable behaviour by firms during contingencies; and efforts by companies to enhance the resilience capabilities of their employees.

This report, prepared by Marsh McLennan for the National Preparedness Commission, examines the opportunities for stronger interactions between public and private sectors. Founded on extensive desk research and interviews with resilience experts in the UK and abroad, it offers ideas for further exploration in the context of a much-needed debate.

CONTENTS

Introduction	1
---------------------	----------

Framing the way ahead	3
------------------------------	----------

1. Shortcomings and disconnects	4
2. Sharpening alignment and traction	6
2.1. Reframe the vision and goals	6
2.2. Refresh roles and responsibilities	8
2.3. Revisit terms and conditions	10
2.4. Reinvigorate relationships and protocols	13

Opportunities	14
----------------------	-----------

1. Government directing private-sector priorities	16
2. Government exercising its power as client	18
3. Government stimulating markets	20
4. Government facilitating innovation	23
5. Government cheerleading business initiatives	26

Conclusion	28
-------------------	-----------

Appendix A. Table of opportunities	30
---	-----------

Appendix B. Opportunities in full	31
--	-----------

Endnotes	50
-----------------	-----------

Acknowledgements	54
-------------------------	-----------

INTRODUCTION

This is a pivotal moment for re-energising resilience efforts at the national level. With the severe, concurrent tests of the COVID-19 pandemic and reverberations from the UK's departure from the European Union by no means over, the government's Integrated Review of Security, Defence, Development and Foreign Policy is already pointing us to a kaleidoscope of strategic challenges that policymakers and the country at large will need to navigate in the next decade.¹

In laying out a strategic framework for action, *Global Britain in a Competitive Age* suggests that our collective approach to addressing possible setbacks and catastrophes should emulate the problematic trends and contingencies the nation might face. In other words, if risks and threats are interdependent by nature with transboundary impacts, it's vital that decision-makers and resilience policies are joined up across government departments. If exigencies have complex causes and spill-over effects, we must both explore upstream solutions and expect to manage downstream consequences. If we give credence to the possibility of high-impact risk scenarios, we must prepare, invest, and regulate in good

time and at scale. If we anticipate crises that might speedily change shape, our capabilities will need to be multifaceted and our deployment of them supple. If the issues are cross-border in nature, it's incumbent on us to work closely with allies and partners and, on some issues, with regimes that do not share our values or our goals.

While these conditions demand more ambitious risk assessments and more astute decision-making, they also require the contribution and collaboration of different sectors of society. Most of the possible emergencies on the horizon cannot be solved or mitigated by government alone. Not only is it undesirable for responsibility to be so concentrated, it also represents an opportunity lost. But galvanising and truly mobilising a 'whole-of-society' response (to use a well-worn phrase in national resilience circles) is more easily said than achieved. All too often there is a chasm between assumptions and reality, plans and execution — sometimes due to unforeseen eventualities but more often due to underwhelming levels of alignment and traction.

While acknowledging the need for a holistic view involving all sectors, this report, prepared by Marsh McLennan for the National Preparedness Commission, examines the opportunities for stronger interactions between public and private sectors. Founded on extensive desk research and interviews with resilience experts in the UK and abroad, it offers ideas for further exploration in the context of a much-needed debate, rather than landing on fixed conclusions and firm recommendations.

To be manageable, the project has had to make choices about scope. The paper therefore targets preparedness for and resilience to risks and possible crises that are of national concern due to their intensity, persistence, or likely evolution, rather than more routine problems.² Within that context, it speaks more to civil contingencies than to purely economic or financial disasters or, indeed, to security challenges such as terrorism, the protection of sensitive technologies, or military confrontation. It does not find space to consider industries that need to be nurtured or vital systems, such as healthcare, that are highly stretched. It is conscious of, without being explicit about, a shifting global environment — geopolitical, climate-related, technological — and the transformational national policy agenda that this demands. It looks more closely at central government capabilities and the firms that might provide the most strategic impact than at local government and the broader economy.

Furthermore, it focuses more on general capabilities and interactions that might be leveraged and adapted in a range of circumstances rather than specific strategies for multiple specific challenges — such as improving food security, governing the deployment of advanced technologies, or adapting to individual extreme weather perils. In passing each fork in the road, we have been very aware of alternative conceptual frames and the valuable work to be done down each path not taken.

The report contains two key sections and a large appendix. Section One briefly summarises key systemic shortcomings in public-private interactions experienced in the context of particular crises before exploring four areas that would help achieve greater alignment and traction. Section Two introduces five roles for government in galvanising the private sector in pursuit of national resilience and presents a collection of opportunities or initiatives that would provide lasting value. These ideas are explored in more detail in an Appendix, which, for each opportunity, sets out the context, analogue schemes already in place, and key considerations.

FRAMING THE WAY AHEAD

Recent crises illustrate both the need and the scope for refreshing how public and private sectors can work together for national resilience. More conscious alignment at all levels of the relationship will make for more lasting traction.

1. SHORTCOMINGS AND DISCONNECTS

High levels of national resilience will be essential as government and the nation at large work to:

- Facilitate a smooth economic recovery from the pandemic, transitioning from crisis support to sustainable and equitable growth
- Counter pervasive, persistent, and evolving risks (e.g. sophisticated cyber-attacks) that are hard to control
- Deliver on bold economy-wide transformational agenda (e.g. decarbonisation and digitalisation) that need high levels of mobilisation
- Reset international relations with a view to deeper trade and investment arrangements and the achievement of stronger global influence.

Addressing each one of these imperatives in isolation is hard enough. Foreseeing additional problems where they rub up against each other requires creative vigilance; needing to resolve simultaneous crises diverts effort, slows progress, and reduces public trust.

Exhibit 1 (on the next page) gives a fuller picture of national-level risks and threats. But a brief look at four current crises — each with different dynamics — is perhaps a more tangible means of highlighting areas for resilience improvement.

First, the COVID-19 pandemic has caused colossal damage to households and the economy. The health system has struggled to cope, many businesses have been severely impaired or folded, and economic inequalities have deepened.³ These outcomes raise questions about the UK's preparedness for infectious disease emergencies, the quality

of crisis response decision-making and capabilities, and the allocation of investment for a speedy recovery.⁴

Second, supply challenges of various kinds have come hot on the heels of each other since the beginning of 2020. Collectively and cumulatively, the effects of COVID-19, the UK's departure from the European Union, the blocking of the Suez Canal by a container ship, the reduced availability across the world of ships and aircraft, the gas price crisis, and fuel shortages continue to reverberate through the economy in multiple ways.⁵ These contingencies raise questions about the quality of regulatory preparedness and scrutiny, the shortcomings of business supply-chain models, and the effort given to contingency planning (especially regarding the continuity of critical functions).

Third, cyber-risk has become yet more pervasive and expensive. Ransomware attacks have surged, internet-based economic crime has soared, foreign state-related incursions continue to be persistent and complex, and mis/disinformation campaigns continue.⁶ Mindful of the prospect of a more catastrophic cyber event, these trends raise questions about the strength of the UK's cybersecurity ecosystem, the level of organisational attention to cyber-risk and workforce training, and the extent of insurance-based protection.

Fourth, climate-related challenges are intensifying with time windows for response shortening. Extreme weather events take place with increasing regularity, long-term changes are eroding the reliability of physical defences and the continued availability of natural resources, and decarbonising the economy has a long way to go.⁷ These developments raise questions about the protection of communities exposed to such disasters, the level and speed of investment in long-term adaptation measures, and the strength of policy and industrial measures to secure changes in all sectors that ensures the UK meet net-zero commitments in an orderly manner.⁸

Exhibit 1: A taxonomy of national-level risks and threats

	Acute/fast-onset	Chronic/steady-state/cyclical	Slow-burn escalation
Malicious human action	<ul style="list-style-type: none"> Invasion: territorial integrity compromise, missile strike Large cyber-attack: e.g. theft disruption, data loss Terrorist attack: e.g. vehicles, weapons, explosives, CBRN (chemical, biological radiological, nuclear materials) Uprising/coup 	<ul style="list-style-type: none"> Espionage/loss of state secrets Endemic corruption Illicit trade/money laundering Gross manipulation of markets or public funds Hybrid threats: propaganda disinformation ventures election hacking Radicalism, extremism sectarianism 	<ul style="list-style-type: none"> Unchecked weapons of mass destruction agenda Unchecked offensive cyber actions War: conventional or irregular asymmetric conflict
Human induced/accident	<ul style="list-style-type: none"> Major industrial accident: e.g. food/water contamination, toxic spill, transport disaster Critical infrastructure failure – e.g. energy, water, communications transport, financial services 	<ul style="list-style-type: none"> Banking system collapse Fiscal crisis Trade conflict/sanctions Public protests and disorder/industrial action National fragmentation/secession Pollution: air, water, land Antimicrobial resistance Public health challenges: e.g. obesity 	<ul style="list-style-type: none"> Loss of national competitive positioning: technology, market competition, asset ownership, skills Poorly managed transformations: low carbon economy, industrial change, political system, automation Unexpected technological consequences: artificial intelligence, gene editing Welfare/health system collapse Natural resource depletion: e.g. soil, forests, fisheries Uncontrollable migration
Natural hazard	<ul style="list-style-type: none"> Extreme weather: e.g. flood, snow, windstorm, freeze, wildfire, heat Nature catastrophe: e.g. tsunami, earthquake, volcano, space weather 	<ul style="list-style-type: none"> Extreme weather: e.g. drought Disease outbreak/pandemic: human, animal, plant 	<ul style="list-style-type: none"> Climate change: e.g. sea-level rise Food system/security failures Demographic time bombs

Source: Marsh McLennan Advantage. (2020, April). [Building national resilience](#).

2. SHARPENING ALIGNMENT AND TRACTION

To strengthen interactions between public and private sectors it is valuable to explore challenges and opportunities in four areas: vision and goals, roles and responsibilities, terms and conditions, and relationships and protocols.

2.1. Reframe the vision and goals

Without a broad cross-sectoral appreciation of the need, attempts to strengthen national resilience may founder. After all, in times of

‘peace’ the cost of resilience is keenly felt — by both government and companies alike — while the value is all too often hidden. Resilience should be reframed not just as countering a negative (risk) but as an ambition that is accretive to prosperity and wellbeing for both individual organisations and the UK as a whole. Better preparedness for exogenous surprises makes for lower performance volatility, shallower damage from shock events, and greater government policy stability. All in all, a better environment in which to plan and invest, where public- and private-sector leaders can deploy capital more safely to the missions that will deliver the strongest social and economic returns.

Framing the national endeavour in terms of three distinct goals (see Exhibit 2) helps signal both obligations and opportunities for public- and private-sector actors and thus how they might interact.

Exhibit 2: Goals for national resilience



01

Reducing broadly defined societal vulnerabilities



02

Maintaining the reliability of critical ecosystems



03

Securing the UK’s long-term strategic imperatives

- Reducing broadly defined societal vulnerabilities means lessening the impact of potential disasters on communities across the UK and spurring faster, more equitable recovery from them. This is achieved by enhancing the preparedness of individuals, communities, and businesses for both sudden-onset crises and also slow-burn, but inexorable, situational transformations. (Climate change and cyber threats might fit under both categories.) Principally, it requires timely investment (centralised and decentralised) in ‘structural’ resilience, a risk culture that is watchful and supportive, and an ability (physical, organisational, or financial) to absorb shock events when they occur.
- Maintaining the reliability of critical ecosystems means ensuring the continuity of critical functions, flows, and services on which economic flows and societal wellbeing are dependent, with a particular emphasis on the economic infrastructure (such as energy, transportation, telecommunication, and banks) and the societal infrastructure (such as hospitals, schools, and government operations) that underpin them. Some of these assets and systems require large-scale investment to future-proof them against erosion and collapse (in the near or long term); many are high-profile targets of malicious attacks, not least for the cascading challenges that might ensue. Among other things, this agenda requires a deeper understanding of dependencies both within and between infrastructure systems, including the supply chains that serve them, along with continual operational upgrades and long-term resilience programmes.
- Securing the UK’s long-term strategic imperatives means developing the platforms, especially in emerging or fast-evolving fields, that can

help the UK and its citizens enjoy freedom, security, and prosperity in the decades ahead and enable its businesses to be competitive both at home and abroad. This is achieved through nurturing innovations in key technologies and their application, building new markets, and driving through sectoral transformations in a determined manner. Not only does this require vision and pump-priming investment in line with clear goals, it also requires consistent commitment and regulatory foresight to forestall negative outcomes and encourage desirable forms of collaboration.

Pursuit of these goals surfaces perennial strategic challenges where public-private interactions need to align with greater unity of purpose. First, how to balance the needs of different time horizons. While existing infrastructure and related ecosystems may need immediate remedial action, delayed investment in longer-term transformations often results in more volatile performance, greater project complexity, truncated timescales, and higher costs for future generations. Second, how to balance effort across different phases of the resilience life cycle. Much is made of the difficulty of anticipating situational specifics, but even agile crisis response mechanisms and aggressive recovery programmes are likely to be inadequate if pre-emptive mitigation opportunities have been spurned. Third, how to balance different agenda. Addressing most risks of national concern presents unavoidable strategic conflicts between economic growth, societal wellbeing, environmental protection, and national security imperatives. And, fourth, how to balance individual freedoms and collective resilience in the context of a liberal and market democracy, especially at a time of significant societal polarisation. Trust — in both government and the private sector — is critical for lasting impact.

2.2. Refresh roles and responsibilities

Pursuit of the goals presented above opens an array of questions about the roles and responsibilities of government and the private sector, and how they inform both separate and collective action.

Conscious of the risk landscape, where should government step up its commitments based on its unique positioning? Mindful of market failures, where does it need to play a bolder role to mandate and regulate, nurture and facilitate the activities of others? And where, wary of growing contingent liabilities and the encouragement of moral hazard, ought it to back away and simply let market forces suffice? It goes without saying that government interactions with the private sector for resilience ends are not purely framed by regulatory obligation and the use of fiat powers in an emergency. A far more extensive range of collaborative endeavour includes investment stimuli, bailouts, joint research and development agenda, suasion, and celebration that leverage the self-interest and goodwill of the market.

Through a risk lens, the case for greater government intervention lies in those areas where momentum across the country on resilience to priority risks is insufficient (e.g. climate change); it is also valid where

catastrophe is in the offing (e.g. pandemic). Through a national resilience lens, intervention is called for where there may be a mismatch between the financial or operational risk appetite of individual organisations that have systemic influence on the risk landscape and the tolerances of the broader economy that depends on them (e.g. utility supply outages); it is also valid where market behaviours skew actions that are either unfair to some parties (e.g. smaller companies) or result in other risks being avoidably exacerbated via cascading effects. More fully analysing existing resilience arrangements against these criteria may shed light on blind spots and opportunities.

Questions can also be asked of the private sector about where corporate responsibilities for resilience begin and end — acknowledging the very different capabilities of FTSE 100 titans and small enterprises. While many firms would do well to better anticipate extreme scenarios and more thoroughly bake resilience into their commercial endeavours and core operations, how far ought they to go in analysing their dependencies and then taking steps to influence supply chains, their workforce, and their customers? Indeed, to what extent should larger companies take on a more overt role in supporting systemic or societal resilience, and how can smaller, nimbler firms better contribute specific expertise?

Beyond regulatory obligation and the use of fiat powers, government interactions with the private sector should make better use of stimulation, suasion, facilitation, and celebration that leverage the self-interest and goodwill of the market

Recent years have seen corporate interest in these questions grow in three ways.

First, greater global uncertainty had already elevated board and executive team scrutiny of macro-level forces that could destabilise operations and strategic positioning; nonetheless, the pandemic spurred much fresh examination as to what constitutes organisational resilience and how that can best be achieved both within a crisis and in advance.⁹ Moreover, the COVID-19 experience has prompted firms to take a fresh look at risks in seldom-examined parts of their risk registers, explore more extreme risk scenarios, and recognise the likely need to grapple with concurrent crises.

Second, many companies have become more sensitive to their societal commitments. The pandemic amplified workforce wellbeing programmes, which increasingly recognised that employee resilience doesn't stop at the office foyer or the factory gate. At the same time, companies large and small deepened their engagement with local communities and others in their ecosystem.¹⁰ This reflects pre-pandemic momentum within many corporations to embrace a responsible capitalism mentality —

foregrounding a commitment to all stakeholders, blending profit and purpose for sustainable growth.¹¹ Indeed, customers, employees, and investors are holding companies to an ever higher bar not only regarding their ESG (environmental, social, and governance) ambitions but also to their actual performance in pursuing them.¹²

Third, an increasing number of companies are seeking a more active role in addressing large-scale public policy challenges that affect their business but can't be resolved by government alone.¹³ There is steady evidence of growing non-competitive alignment and cooperation between companies and with government (national and local) on cross-cutting challenges such as cyber-risk, climate change, artificial intelligence, diversity and inclusion, and the circular economy.¹⁴ Such collaboration on societal issues is endorsed by nearly four-fifths of the public, according to one poll, with three-fifths holding the view that business leaders should step in and take the lead when government has not found the right way ahead.¹⁵ A similar proportion of those in the workforce professes to choose their employer based on that employer's values and beliefs, and elects to leave or avoid organisations that have an incompatible stance on social issues or that fail to address moral imperatives.¹⁶

2.3. Revisit terms and conditions

Without the right small print, engagement with laudable goals and well-aligned responsibilities will likely wither over time. Three sticking points in particular would benefit from fresh thinking: who bears the risk and cost, standards and regulation, and data sharing (see Exhibit 3).

Risk and cost allocation. Government understandably wants to lever in private capital and shed risk from its balance sheet to manage the overall burden on the public purse. While accepting that commercial returns are seldom risk free, the private sector understandably wants to be compensated for risks it is asked to assume that go beyond those that are justified by a commercial business case. Examples of such compensation include co-investment (infrastructure), offtake agreements (power producers), liability backstops (insurance sector), and indemnity agreements (COVID-19 vaccine manufacturers due to limited testing and emergency authorisation procedures). Normal accommodations on these issues can reach a breaking point when the risks get manifestly larger, government seeks to pass on more risk due to stretched fiscal positions, and the private sector has alternative opportunities for deploying capital.

More transparent, analysis-led discussions about risk between public and private sectors could lead more easily to equitable, creative solutions at a time of significant situational change and where the costs of inaction could leave the nation more exposed to physical and economic disaster.¹⁷ Not only should these address the pricing of risk — and not just with respect to the insurance sector — they should also explore the range of fiscal and market solutions (including reserve funds, stabilisation funds, risk pools, catastrophe bonds, corporate levies, and borrowing) that might mitigate fallout in the event of crisis.¹⁸

Regulation. Few would dispute the need for directive frameworks (legislation, regulation, standards); the question is more whether they are sufficiently responsive to evolving circumstances and succeed in driving the right outcomes. Indeed, contrary to the precautionary principle that governs much scientific and medical agenda, in many other areas legislation for resilience (broadly defined) can be belated and backward-looking rather than well-attuned to future risks, market contexts, and solutions. Hard as it can sometimes be, greater efforts might be deployed to anticipate possible risk and sectoral developments to future-proof legislation more effectively.

Exhibit 3: Resilience levers meriting revision



Risk and cost allocation



Regulation



Data and intelligence sharing

Noting that the powers of oversight bodies differ significantly between sectors, regulation can struggle in three ways. First, a focus on holding individual asset owners accountable can make it hard to take a truly systemic view, especially when there are key interfaces and dependencies beyond the assets being regulated and where the whole system itself (e.g. energy, banking, and digital) is evolving apace. Second, it is hard to balance competing priorities at the same time (e.g. housing needs vs. construction on flood plains, expansion of capabilities and services vs. unwelcome side effects in the digital realm, consumer prices vs. long-term infrastructure functionality in the water sector, international competitiveness vs. national system stability in the financial sector). And third, enforcement is not always easy given difficulties in reliably assessing or verifying institutional performance with limited resources and also where penalties offer limited deterrence relative to the gains that might be achieved.

By way of developing arrangements that are more fit for purpose, several developments could be pursued.

It would be useful to review whether there are systemically important sub-sectors and firms that ought to experience greater oversight. These might include ‘hidden’ assets, such as parts of digital or technological ecosystems that are growing in importance or leading firms in niche industries whose operations supply other sectors. Alternatively, it might include growing segments of certain sectors (e.g. shadow banking or utility supply services) where the plausible near-simultaneous failure of several providers would have far-reaching consequences. The burden of expanded oversight might be mitigated by tiering expectations according to the size of the business, as in the banking sector. Indeed, while some regulatory

provisions need to be the same for all, it’s important to ensure that regimes enable small and medium-sized enterprises (SMEs), not just large firms, to thrive. Recently proposed new powers for the Competition and Markets Authority ought to help in this regard.¹⁹

There is merit in making resilience a more central tenet of regulatory regimes for which it currently seems an ancillary interest. Where the chief goal, as for many utility regulators, is to protect the pockets of present-day consumers based on an expectation of operational resilience, it can be hard to develop and implement cost-effective investment plans that anticipate both near- and long-term contingencies. Against this backdrop, it would be useful to expand stress testing of different types (strategic, financial, operational) across different critical infrastructure sectors as a matter of routine. Moreover, stronger cross-sector regulatory hubs — such as the UK Regulators Network and the Digital Regulation Cooperation Forum — could sharpen debate and help reconcile differing agenda of bodies with separate statutory powers.²⁰ Indeed, it has been frequently observed in the last few years that sectoral, industrial and corporate evolution has blurred many traditional boundaries, presenting problems for regulators with dated, siloed authorities.²¹

Finally, there may be opportunities to be more imaginative in the deployment of regulation. By way of example, perhaps incentives and sanctions could be more effectively combined in one regime. Widening the differential between stronger and weaker resilience performance might sharpen engagement and reduce attempts at free riding. Additionally, there is often scope to make better use of suasion on strategic issues where further industry leadership is needed — for example, through industry-initiated standards or pressure on systemically-important firms.²²

Data and intelligence sharing. Commercial confidentiality and national security sensitivities are often cited in the context of interaction or cooperation failures between public and private sectors. While intellectual property, commercial data, personal data, and a significant amount of government intelligence unquestionably need to be protected and not shared for a variety of reasons, significant scope exists for better data sharing under the right circumstances.²³ Where this works well it can be a powerful tool. Government's greater openness regarding threats from Russia (viz. regular cyber-attack attributions) has helped sharpen the nation's awareness about the disruptive agenda of foreign powers. In a very different way, the Financial Sector Cyber Collaboration Centre (FSCCC), in partnership with the National Cyber Security Centre (NCSC), usefully aggregates and shares information on incidents from across the sector to assist attack responses.²⁴

Nonetheless, data is all too often subject to institutional protective instincts and structural (regulatory or policy-driven) barriers. While sometimes government and companies have come together well (e.g. to address food supply concerns during the first COVID-19 lockdown), at other times intelligence and perspectives on impending challenges have not been fully shared or put to best use in good time. Data sharing with and between critical industry operators can be patchy and, where it is not fully

comparable, it can be hard to obtain an industry-wide or cross-sectoral view on resilience. Appreciating their data-based contribution to the COVID-19 response and other agenda, there is undoubtedly more that the big technology firms can do to help mitigate mis/disinformation, internet harms, cyber-attacks, and criminal activity.²⁵ For its part, government's predisposition to classify documents and intelligence that might have widespread value has been frequently questioned.²⁶

Among opportunities for change, government could take greater advantage of the growing grey zone between open source, public, and private data, and build that into its analytics; it could also explore new approaches for real-time data sharing that can support decision-making. Honing conventions (such as temporary suspensions of the Competition Act) that enable private-sector companies to contribute data to collaborative endeavours that would benefit their own resilience as well as that of others would also be desirable.²⁷ Following the example of Australia regarding cyber-attacks, government might also seek powers to compel critical infrastructure operators to hand over data in the event of a clear breach of resilience.²⁸ In addition, sharing risk scenarios that are not sensitive on national security grounds would be a helpful and credible starting point for companies that have limited risk resources but which would like to examine their ability to cope with different contingencies.

Government could seek to harness the grey zone between open, public, and private data, explore new approaches for real-time data sharing, endorse greater private-sector data collaboration, and compel post-breach data disclosures

2.4. Reinvigorate relationships and protocols

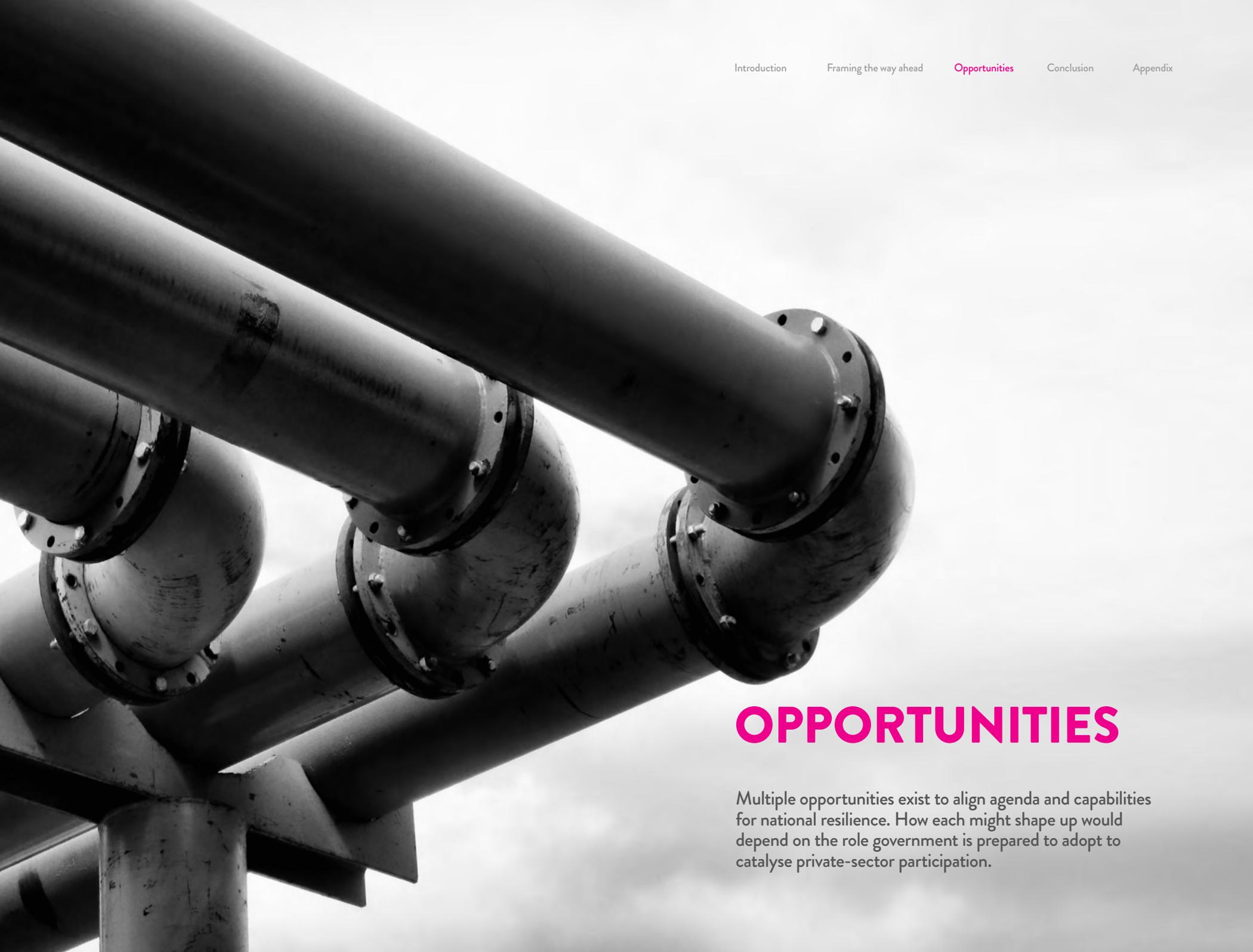
To adapt an old adage: Frameworks are good, but behaviours prevail. If the pursuit of national resilience is a ‘whole-of-society’ effort with many independently moving parts, how public and private sectors engage with each other — within and outside formal initiatives — will greatly influence outcomes.

Respecting national security considerations, the private sector could participate more deeply in strategic national-level risk and resilience discussions — not only with respect to single-sector or single-issue analyses with narrowly defined purposes (many of which happen already) but also in more broad-based forums in which experts and practitioners from different sectors might contribute to and challenge government thinking on cross-cutting agenda on a regular basis.²⁹ Done well, not only would this enhance situational awareness and possibly under-appreciated spill-over effects, it might also counter stovepiping tendencies within government and lead to greater innovation and broader traction with emerging solutions.³⁰

Moreover, a collaborative approach to addressing strategic problems and implementing solutions is often most productive — even where fiat is the most appropriate mode of government intervention. Where the private sector lacks a real seat at the table, suboptimal outcomes can result: compliance alone is rarely the true goal and inertia can make generally good initiatives fail.

Stronger, more dynamic interactions between public and private sectors in a crisis are also vital. At times of heightened concern, it is entirely sensible that government should adapt priorities, policies, and operating practices: the ability to tighten or ease regulations in an emergency can mitigate escalating problems or act as a shock absorber. By way of example, the first 15 months of the pandemic saw major encumbrances on operations and working practices in all sectors. At the same time, other impositions were eased: various categories of enterprise were offered business rates relief, government procurement protocols were relaxed, and barriers to collaborative action between firms in certain competitive environments were eased.³¹

Under such circumstances (and each new crisis brings its own exigencies), rigidity is undoubtedly an enemy of resilience. At the same time, consistent signalling and communication from government builds trust and enables business to take (often bold) decisions on contingency plans with reasonable confidence in their appropriateness. While complex, fast-moving situations mean that government policy may well evolve, clearly stated priorities and decision thresholds enable companies to get a head start in anticipating future policy scenarios and the implications for their business.³² Moreover, the application of flexibility needs to be ethical and transparent, justified not only by the perceived benefits but also by a view on the possible unintended consequences, and governed by clear procedures for reverting to ‘peacetime’ practices in due course.



OPPORTUNITIES

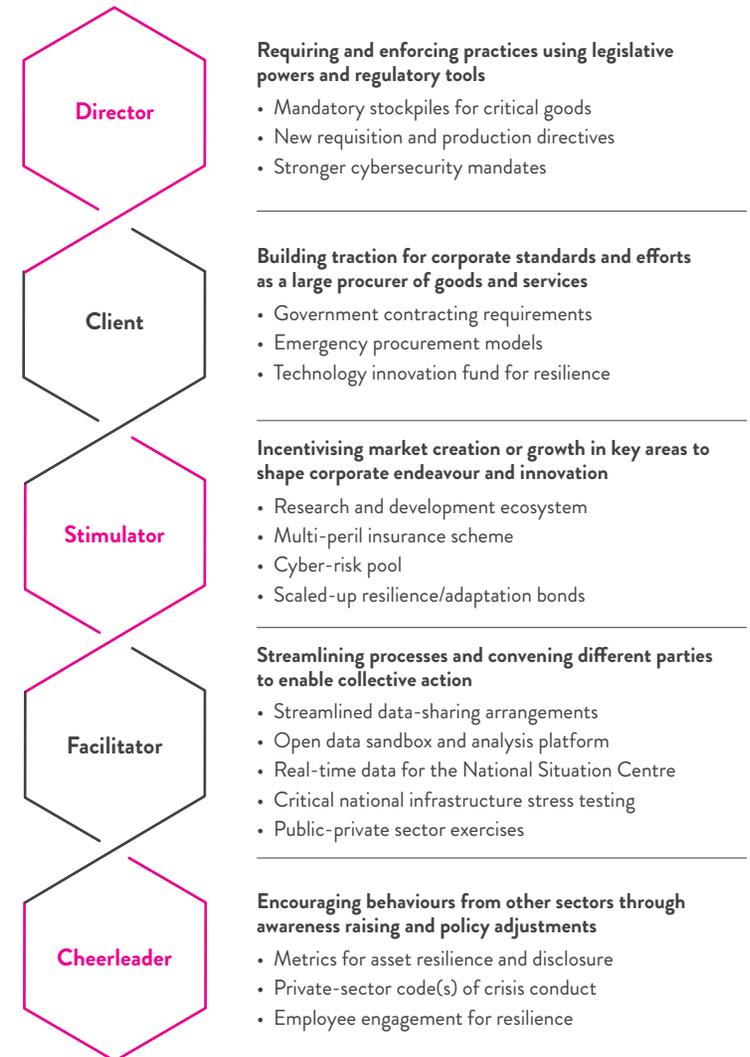
Multiple opportunities exist to align agenda and capabilities for national resilience. How each might shape up would depend on the role government is prepared to adopt to catalyse private-sector participation.

This final section sets out a collection of possible initiatives that emerge from the thinking in the previous section. They are not recommendations, merely food for thought. The organising principle is the role that government might play (see Exhibit 4), from being highly directive at one end of the spectrum to hands-off encouragement at the other. Some ideas could also fit in a different category, if alternative levers were chosen.

Most of the opportunities presented are not peril-specific; they concern themselves more with the enhancement of fungible capabilities that can help responsible parties anticipate and respond to different risks and crises. Their genesis lies in wondering how private-sector resources — finance, physical assets, workforce, capabilities, and innovation — might be leveraged or nurtured for national resilience either in combination with government capabilities or in combination with each other in a setting that needs to be made available by government. In each case, efforts have been made to articulate what drives the need, how initiatives benefit both national resilience and private-sector participants, and, where applicable, how implementation would expand or reorient existing endeavours in the same or adjacent spaces.

This chapter just presents the essence and value of each opportunity. An appendix sets out — for each — further details on context and rationale; analogue interventions in the UK and abroad; and key considerations that would need to be addressed in further exploration. Another appendix comprises a table that schematises the suite of opportunities and how they interconnect.

Exhibit 4: Opportunities and the role of government



Source: Marsh McLennan Advantage

1. GOVERNMENT DIRECTING PRIVATE-SECTOR PRIORITIES

Opportunities exist to implement or deploy more robust arrangements where deficiencies in critical outcomes are most manifest. Expanded government powers would be valuable where enforcement is challenging, flexibility is required to navigate uncertainty, or direct intervention is necessary in times of crisis.



1.1. Mandatory stockpiles for critical goods

Government could explore the provisions within existing powers, or pass new legislation, to mandate private-sector producers or users of critical goods to maintain a level of excess production and/or storage capacity or demonstrate an ability to expand operations at short notice. In so doing, it could retain the authority to audit compliance in peacetime as well as tap on these capacities during crises.

Mandates for excess capacity in the private sector would help alleviate fiscal and logistical burdens in times of crisis. Market forces would help ensure that products with limited lifespans are expended before their expiry date. For private-sector providers, being compelled to build out production and storage capacities, particularly where they might have previously lacked an immediate incentive to do so, would result in greater long-term resilience to supply-chain disruptions as they become more able to ramp production up or down seamlessly and as necessary.

For further details on context, analogues, and considerations, [click here](#)





1.2. New requisition and production directives for emergencies

Where existing powers fall short, government could seek new authorities, separate to the Civil Contingencies Act (CCA), that granted it authority during less extreme crises to direct private companies to prioritise government orders; allocate materials, services, and facilities to response efforts; and restrict hoarding of goods. These directives would be more widely applicable while also being weaker than the CCA, given that some CCA powers may be excessive in circumstances that are less severe than those for which the CCA was originally conceived.

Noting that trade-off, it may work to develop a set of directives applicable to different types of crisis. The measures would be framed such that the government could more freely invoke them where the CCA may not be viable; they could also contain authorisation for companies to coordinate production and supply with each other without violating antitrust laws.

Such powers would reduce the government's reliance on ad hoc market-based incentives to spur private companies to act in the interest of the public good during crises, thereby strengthening the production of critical goods in times of need. Provisions to protect private firms from antitrust scrutiny during crises would also reduce the risk borne by companies that support response and recovery efforts through greater coordination with competitors.

For further details on context, analogues, and considerations, [click here](#)



1.3. Cybersecurity mandates on system-wide vulnerabilities

Government could seek powers that give it a wider scope of authority in three areas. First, it might compel owners and operators of systemically important critical national infrastructure (CNI) to undertake specific government-prescribed cybersecurity directives, with the NCSC or the Centre for the Protection of National Infrastructure (CPNI) perhaps acting as a key conduit. Second, it might provide a mandate to intervene and assist directly during or after a significant cyber-attack on such businesses. Third, it might mandate that such businesses conduct regular due diligence on the cyber resilience of their supply chains.

While current intervention powers are reserved for extreme cases or emergency use, additional authorities would achieve several objectives. They would expand government's sphere of influence in implementing cybersecurity mandates, enhance the depth of its reach, and be permanently in force. These changes would centralise nationwide cybersecurity governance, affording the government greater oversight over areas of critical national importance in anticipation of more challenging scenarios.

Moreover, mandatory cybersecurity measures would enhance societal resilience by strengthening the cyber resilience of CNI and their supply chains. The private sector would in turn benefit from reduced risk of potential disruptions caused by cyber-attacks, increased customer confidence, and reduced cyber-insurance premiums.

For further details on context, analogues, and considerations, [click here](#)

2. GOVERNMENT EXERCISING ITS POWER AS CLIENT

Taking advantage of its status as the nation's largest procurer of goods and services, government could either build traction for, or outright require, enhanced corporate resilience efforts. This would influence private-sector behaviour without the need for legislative or regulatory instruments that might be regarded as overreaching.



2.1. Government contracting requirements

Government could require corporate commitments as part of major outsourcing contracts. These commitments might encompass both internal resilience objectives as well as external engagements. The former could include palpable capacity-building programmes to strengthen business continuity, contracts with cybersecurity experts for emergency support, asset hardening programmes, regular vulnerability assessments, formal risk management protocols. More precise features or investments could also be mandated, such as cyber-insurance coverage or systematic oversight of supply-chain vulnerabilities and risks. The latter, meanwhile, could involve providing demonstrable financial or human capital support to local community organisations for wellness and preparedness efforts, collaboration across community networks, and support for vulnerable populations.

Incentivising such actions through public procurement allows government to shape private-sector behaviour at minimal public cost. By making such commitments a prerequisite for bidding, the government could ensure that more companies — not just the successful respondent — actively and continually improve both their internal resilience efforts as well as their contribution to the community at large. Enhanced resilience efforts would not only improve private contractors' business stability in the long run, but also enhance their reputation with other stakeholders.

For further details on context, analogues, and considerations, [click here](#)



2.2. Response and recovery procurement models

The government could create a suite of new emergency procurement models that relate to different crises or forms of desired private sector support. This would require the identification of likely key goods and services during response and recovery phases as well as potential vulnerabilities in supplier networks that could come under pressure during a crisis.

Specific models would likely require a mix of contingent contracts and crisis-specific procurement guidelines such as assessment criteria (supplier timeliness and resilience, business continuity arrangements, and other non-financial key performance indicators [KPIs]), and contract transparency. Such models would enhance public trust in contingency planning arrangements when normal levels of due diligence have to be suspended. Pre-signalling such opportunities would help likely private-sector providers hone their adaptive capacities to respond to suddenly changing needs and opportunities. Periodic testing in scenario-based tabletop exercises would help check their validity.

For further details on context, analogues, and considerations, [click here](#)



2.3. Technology innovation fund

The government could establish a technology innovation challenge fund that would galvanise the engagement and collaboration of stakeholders from different sectors. Areas of focus might be specific disruptions within the National Security Risk Assessment (NSRA), the cascading effects of sudden-onset events or slow-burn risks, or strategic or tactical response opportunities. Such a fund could form an element of a mission-based approach to national resilience wherein the government provides top-down guidance and funding but does not directly influence project ideation or design, thereby enabling an organic proliferation of bottom-up solutions.

This would not only advance technological approaches to resilience to a new level but might also yield solutions that could be shared with partner countries across the world. Additionally, the fund could help further the government's ambition for the UK to become a 'science superpower' and generate approaches with dual-use applications. Private firms would gain access to funding that might otherwise be difficult to secure, in addition to a unique platform that facilitates collaboration, engagement, and sharing. Beyond their participation in the challenge, such resources might enable further internally led research and development efforts that in turn generate new business opportunities or even cycle back to boost national resilience.

For further details on context, analogues, and considerations, [click here](#)



3. GOVERNMENT STIMULATING MARKETS

Where market forces principally dictate the speed and scope of innovation, economic or financial incentives may accelerate the crowding in of needed levels of capital and expertise. In some instances, government can adapt existing arrangements for national resilience ends; elsewhere, it might backstop possible losses that the market could not endure.



3.1. Research and development ecosystem

The government could cultivate an open and thriving research ecosystem where technology, innovation, and data can be combined in a pre-competitive environment to uncover win-win solutions for national resilience. Such an ecosystem would bolster the UK's scientific and technological research efforts and could look to support both innovations solely for use within the national resilience ecosystem and also dual-use technologies.

Such efforts could culminate in cutting-edge solutions to resilience challenges such as the smart manufacturing of critical goods (PPE, medicines, etc.), analysing and modelling infrastructure challenges, early-warning systems that leverage evolving satellite technology, and surveillance and analytical capabilities that can detect emerging domestic and cross-border health threats. The innovation efforts of individual businesses would also benefit from an active and open network wherein data sharing and collaboration are both incentivised and facilitated.

For further details on context, analogues, and considerations, [click here](#).



3.2. Multi-peril insurance scheme for catastrophes

The government and insurance industry could develop a new scheme that embraces various complex perils, with a focus on extreme eventualities. The product might seek to incorporate a parametric approach (where appropriate), which would designate clear event triggers yet also incentivise – through lower premiums or faster access to funds – risk-mitigation efforts made by policyholders. This would deliver the twin benefits of speedy payouts (which would mitigate broader economic damage) and the gradual enhancement of organisational, and thus national, resilience over time.

Combining catastrophic risks that are uncorrelated and have different impact profiles could make for significant diversification benefits that would expand insurance capacity and coverage beyond what might be available via individual insurer offerings or separate pools. It might also be more efficient institutionally, especially regarding back-office activities.

Strategically, a broad scope would also address the frequent criticism of complex interventions – that they only address the last crisis and not the next. A single product that focuses on catastrophic events from various sources might be more appealing to customers concerned about extreme incidents than a suite of separate tail risk products with separate costs (see Exhibit 5).

An insurance solution might have several advantages over direct government financing, particularly where government support mechanisms need to be established hastily in a crisis. It could provide ex-ante transparency and certainty on the level of benefits that would be provided and leverage the existing claims payment infrastructure. It could attract private capital from insurance, reinsurance, and capital markets, which might absorb some of the losses even in cases where most of the risk is borne by government. Nonetheless, effective implementation would lower the burden on the public purse by reducing losses and facilitating faster economic recovery.

For further details on context, analogues, and considerations, [click here](#).

Exhibit 5: Public-private insurance/reinsurance models

Private		Public
←		→
<p>Semi-private pooling reinsurance scheme</p> <p>Joint entity created by insurers to pool risk and share knowledge</p> <p>Participation may be voluntary or legally mandated</p> <p>Financing primarily provided by the private sector, with limited (if any) initial government financing and typically no committed reserve</p>	<p>Public-private partnership (PPP) reinsurance schemes</p> <p>Structured risk-sharing model between policyholders, insurers, and government</p> <p>Government explicitly provides backing to the private sector to cap exposure and drive affordability</p> <p>Participation may be voluntary or legally mandated</p>	<p>Public funds for noninsurable risks</p> <p>Pure government setup, without any direct private involvement (other than aligning coverage)</p> <p>Fund is created with a reserve, built up over time, that can be used to pay out claims in the event of a pandemic</p> <p>Claims against the fund should be aimed at covering risk events that cannot be covered by existing insurance offerings</p>

Source: Marsh



3.3. Cyber-risk pool

To keep pricing affordable, enhance coverage, and generally improve cyber resilience, government and the insurance industry could develop a levy and pool system to support cyber-insurance accessibility for UK businesses. Such a scheme would require appropriate backstops, modelled on other government-backed reinsurance schemes.

Two potential areas of focus stand out. First, providing coverage for ‘infrastructure loss’ events or catastrophic damage to key digital infrastructure networks that result in widespread impacts. Second, supporting access to coverage for SMEs by assisting with affordability and enhancing the specialist support that already plays a role for insured businesses before, during, and after an incident.

A ‘Cyber Re’ could help raise baseline cybersecurity practices of UK organisations as well as alleviate payouts in crises if it included provisions that required good organisational cyber-risk management. Government could also encourage insurers to adopt minimum security standards in risk assessments through, for example, Cyber Essentials accreditations. The government might also wish to mandate a certain level of cyber coverage for responses to public-sector tenders, similar to existing requirements on public and private liability coverage. Government could also consider passing supporting legislation that contained provisions on mandatory data and threat information sharing.

For further details on context, analogues, and considerations, [click here](#)



3.4. Scaled-up resilience/adaptation bonds

Government could expand the scale and scope of the resilience and adaptation bonds it already issues and actively encourage private-sector beneficiaries to participate (a resilience bond is a fixed income instrument issued to raise low-cost private capital for projects that enhance national resilience and generate investment returns). This would facilitate government-initiated cost-sharing with the private sector on ‘hard’ measures such as sea defences, levees, and infrastructure toughening as well as ‘soft’ measures such as catchment restoration and forestry management initiatives. Government could also support the design process of bond-backed developments by providing project financing expertise from HM Treasury and grants for modelling as well as creating facilitation guidelines and best practice documentation.

At a time of increasing institutional investor interest in opportunities with strong ESG profiles, offerings in this area would present new investment opportunities with a distinct risk-return profile. Distributed ledger technology could support the traceability of projects and their impacts, and also reduce transaction costs. In the long run, expanding this form of bond issuance would accelerate progress in sustainable development within the UK.

For further details on context, analogues, and considerations, [click here](#)

4. GOVERNMENT FACILITATING INNOVATION

Often the right conditions are critical for liberating private-sector capabilities, especially where collaboration is required. Against this backdrop, government can act as a convening power, help reduce barriers to engagement, enable unexpected solutions to emerge, and provide a frame that ensures value both for private-sector participants and national resilience.



4.1. Streamlined data-sharing arrangements

The government could clarify or adapt legal guidance on data sharing, including any safe harbour arrangements in a crisis, to alleviate uncertainty and encourage participation. This could be complemented by standard templates for data access agreements, collaboratively developed with business, that would help reduce cost and confusion further, especially for smaller firms. These foundations could be enhanced by more forward-thinking data-sharing strategies, universal metadata standards, the development of portals or data lakes, and the design of appropriate security provisions for sensitive data.

By enabling greater access to diverse datasets before and during a crisis, the government could leverage the speed and innovation of the private sector in response and recovery as well as attain more accurate situational awareness in fast-moving or complex crises. Improved guidance and clearer standards would reduce costs and operational inefficiencies for private firms seeking to build out their data-driven capabilities.

For further details on context, analogues, and considerations, [click here](#)



4.2. Open data sandbox and complex analysis platform

Possibly as part of National Digital Research Infrastructure plans, the government could provide researchers, civil society, and the private sector with access to diverse, high-fidelity, interconnected, longitudinal data and state-of-the-art analytical tools through a data sandbox platform. This would facilitate the integration and interrogation of different public and private data sources, including (with appropriate privacy safeguards) de-identified data — such as income, demographics, and health statistics — that come from different government departments. Especially where the opportunity arises to support projects for the public good, the government could also grant public access to large computational resources within the sandbox that are designed for artificial intelligence or machine-learning applications to enable advanced analytics that would otherwise be too expensive for SMEs and researchers.

A powerful platform with appropriate safeguards could funnel more diverse, high-quality data into a centralised repository, thereby equipping government bodies as well as other stakeholders across society to better tackle national resilience challenges and conduct more comprehensive vulnerability assessments and research into effective crisis response strategies. It could, moreover, facilitate the combination or comparison of distinct datasets to derive cross-cutting, interdisciplinary insights that may serve as a bedrock of innovation — as with recent efforts linking mobility and health data to assess the effectiveness of COVID-19 lockdown measures. Access to the sandbox's databases and resources would also help fast-track data-driven insights on vulnerabilities and resilience strategies from private firms to supporting resilience efforts such as modelling the pandemic. This sort of work could also serve other national priorities (e.g. economic security, climate mitigation) and enhance the standing of UK science.

For further details on context, analogues, and considerations, [click here](#)



4.3. Real-time data integration into the National Situation Centre

The government could ensure that the recently announced National Situation Centre (NSC) is equipped to integrate data from a range of sources. These might include ever-growing real-time data from smart meters and the Internet of Things on mobility patterns, public sentiment streams, environmental factors (such as water height, wind speed, temperature), stockpile levels and the movement of key goods, and response capabilities.

Leveraging private-sector data would provide the NSC with a more holistic and dynamic dashboard representation of the risk landscape, response capabilities, and societal capacities that might better anticipate cascading impacts in times of crisis. By collecting, cleaning, and integrating such datasets over time, trend analysis could also support the development of early-warning signals for emerging threats and help resource allocation in preparation for and during events.

Such a capability would also be foundational for exploring different planning scenarios that would better ensure the continuity of societal functions. Moreover, improvements to data availability, matching, and standardisation would support national risk assessment work by compiling a national data taxonomy to help identify data gaps that might be filled by further research. Such efforts would also allow for the provision of intelligence to the private sector, especially critical infrastructure sectors such as health, transport, and food, generating enhanced insights into emerging supply-chain risks and demand surges.

For further details on context, analogues, and considerations, [click here](#)



4.4. Critical national infrastructure interdependency stress testing

Government could facilitate sector-wide and cross-sector stress testing of CNI assets and their supply chains against major contingencies. Regulators would need to coordinate efforts and design scenarios that tested the collective strength of the UK's critical networks against extreme and compound threats. Periodic stress testing would allow CNI owners and operators to understand what and how much is at risk, including from external dependencies, as well as examine how to enhance preparedness and resilience through targeted measures for critical network elements. A government-led forum could facilitate dialogue to share learnings in a non-competitive setting.

Such complex stress testing would involve the development of CNI simulation modelling capabilities by integrating public and private data on networks, dependencies, supply chains, and failure thresholds in a centralised national repository to be used by operators for vulnerability assessments. These capabilities would enable threat scenarios to be analysed, losses and damages to be estimated, and mitigation actions to be designed and tested. A centralised approach to modelling and stress testing would enable enhancements over time to benefit operators.

For further details on context, analogues, and considerations, [click here](#)



4.5. Public-private sector exercises across the crisis cycle

Public agencies could more actively invite relevant private-sector businesses, particularly those operating critical infrastructures and systems, to participate in joint crisis exercises for preparedness, response, and recovery. In certain instances, there may be a case for mandating involvement. These exercises might focus on validating emergency plans, developing staff capabilities, testing procurement procedures, and other critical activities. To enable this, private-sector involvement would need to be explicitly included in relevant doctrines such as the Resilience Capabilities Programme and associated guidance on emergency planning and preparedness.

The inclusion of actors from different sectors (discussion-based or tabletop exercises being less burdensome) would provide more opportunities for public-private interaction and mutual learning. Not only would this likely reveal unanticipated vulnerabilities and operational snags, it would also strengthen relationships and trust, enhance an understanding of different capabilities and working styles, and develop muscle memory that can be accessed in the future. Companies participating in these exercises would gain a better understanding of their own exposure to crises and business continuity weaknesses.

For further details on context, analogues, and considerations, [click here](#)

5. GOVERNMENT CHEERLEADING BUSINESS INITIATIVES

Where there is alignment on the core goals, many initiatives are likely to arise from the private sector. Under such circumstances, government may wish just to provide input or guidance, encourage expansion, or otherwise promote more widely.

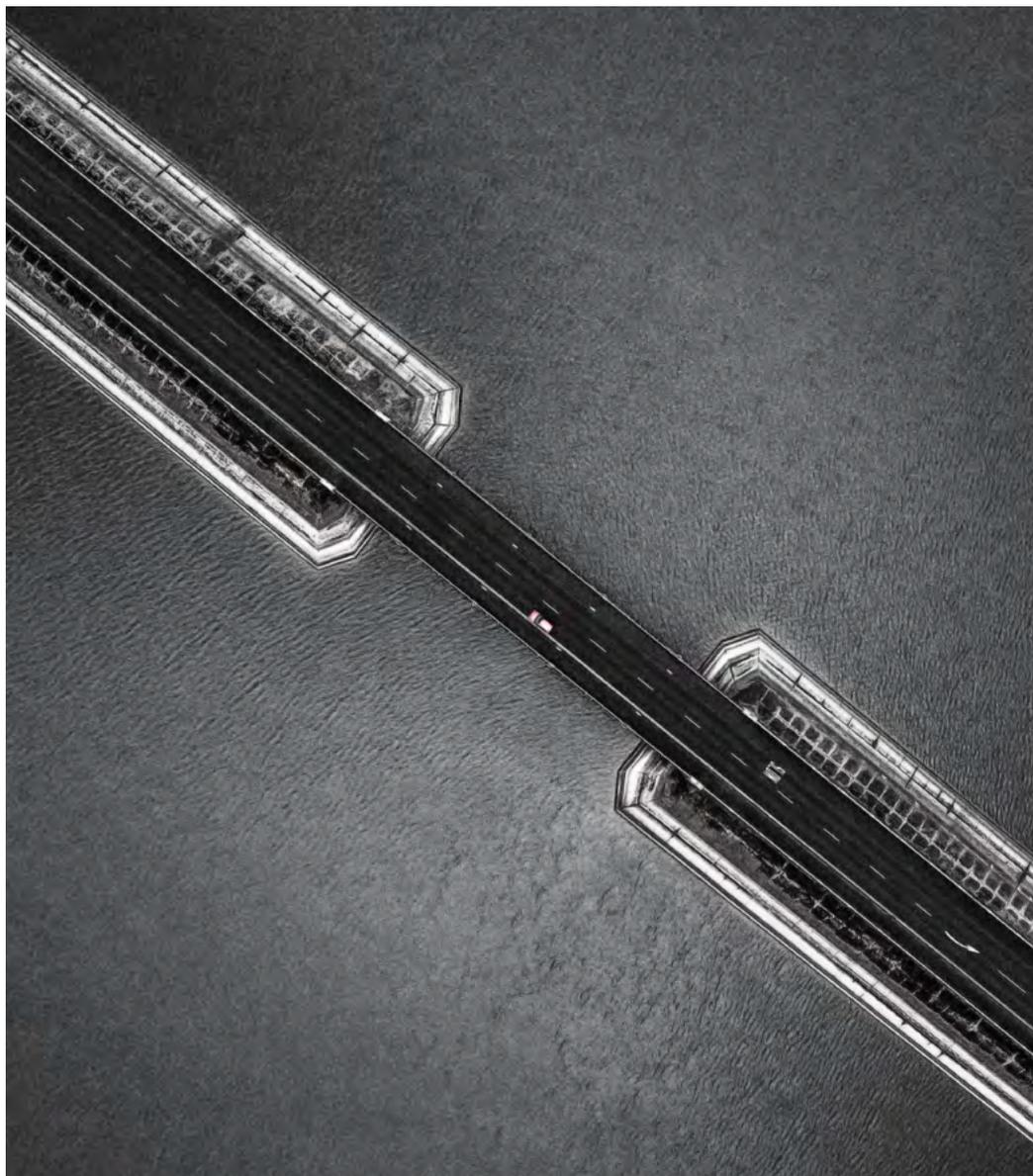


5.1. Metrics for asset resilience and disclosure

To incentivise timely asset upgrading and maintenance, government could advocate for the inclusion of metrics on asset resilience and risk governance – including design standards, maintenance records, and risk-engineering reports – in outputs from rating agencies and investment data providers. Additionally, government could also lead by example and publish such metrics on its own assets to encourage more widespread adoption and ultimately induce a paradigm shift towards a convention of asset resilience reporting and disclosure.

More granular metrics and improved reporting would help long-term investors direct capital towards assets that are better managed for resilience, thereby raising questions for owners and operators of less resilient assets. As rating agencies adopted such metrics, the underlying data could also inform the cost and design of loans, which would yield cost savings for private firms and hence create financial incentives for better asset management in the long run. Such metrics could also be used as the key trackable KPIs required for ongoing access to sustainable and transition-linked finance. The net outcome would be greater trust in the reliability of critical societal functions.

For further details on context, analogues, and considerations, [click here](#)





5.2. Private-sector code(s) of crisis conduct

Government could encourage industries to develop crisis codes of conduct that would help establish and clarify expectations as to reasonable behaviour by private firms during contingencies that trigger a State of Emergency declaration or during other extraordinary circumstances. Any such code should include ‘best-practice’ provisions — developed by those industries with government input — on critical issues including data sharing, pricing, intellectual property rights, treatment of employees and suppliers, and capacity management. For example, a code of conduct for biopharmaceutical companies might include guidelines on licensing and supply agreements for essential drugs during a pandemic.

Successful implementation of any private-sector crisis code of conduct, particularly for firms providing critical services, would bolster societal resilience as private firms would be better placed to more seamlessly and efficiently allocate resources and capabilities during crises. This would accelerate private-sector responses under emergency circumstances, resulting, for example, in shorter procurement timelines. A formal code that helped clarify expected behaviours and was widely adopted would empower individual firms to cooperate without fear of being disadvantaged relative to their peers.

For further details on context, analogues, and considerations, [click here](#)



5.3. Employee engagement for resilience

Government could encourage companies, especially large employers, to enhance the disposition and capabilities of their workforces. A multi-pronged strategy might blend the inclusion of a resilience dimension into health and benefits offerings, educational opportunities on risk mindfulness, employer-based training for actions to be undertaken in the event of specific contingencies, and support for local resilience-related community and charitable organisations — such as through offering employees paid leave to undertake community-based volunteering activities.

Expanding these efforts would benefit employees as individuals in major life choice decisions, contribute to a stronger corporate risk culture, and deepen employee loyalty. More broadly, it would help foster a ‘whole-of-society’ culture-oriented approach to national resilience that would reduce the need for government intervention.

For further details on context, analogues, and considerations, [click here](#)



CONCLUSION

Sustained supply-chain challenges, extreme weather events, large-scale cyber-attacks, energy crises of different kinds, and an evolving COVID-19 virus all argue strongly for national-level preparedness and resilience to be strengthened and made more supple. Indeed, despite widespread hunger up and down the country to return to normality after the constraints of the past couple of years, it is evident not only that the pandemic is still with us but that new crises have already surfaced and further challenges and contingencies lie just over the horizon.

Against that backdrop, a new national resilience strategy — which asks hard questions of the country's performance, targets the future, contains bold ideas, and embraces the participation of all sectors — is much needed. Deep-seated tensions need to be acknowledged and worked through, some of which set the demands imposed by a more challenging risk environment against our values as a liberal and market democracy. Nonetheless, the opportunities for stronger public-private engagement, based on true partnering for shared goals, are numerous and huge. But, as should be apparent from this report, framing interactions and collaborations in the right way will be crucial for achieving a lasting enhancement of capabilities and effort.



APPENDIX

	Government role	Opportunity	Resilience goals	Crisis phase	Private sector – Contribution					Related opportunities
1.1	Director	Mandatory stockpiles for critical goods	Maintaining the reliability of critical ecosystems	• Pre-emptive	●	●	●		●	5.1; 5.2
1.2		New requisition and production directives for emergencies		• Incident response • Recovery	●		●			2.2; 4.3
1.3		Cybersecurity mandates on system-wide vulnerabilities	Reducing broadly defined societal vulnerabilities	• Pre-emptive		●			●	3.3; 5.1
2.1	Client	Government contracting requirements	Reducing broadly defined societal vulnerabilities	• Pre-emptive	●		●		●	3.3; 5.1; 5.2
2.2		Response and recovery procurement models	Maintaining the reliability of critical ecosystems	• Incident response • Recovery	●		●			1.2; 4.5
2.3		Technology innovation fund	Securing the UK's long-term strategic imperatives	• Pre-emptive		●	●	●		3.1; 3.4; 4.2
3.1	Stimulator	Research and development ecosystem	Securing the UK's long-term strategic imperatives	• Pre-emptive		●	●	●		2.3; 3.4
3.2		Multi-peril insurance scheme for catastrophes	Reducing broadly defined societal vulnerabilities						●	3.3
3.3		Cyber-risk pool							●	1.3; 3.2
3.4		Scaled-up resilience/adaptation bonds				●	●	●		
4.1	Facilitator	Streamlined data-sharing arrangements	Maintaining the reliability of critical ecosystems	• Pre-emptive • Incident response • Recovery			●			4.2; 4.3; 5.2
4.2		Open data sandbox and complex analysis platform	Reducing broadly defined societal vulnerabilities			●	●	●		4.1; 4.3
4.3		Real-time data integration into the National Situation Centre	Maintaining the reliability of critical ecosystems	• Incident response • Recovery			●			4.1; 4.2
4.4		Critical national infrastructure interdependency stress testing		• Pre-emptive	●	●	●			4.2; 5.1
4.5		Public-private sector exercises across the crisis cycle		• Pre-emptive • Incident response • Recovery	●	●	●		●	2.2; 4.1; 4.2; 5.2
5.1	Cheerleader	Metrics for asset resilience and disclosure	Maintaining the reliability of critical ecosystems	• Pre-emptive			●			1.1; 4.4
5.2		Private-sector code(s) of crisis conduct		• Incident response • Recovery	●	●	●		●	1.1; 2.1; 2.2; 4.1; 4.5
5.3		Employee engagement for resilience	Reducing broadly defined societal vulnerabilities	• Pre-emptive		●	●		●	N.A.

Physical assets
Human resource
Capabilities
Innovation
Finance

Source: Marsh McLennan Advantage

1. GOVERNMENT DIRECTING PRIVATE-SECTOR PRIORITIES

1.1. Mandatory stockpiles for critical goods

Context: The burden of stockpiling critical goods against future crises currently falls most heavily on public-sector entities, which may not hold usable supplies for all emergencies. The private sector's 'just-in-time' manufacturing and supply processes, resulting from a pursuit of efficiency, mean that companies often struggle to meet surge demand following the onset of a crisis. Together, these arrangements can lead to rapid exhaustion of inventories and damaging delays in restocking.

In the early days of the COVID-19 pandemic, national stockpile shortcomings and procurement strategy weaknesses contributed to shortages of personal protective equipment (PPE), human-resource constraints, and large amounts of stock that no longer met current safety standards. The pandemic stockpile at the time was geared towards an influenza outbreak and not a novel virus like COVID-19; moreover, government faced questions about being slow to engage industry in ramping up domestic production of PPE.³³

Idea and value: Government could explore the provisions within existing powers, or pass new legislation, to mandate

private-sector producers or users of critical goods to maintain a level of excess production and/or storage capacity or demonstrate an ability to expand operations at short notice. In so doing, it could retain the authority to audit compliance in peacetime as well as tap on these capacities during crises.

Mandates for excess capacity in the private sector would help alleviate fiscal and logistical burdens in times of crisis. Market forces would help ensure that products with limited lifespans are expended before their expiry date. For private-sector providers, being compelled to build out production and storage capacities, particularly where they might have previously lacked an immediate incentive to do so, would result in greater long-term resilience to supply-chain disruptions as they become more able to ramp production up or down seamlessly and as necessary.

Existing analogue(s): The UK requires major businesses producing, supplying, or using petroleum products to ensure minimum stock levels at all times.³⁴ In the electricity sector, the Capacity Market ensures security of electricity supply by providing a payment for reliable sources of capacity.³⁵ Other countries have successfully responded to COVID-19 on the back of stockpile mandates. Finland's National Emergency Supply Agency (NESA) drew on its policy of mandating certain suppliers to maintain stockpiles of indispensable goods such as grain and medical supplies, while simultaneously storing

some of those suppliers' stock in its own warehouses. In 'peacetime', suppliers can sell the goods stored in NESA warehouses and exchange older models for new stock.³⁶

Key considerations: The NSRA and subsequent planning assumptions, based on inputs from different sectors, would be foundational in specifying what supplies might be needed, the standards required, how much of each item should be stockpiled, and the length of notice at which they would need to be delivered. Not all goods may need to be stockpiled if firms can prove that they can ramp up production (especially of items with a short shelf life) at short notice. Even for these, it would be vital to understand the short notice availability of raw materials alongside other potential bottlenecks, including skillsets and storage and transportation capacities. It would also be important to monitor and audit the possibly large number of new, decentralised stockpiles and production facilities, and also the impending expiry dates of goods — where relevant.

Moreover, given the net benefit to the public purse, it would be important to explore whether or where government should incentivise companies to hold more critical goods inventory than they otherwise would, as doing so would have working capital and cash flow impacts as well as storage costs.

 [To return to summary of opportunities, click here](#)

1.2. New requisition and production directives for emergencies

Context: Although private sector companies have access to a wide range of assets and capabilities that would significantly strengthen national crisis response and recovery efforts, they may not feel incentivised to meet surge demand during crises and, depending on the circumstances, may deem it more advantageous to hoard supplies. The Civil Contingencies Act (CCA) contains provisions that theoretically enable government to address these issues, although short review windows and a ‘triple-lock guarantee’ limit its invocation to a subset of phenomena in accordance with a narrow definition of ‘emergency’.³⁷

Consequently, the CCA was not activated during the COVID-19 crisis — arguably the greatest challenge the nation has faced since World War II. In the years since coming into force, commentators have noted the government’s disinclination to invoke the CCA due to its perceived limitations.³⁸ There is hence a need for new, distinct directives that supplement the CCA by permitting emergency powers in response to a wider range of threats, albeit without encouraging government overreach.

Idea and value: Where existing powers fall short, government could seek new authorities, separate to the Civil Contingencies Act (CCA), that granted it authority

during less extreme crises to direct private companies to prioritise government orders; allocate materials, services, and facilities to response efforts; and restrict hoarding of goods. These directives would be more widely applicable while also being weaker than the CCA, given that some CCA powers may be excessive in circumstances that are less severe than those for which the CCA was originally conceived.

Noting that trade-off, it may work to develop a set of directives applicable to different types of crisis. The measures would be framed such that the government could more freely invoke them where the CCA may not be viable; they could also contain authorisation for companies to coordinate production and supply with each other without violating antitrust laws.

Such powers would reduce the government’s reliance on ad hoc market-based incentives to spur private companies to act in the interest of the public good during crises, thereby strengthening the production of critical goods in times of need. Provisions to protect private firms from antitrust scrutiny during crises would also reduce the risk borne by companies that support response and recovery efforts through greater coordination with competitors.

Existing analogue(s): Provisions already exist in the CCA for requisitioning assets and directing private-sector production — new directives would simply lower the

thresholds for activation. The US Defense Production Act, which can be enacted through an Executive Order, contains activation mechanisms and conditions that are far more lenient than those of the CCA.³⁹ Crucially, the Defense Production Act empowers the federal government to direct private-sector suppliers even during peacetime to support causes including emergency preparedness activities, the protection or restoration of infrastructure, and efforts to mitigate terrorist threats.

Key considerations: These powers might still only be used as a last resort where pre-existing contingency contracts are not already in place (see Opportunity 2.2). Directives might usefully include powers as well as formal guidance for stronger and swifter emergency procurement measures. It would be important to frame and message the provisions with care to ensure trust among the private sector and the general public. To that end, key safeguards should be built into the legislation to prevent misuse.

 [To return to summary of opportunities, click here](#)

1.3. Cybersecurity mandates on system-wide vulnerabilities

Context: Intensifying geopolitical rivalries and growing dependencies on digital networks are precipitating damaging cyber-attacks sponsored by malicious government actors, proxy hacking groups, and criminal enterprises. Private operators of critical national infrastructure (CNI), including those with strong cybersecurity programmes, are likely to find it increasingly difficult to defend against and recover from these threats by themselves. In extreme cases, the government has the power to intervene in the interests of national security if CNI cyber-risks are not adequately managed, but it otherwise only wields powers of inspection and serves information, enforcement, and penalty notices.⁴⁰ The UK General Data Protection Regulation regime also does not extend much beyond requiring firms to disclose the scope and severity of any data breaches suffered.⁴¹

Ransomware has become a rapidly escalating and pervasive challenge.⁴² Reported cases rose by more than 400 percent last year, while cyber-insurance payouts now top 70 percent of all property and casualty premiums collected.⁴³ Such attacks can have destabilising impacts on society, particularly when targeted at vulnerable points in the supply chain. By way of example, in July 2021, a Russia-linked attack on more than 20 global managed service providers (MSPs) allowed hackers to infiltrate the MSPs' customers as well — ultimately affecting more than 1,000 businesses in more than 17 countries.⁴⁴

Idea and value: Government could seek powers that give it a wider scope of authority in three areas. First, it might compel owners and operators of systemically important critical national infrastructure (CNI) to undertake specific government-prescribed cybersecurity directives, with the NCSC or the Centre for the Protection of National Infrastructure (CPNI) perhaps acting as a key conduit. Second, it might provide a mandate to intervene and assist directly during or after a significant cyber-attack on such businesses. Third, it might mandate that such businesses conduct regular due diligence on the cyber resilience of their supply chains.

While current intervention powers are reserved for extreme cases or emergency use, additional authorities would achieve several objectives. They would expand government's sphere of influence in implementing cybersecurity mandates, enhance the depth of its reach, and be permanently in force. These changes would centralise nationwide cybersecurity governance, affording the government greater oversight over areas of critical national importance in anticipation of more challenging scenarios.

Moreover, mandatory cybersecurity measures would enhance societal resilience by strengthening the cyber resilience of CNI and their supply chains. The private sector would in turn benefit from reduced risk of potential disruptions caused by cyber-attacks, increased customer confidence, and reduced cyber-insurance premiums.

Existing analogue(s): Upcoming legislative reforms in Australia include government-prescribed cybersecurity directives, such as mandatory vulnerability assessments and regular reporting of system information, as well as enhanced powers for direct intervention.⁴⁵ In the US, the recent Executive Order on Improving the Nation's Cybersecurity includes measures to enhance software supply-chain security and establish a Cyber Safety Review Board composed of representatives from both the private and public sectors.⁴⁶

Key considerations: It might be necessary to broaden the list of infrastructure, services, and other assets rated as systemically important to the nation and its society, economy, and security — to include facilities such as data storage and processing. Thought should be given to how regulators might accurately assess private sector performance of its mandates, balancing the challenge of numerous individual business audits and compliance checks with the likely lower reliability of self-reporting mechanisms. It would also be vital for the government to continually enhance its own cyber capabilities alongside its expanded powers so that it could provide meaningful assistance or intervene more effectively as attack vectors and crises change over time.

 [To return to summary of opportunities, click here](#)

2. GOVERNMENT EXERCISING ITS POWER AS CLIENT

2.1. Government contracting requirements

Context: Given that over £290 billion is spent on public procurement annually, more could be done to harness the government's considerable purchasing power as a key consumer of private-sector goods and services.⁴⁷ Government could leverage its influence as a large client to steer firms towards enhancing their own risk management and resiliency efforts and also benefitting the communities in which they operate.

Idea and value: Government could require corporate commitments as part of major outsourcing contracts. These commitments might encompass both internal resilience objectives as well as external engagements. The former could include palpable capacity-building programmes to strengthen business continuity, contracts with cybersecurity experts for emergency support, asset hardening programmes, regular vulnerability assessments, formal risk management protocols. More precise features or investments could also be mandated, such as cyber-insurance coverage or systematic oversight of supply-chain vulnerabilities and risks. The latter, meanwhile, could involve providing demonstrable financial or human capital support to local community organisations for wellness and preparedness efforts, collaboration across community networks, and support for vulnerable populations.

Incentivising such actions through public procurement allows government to shape private-sector behaviour at minimal public cost. By making such commitments a prerequisite for bidding, the government could ensure that more companies – not just the successful respondent – actively and continually improve both their internal resilience efforts as well as their contribution to the community at large. Enhanced resilience efforts would not only improve private contractors' business stability in the long run, but also enhance their reputation with other stakeholders.

Existing analogue(s): Government has recently introduced procurement requirements for net-zero targets and pathways for large contracts (valued at more than £5 million) as well as longstanding contracting provisions on energy efficiency, equality, and quality management, among other obligations.

Key considerations: Government would need to frame expectations in a way so that those evaluating tenders could be sure that claims were meaningful. It would also be critical to avoid overburdening small and medium-sized enterprises, and thus consolidating contract opportunities among large, established players. A tiered approach may be appropriate, with enhanced expectations in place for larger contracts.

 [To return to summary of opportunities, click here](#)

2.2. Response and recovery procurement models

Context: Normal procurement processes, designed to ensure fair competition and value for money, often operate too slowly in crises that require governments to procure goods and services at short notice to save lives and limit physical damage. This can also be the case as attention turns to crisis recovery, when speedy procurement is essential for restoring vital infrastructure and economic activity.

However, the abandonment of due process can undermine trust and affect quality. By way of example, the COVID-19 crisis exposed deficiencies in the national stockpile of supplies such as PPE and raised problems in the rapid procurement of ventilators, tracing software, and more, leading to over £127 billion in expenditure.⁴⁸ Emergency processes that involved accelerated review timelines, the modification of existing contracts, and direct contract awards showed a lack of transparency regarding supplier selection, raised questions about bias and conflicts of interest, and yielded mixed outcomes by way of results.⁴⁹

Idea and value: The government could create a suite of new emergency procurement models that relate to different crises or forms of desired private-sector support. This would require the identification of likely key goods and services during response and recovery phases as well as potential vulnerabilities in supplier networks that could come under pressure during a crisis.

Specific models would likely require a mix of contingent contracts and crisis-specific procurement guidelines such as assessment criteria (supplier timeliness and resilience, business continuity arrangements, and other non-financial key performance indicators [KPIs]), and contract transparency. Such models would enhance public trust in contingency planning arrangements when normal levels of due diligence have to be suspended. Pre-signalling such opportunities would help likely private-sector providers hone their adaptive capacities to respond to suddenly changing needs and opportunities. Periodic testing in scenario-based tabletop exercises would help check their validity.

Existing analogue(s): The repeated experience of natural disasters in the US has led the Federal Emergency Management Agency (FEMA) to refine and augment its system of advanced contracts for the rapid delivery of supplies and services in a crisis.⁵⁰ At a sub-national level, FEMA encourages and supports similar strategies. More innovatively, following the 2011 Christchurch earthquake, New Zealand authorities developed a model for reconstruction contracting that sought to combine principles of both competition and collaboration.⁵¹ The Stronger Christchurch Infrastructure Rebuild Team Model initially allocated equal work between five delivery teams, but subsequently used accomplishment against both cost and non-cost performance metrics to determine the further division of opportunities across the five-year construction effort as it unfolded.

Key considerations: A core suite of procurement models would likely vary by threat type (e.g. cyber vs. human health threat), stage of crisis (response vs. recovery), or type of support (goods or services) being requested. A key starting point would be the National Resilience Planning Assumptions. Developing such models in collaboration with industry ought to yield solutions that are more workable, efficient, and replicable. It would also be necessary to work out the burden of evidence for participating companies and to monitor how their capabilities may have changed over time. At the same time, it would be important to mitigate bias against large 'incumbent' firms to ensure opportunities for smaller players, taking care to avoid unnecessary inefficiencies and complexities.

Government might also consider how procurement models could be adapted to secure engagement from organisations less familiar and/or resourced to fully respond to procurement requirements. For example, with regard to seeking insurance market capital and (re)insurance capacity, the administrative hurdles involved in current public procurement requirements might deter some organisations from participation; this would limit choice and possibly value for money. One suggestion would be to create an overarching qualification for (re)insurance that applied to all government-related procurement, thereby limiting the repetitive administrative burden for the organisations involved.

 [To return to summary of opportunities, click here](#)

2.3. Technology innovation fund

Context: Over the past decade, government has steadily upgraded its approaches to risk assessment and resilience planning. While this has often been thoughtful, both exercises have struggled to analyse with any great depth how complex risks intersect; the inevitability of interdependent, cascading consequences; and the merits of different response options.

Advances in, and the convergent deployment of, different technologies present fresh opportunities for sourcing and working with newly available data and analysing it at speed. This can provide new understandings of risk impacts, better early-warning intelligence, and more robust business cases for resilience solutions.⁵²

Idea and value: The government could establish a technology innovation challenge fund that would galvanise the engagement and collaboration of stakeholders from different sectors. Areas of focus might be specific disruptions within the National Security Risk Assessment (NSRA), the cascading effects of sudden-onset events or slow-burn risks, or strategic or tactical response opportunities. Such a fund could form an element of a mission-based approach to national resilience wherein the government provides top-down guidance and funding but does not directly influence project ideation or design, thereby enabling an organic proliferation of bottom-up solutions.

This would not only advance technological approaches to resilience to a new level but might also yield solutions that could be shared with partner countries across the world. Additionally, the fund could help further the government's ambition for the UK to become a 'science superpower' and generate approaches with dual-use applications. Private firms would gain access to funding that might otherwise be difficult to secure, in addition to a unique platform that facilitates collaboration, engagement, and sharing. Beyond their participation in the challenge, such resources might enable further internally led research and development efforts that in turn generate new business opportunities or even cycle back to boost national resilience.

Existing analogue(s): The Defense Advanced Research Projects Agency (DARPA) in the US has for decades accelerated the development of cutting-edge, ground-breaking technologies even beyond immediate military requirements — not least the internet. On a smaller scale, the UK's National Security Strategic Investment Fund aims to accelerate the adoption of national security and defence capabilities as well as develop the UK's dual-use technology ecosystem.⁵³ The UK's forthcoming Advanced Research and Innovation Agency (ARIA) will be independent

of government, researcher led, and focus on high-risk projects with transformative potential to push scientific boundaries.⁵⁴

The European Union (EU)'s Horizon 2020 programme distinguishes between broader Sustainable Development Goal-based challenges and more granular 'missions' with clear objectives that prompt concrete projects proposing a range of solutions.⁵⁵ Additionally, other more niche innovation funds and networks in the UK have been successful in the past, with several government grant funds directly precipitating hydrogen technologies, advanced materials, and advances in AI and data analytics, among other target areas.⁵⁶ Recently, Ofgem and Innovate UK have launched a Strategic Innovation Fund to accelerate the decarbonisation of energy networks, while the government is holding an open competition to explore the feasibility of running fibre optic cables through water pipes.⁵⁷

Key considerations: The government's role in operating such a fund should be one of risk-tolerant, problem-driven market shaping — galvanising the private and third sectors to explore novel ideas — as opposed to risk-averse market

fixing targeted at specific sectors.⁵⁸ As such, to attract the best innovators, the fund would need to balance a clear sense of focus with an openness to complex, unconsidered approaches to the end goal of national resilience. Solutions should not only be scalable but also show how they are open to enhancement over time. It would be vital for project consortiums to involve experts from different fields and end users with emergency management and resilience mandates.

Regarding the private sector, the opportunity should actively seek the involvement of SMEs as well as larger players. Project funding would need to be commensurate with the scale of the opportunity, and the approach to intellectual property rights would need to be conducive to participation; existing intellectual property models like DEFCON 705 might have to evolve substantively.⁵⁹ One possible means of incentivising participation would involve engagement opportunities with relevant government agencies and access to powerful data and computational resources (see Opportunity 4.2).

 [To return to summary of opportunities, click here](#)

3. GOVERNMENT STIMULATING MARKETS

3.1. Research and development ecosystem

Context: Solutions that tackle the ‘wicked’ nature of new, accelerating, and intersecting threats require non-competitive environments where sectors can come together, share best practices and data, identify common barriers, and act collaboratively. However, creating healthy research and development ecosystems can be challenging due to commercial sensitivities, an absence of incentives, and difficulties in creating an equitable distribution of risk and costs.

Without active participation from the private sector, much innovation that might support national resilience may not be possible. By way of backdrop, in 2019, the level of research and development (R&D) investment in the UK (1.74 percent of GDP) trailed peers such as Germany (3.2 percent) and the US (3.1 percent).⁶⁰

Idea and value: The government could cultivate an open and thriving research ecosystem where technology, innovation, and data can be combined in a pre-competitive environment to uncover win-win solutions for national resilience. Such an ecosystem would bolster the UK’s scientific and technological research efforts and could look to support both innovations solely for use within the national resilience ecosystem and also dual-use technologies.

Such efforts could culminate in cutting-edge solutions to resilience challenges such as the smart manufacturing of critical goods (PPE, medicines, etc.), analysing and modelling infrastructure challenges, early-warning systems that leverage evolving satellite technology, and surveillance and analytical capabilities that can detect emerging domestic and cross-border health threats.⁶¹ The innovation efforts of individual businesses would also benefit from an active and open network wherein data sharing and collaboration are both incentivised and facilitated.

Existing analogue(s): Many different models exist that might be a home for this effort. The Industrial Strategy Challenge Fund (ISCF), managed by UK Research & Innovation, addresses the big societal challenges being faced by UK businesses today.⁶² The UK’s recently announced Centre for Greening Finance & Investment and Australia’s Cooperative Research Centre programme provide long-term funding for industry-led research collaborations to improve the competitiveness, productivity, and sustainability of industries; increase R&D capacity in SMEs; and enhance industry take-up of academic research. The Cyber Central development in Cheltenham, near the Government Communications Headquarters, promises to be an innovation-focused business park for cyber companies large and small.⁶³ The UK Collaboratorium for Research on Infrastructure and Cities is an integrated research capability that engages government, industry, academia, and end users on systems-based solutions for the renewal, sustainment, and improvement of infrastructure and cities.⁶⁴

The Trinity Challenge has united leaders from business, academia, and civil society with the goal of strengthening health systems and improving preparedness for health emergencies.⁶⁵ Spurred by the Yozma programme of the 1990s, Israel has a well-developed innovation system that brings together venture capital and applied research and technology development for commercial and state security objectives.⁶⁶

Key considerations: Government would need to take the lead in cultivating and overseeing such an ecosystem. As with the technology innovation fund discussed above, different models may be needed for different initiatives to encourage cross-sectoral participation. Regulatory sandboxes may be valuable, with certain rules lifted to develop and test innovations; public procurement may provide a ready market for new products and services.

Approaches to intellectual property rights would need to be specified, especially as innovations with commercial value may result. And information-sharing requirements and the demarcation of spheres of influence for different types of actors may be necessary: for instance, the ecosystem would likely limit the access of private firms to personally identifiable information of individual citizens.

 [To return to summary of opportunities, click here](#)

3.2. Multi-peril insurance scheme for catastrophes

Context: Organisations of all kinds face the prospect of catastrophic events from a range of unconnected perils, including large health incidents, extreme weather, cyber-attacks, and terrorism. While sudden physical damage to assets presents obvious losses, non-damage challenges (such as business interruption, event cancellation, and trade credit problems) can equally threaten business operations and survival, with consequent impacts for economic activity and employment.⁶⁷

The appetite of insurers or capital markets to provide financial protection against catastrophic risks is strongly influenced by their ability to model those risks, price them, and limit their exposure. Insurance pools — which involve the participation of multiple insurers in a market and are sometimes underpinned by a government backstop — are a way of increasing the viability of coverage where there might otherwise be a reluctance to engage. Most address single perils; some have a broader scope.

Idea and value: The government and insurance industry could develop a new scheme that embraces various complex perils, with a focus on extreme eventualities. The product might seek to incorporate a parametric approach (where appropriate), which would designate clear event triggers

yet also incentivise — through lower premiums or faster access to funds — risk-mitigation efforts by policyholders. This would deliver the twin benefits of speedy payouts (which would mitigate broader economic damage) and the gradual enhancement of organisational, and thus national, resilience over time.⁶⁸

Combining catastrophic risks that are uncorrelated and have different impact profiles could make for significant diversification benefits that would expand insurance capacity and coverage beyond what might be available via individual insurer offerings or separate pools. It might also be more efficient institutionally, especially regarding back-office activities.

Strategically, a broad scope would also address the frequent criticism of complex interventions — that they only address the last crisis and not the next. A single product that focuses on catastrophic events from various sources might be more appealing to customers concerned about extreme incidents than a suite of separate tail risk products with separate costs (see Exhibit 5).

An insurance solution might have several advantages over direct government financing, particularly where government support mechanisms need to be established hastily in a crisis. It could provide ex-ante transparency and certainty on the level of benefits that would be provided

and leverage the existing claims payment infrastructure. It could attract private capital from insurance, reinsurance, and capital markets, which might absorb some of the losses even in cases where most of the risk is borne by government. Nonetheless, effective implementation would lower the burden on the public purse by reducing losses and facilitating faster economic recovery.

Existing analogue(s): Government and the insurance industry can draw on significant prior experience with single-peril schemes such as Pool Re and Flood Re, and more recent developments such as the Trade Credit and Live Events schemes — each of which has different design characteristics.

Similar government-backed initiatives for catastrophic risks exist globally, including France's natural disasters compensation scheme and the US Terrorism Risk Insurance Program.⁶⁹ Multi-peril natural catastrophe mechanisms in the Caribbean (CCRIF) and South East Asia (SEADRIF) are backed by the World Bank and enhance diversification through pooling multiple nations together.⁷⁰

Other market-based solutions to insuring against pandemics and other perils have also been proposed in response to COVID-19.⁷¹ More niche parametric products covering non-damage business interruption losses for SMEs from cyber events, outages, and terror-related events also exist on the market.⁷²

Key considerations: A multi-peril scheme contains complexities that may make it harder and longer to bring to fruition. A key question relates to scope — which perils should be included or excluded and how cross-border issues should be treated. While a flood or terrorist attack is location-specific, a cyber-attack may affect a UK company overseas or a foreign company's operations in the UK; pandemics present similar questions regarding suitability.

In a multi-peril scheme founded on diversification benefits, a balanced portfolio of risks and an associated view on the magnitude of events that trigger payouts would be critical. A parametric approach would reduce need for loss adjustment and also make any cover more affordable; on the other hand, it may not be appropriate for all chosen perils. Strategically, the fit with (or roll-up of) existing single-peril schemes would need to be examined closely, as would the precise operating model.

In this context, questions about market demand would need to be addressed — potential customers need to convince themselves that the coverage is worth having. Lessons from pools outside the UK suggest that early education of the policyholder base is vital for good take-up, and that messages on resilience are often best communicated by

trusted sources other than government and the insurance industry. In this context, the role of incentives would be important.

Data and analytical challenges would impede a view on pricing and limits. Additionally, the design might need a creative approach to financing that involves capital markets, a government backstop, and corporate or other levies. Indeed, the potential for residual surprises in such a complex scheme means a government guarantee would be vital to draw in both insurers (by limiting their liabilities) and customers (by making for a more attractive product).

 [To return to summary of opportunities, click here](#)

3.3. Cyber-risk pool

Context: The UK economy exhibits a high level of digital dependency, rendering organisations vulnerable to cyber-attacks from ordinary criminals, organised crime syndicates, and state-affiliated actors. Shifting operational practices during the pandemic — including remote working, expanded digital sales channels, and greater workflow automation — have expanded the attack surface for hackers, resulting in a rise in the number of attacks

across multiple vectors, especially ransomware. The first half of 2021 saw 304.7 million attempted ransomware attacks globally, up 151 percent over the same timeframe in the year prior and already eclipsing the 304.6 million attempts logged for the entirety of 2020.⁷³

The increasing frequency and severity of claims has led many insurers to increase rates, reduce capacity, and restrict coverage, with some introducing sub-limits and/or co-insurance with respect to ransomware-related claims. In the second quarter of 2021, cyber insurance premiums in the UK rose by 126 percent year on year.⁷⁴ Such hikes threaten the affordability of cyber coverage, especially for SMEs, thereby reducing the resilience of vital digital networks and businesses.

Idea and value: To keep pricing affordable, enhance coverage, and generally improve cyber resilience, government and the insurance industry could develop a levy and pool system to support cyber-insurance accessibility for UK businesses. Such a scheme would require appropriate backstops, modelled on other government-backed reinsurance schemes.

Two potential areas of focus stand out. First, providing coverage for ‘infrastructure loss’ events or catastrophic damage to key digital infrastructure networks that result in widespread impacts. Second, supporting access to coverage for SMEs by assisting with affordability and enhancing the specialist support that already plays a role for insured businesses before, during, and after an incident.

A ‘Cyber Re’ could help raise baseline cybersecurity practices of UK organisations as well as alleviate payouts in crises if it included provisions that required good organisational cyber-risk management. Government could also encourage insurers to adopt minimum security standards in risk assessments through, for example, Cyber Essentials accreditations. The government might also wish to mandate a certain level of cyber coverage for responses to public-sector tenders, similar to existing requirements on public and private liability coverage. Government could also consider passing supporting legislation that contained provisions on mandatory data and threat information sharing.

Existing analogue(s): Funded mostly by a levy on the insurance industry, Flood Re is arranged to provide flood

coverage for otherwise unaffordable policies for residential properties.⁷⁵ The recent inclusion of flood mitigation efforts and a greater focus on ‘building back better’ point to the potential for government-enabled schemes to enhance national resilience by helping vulnerable constituencies gain access to discounted insurance premiums and remedy their situational weaknesses.⁷⁶

Pool Re is designed to cover the impact of catastrophic terrorism events to commercial property that the insurance market could not otherwise absorb.⁷⁷ Currently backstopped by an unlimited guarantee (under review), it has created an environment for the commercial market to achieve maturity, thereby insulating the taxpayer from financial losses arising from acts of terrorism.

Key considerations: As referenced in Opportunity 3.2, the fact that cyber-risk knows no borders prompts coverage questions both for UK companies with business abroad and foreign companies with business in the UK. Not only does this expand the liabilities, it also complicates the assessment of levies to the pool, which might, under one model, see overseas insurance companies paying a levy to the pool for the UK exposure of their insureds.

Albeit tricky at a time of rising rates, a focus on premiums would help with a growing protection gap at a time when more coverage is needed. Backstop arrangements would mitigate insurer concerns about accumulation risk and their own exposures, while greater transparency in defining each category of cyber-risk would both reduce coverage uncertainty for organisations and reduce insurer exposure to hidden cyber-risks.

Political traction for a ‘Cyber Re’ would likely be informed by two factors. First, government might be reluctant to provide indemnification for the payment of ransoms under policies currently on offer from insurers as it would not wish to be seen to be de facto paying criminals and/or terrorist organisations. Second, it would be important to resolve the potential for perverse incentives. Government also acts as a regulator penalising data loss and other cybersecurity breaches. However, since insurance claims are often used by organisations to cover such penalties and the cost of disputing them, ‘Cyber Re’ might create conflicts of interest that government would have to resolve in discharging dual duties.

 [To return to summary of opportunities, click here](#)

3.4. Scaled-up resilience/adaptation bonds

Context: The burden of financing resilience and climate adaptation efforts for public infrastructure falls almost wholly on the public purse, which is unsustainable as costs increase and government finances are under significant pressure from other priorities. Although private finance has been used to finance public infrastructure projects for decades, it has been harder to draw in funds to develop, upgrade, and maintain sustainable or resilient infrastructure and ecosystems. Schemes have been stymied by difficulties in identifying clear profitable returns, navigating a lack of common standards and definitions across projects, and achieving value for a diverse set of beneficiaries.⁷⁸

Idea and value: Government could expand the scale and scope of the resilience and adaptation bonds it already issues and actively encourage private-sector beneficiaries to participate (a resilience bond is a fixed-income instrument issued to raise low-cost private capital for projects that enhance national resilience and generate investment

returns). This would facilitate government-initiated cost-sharing with the private sector on ‘hard’ measures such as sea defences, levees, and infrastructure toughening as well as ‘soft’ measures such as catchment restoration and forestry management initiatives. Government could also support the design process of bond-backed developments by providing project financing expertise from HM Treasury and grants for modelling as well as creating facilitation guidelines and best practice documentation.

At a time of increasing institutional investor interest in opportunities with strong ESG profiles, offerings in this area would present new investment opportunities with a distinct risk-return profile. Distributed ledger technology could support the traceability of projects and their impacts, and also reduce transaction costs.⁷⁹ In the long run, expanding this form of bond issuance would accelerate progress in sustainable development within the UK.

Existing analogue(s): The Department for Environment, Food, and Rural Affairs has backed the development of

green bonds to generate funds for the protection and restoration of natural habitats.⁸⁰ In California, legislative proceedings are under way for the issuance and sale of bonds to finance projects such as flood protection, extreme heat mitigation, and workforce development.⁸¹ These efforts can be amplified and applied in a resilience context to incentivise private firms to invest in infrastructure that delivers both long-term environmental benefits and sustainable financial returns.

Key considerations: To attract significant levels of interest, the government would need to provide both financial and non-financial support to address investor concerns. This might include technical support and funding to help investors identify bankable projects and the sharing of administrative costs to help kickstart projects. Standardised metrics and guidelines would make for more transparent and rigorous project evaluation, which would serve to encourage investors deterred by uncertainty and ambiguity.

 [To return to summary of opportunities, click here](#)

4. GOVERNMENT FACILITATING INNOVATION

4.1. Streamlined data-sharing arrangements

Context: The ability to draw on large pools of diverse, salient data in a timely way can be vital for preventing crises and mitigating impacts. Such data might relate directly to key risks and vulnerabilities; it might also be more contextual, revealing spending, consumption, and mobility patterns. However, perceived ambiguity in data-sharing laws and regulations, along with complexities in data access, often constrain disclosure and deployment and contribute to a culture that prioritises protection.

In the COVID-19 crisis, data-sharing constraints hampered an efficient joined-up response between central government, local authorities, and utilities regarding the location of at-risk individuals and households.⁸² Separately, data access that is dependent on relationships and connections inevitably raises questions about analytical bias and the quality of the insights that result.⁸³

Idea and value: The government could clarify or adapt legal guidance on data sharing, including any safe harbour arrangements in a crisis, to alleviate uncertainty and encourage participation. This could be complemented by standard templates for data access agreements,

collaboratively developed with business, that would help reduce cost and confusion further, especially for smaller firms. These foundations could be enhanced by more forward-thinking data-sharing strategies, universal metadata standards, the development of portals or data lakes, and the design of appropriate security provisions for sensitive data.

By enabling greater access to diverse datasets before and during a crisis, the government could leverage the speed and innovation of the private sector in response and recovery as well as attain more accurate situational awareness in fast-moving or complex crises. Improved guidance and clearer standards would reduce costs and operational inefficiencies for private firms seeking to build out their data-driven capabilities.

Existing analogue(s): The UK's data.gov.uk portal, which publishes data from central government, local authorities, and public bodies on a range of variables is a first step towards normalising open data arrangements. Non-regulatory tools that are mindful of emerging innovations, such as industry-led technical standards, are a good starting point for designing more granular data-sharing rules that accommodate cross-cutting opportunities emerging from ever-evolving digital capabilities.⁸⁴

The FSCCC is one exemplar of a public-private data sharing partnership. Involving approximately 40 financial

institutions and organisations such as the NCSC, the Cyber Defence Alliance, and the US Financial Services Information Sharing and Analysis Center, the FSCCC corroborates intelligence on potential threats and shares aggregated analysis for improving cyber resilience in the UK financial sector.⁸⁵

The EU's Data Governance Act, which governs private-sector reuse of public-sector data and access to individuals' personal and non-personal data, might also provide lessons for a legal framework that facilitates data sharing while enabling government oversight of its use by businesses.⁸⁶ Elsewhere, the Australian Government's Data Sharing and Release Bill introduces regulatory arrangements and establishes a National Data Commissioner who is tasked with guiding, regulating, and enforcing the national data-sharing scheme.⁸⁷

Key considerations: To craft the right regulatory amendments, it would be vital to understand more deeply the reservations and concerns that businesses have for data sharing.⁸⁸ Working with them on agreement templates should reduce confusion, avoid overly complicated operational requirements, and strike a sensible balance regarding commercial and public sensitivities.

 *To return to summary of opportunities, [click here](#)*

4.2. Open data sandbox and complex analysis platform

Context: The public and private sectors are increasingly capturing more data on a range of relevant issues that can support vulnerability assessments and the development and testing of effective response strategies. However, access to secure environments for matching, linking, and then interrogating such datasets is often limited. With researchers and civil society being left behind in the war for computing power due to rapidly increasing costs, cutting-edge technologies are increasingly being deployed to secure short-term commercial wins rather than confront society's biggest challenges.⁸⁹

Idea and value: Possibly as part of National Digital Research Infrastructure plans, the government could provide researchers, civil society, and the private sector with access to diverse, high-fidelity, interconnected, longitudinal data and state-of-the-art analytical tools through a data sandbox platform.⁹⁰ This would facilitate the integration and interrogation of different public and private data sources, including (with appropriate privacy safeguards) de-identified data — such as income, demographics, and health statistics — that come from different government departments. Especially where the opportunity arises to

support projects for the public good, the government could also grant public access to large computational resources within the sandbox that are designed for artificial intelligence or machine-learning applications to enable advanced analytics that would otherwise be too expensive for SMEs and researchers.

A powerful platform with appropriate safeguards could funnel more diverse, high-quality data into a centralised repository, thereby equipping government bodies as well as other stakeholders across society to better tackle national resilience challenges and conduct more comprehensive vulnerability assessments and research into effective crisis response strategies. It could, moreover, facilitate the combination or comparison of distinct datasets to derive cross-cutting, interdisciplinary insights that may serve as a bedrock of innovation — as with recent efforts linking mobility and health data to assess the effectiveness of COVID-19 lockdown measures.⁹¹ Access to the sandbox's databases and resources would also help fast-track data-driven insights on vulnerabilities and resilience strategies from private firms to supporting resilience efforts such as modelling the pandemic. This sort of work could also serve other national priorities (e.g. economic security, climate mitigation) and enhance the standing of UK science.

Existing analogue(s): The Office for National Statistics' Secure Research Service is one exemplar environment conducive to data interrogation. Its utility can be bolstered through integrating more data sources and broadening access to stakeholders involved in collaborative resilience research efforts. The US is also currently exploring a similar initiative through the recently announced National AI Research Resource Task Force.⁹²

Key considerations: It would be crucial to align on the data types and infrastructure to be prioritised in populating the sandbox, seeking high-resolution yet versatile options to maximise utilisation. Additionally, given the level of data throughput expected to run through such a sandbox platform and the width of anticipated access, it would be necessary to build in data integrity, privacy, and security concerns from the outset, including the implementation of strict dataset de-identification standards as well as secure access methods, education and training modules, and an audit function with appropriate sanctions.

 [To return to summary of opportunities, click here](#)

4.3. Real-time data integration into the National Situation Centre

Context: Data used to inform situational awareness, sense-making, and thus decision-making for emerging crises needs to be multi-dimensional, broad-based, credible, and timely. This is hard to achieve when sourcing data purely from government sources. For example, behavioural data – valuable for risk contextualisation and the assessment of societal impacts – is often sequestered in private-sector hands.

Government's variable experience with accessing and using data from other sources can hamper its ability to ask the right research questions, identify the most relevant and useful datasets for specific issues, and integrate them accordingly. The London Office of Data Analytics pilot revealed, among other issues, that local authorities struggled to access important data held by private suppliers; moreover, the lack of data standardisation across the public and private sectors made it challenging to process, clean, and join up data to facilitate analysis.⁹³ Such deficiencies may increase the likelihood of being blindsided by key vectors in the run-up to, and during, an incident, or otherwise failing to maximise the value of analytical opportunities to strengthen national resilience efforts.

Idea and value: The government could ensure that the recently announced National Situation Centre (NSC) is equipped to integrate data from a range of sources. These might include ever-growing real-time data from smart meters and the Internet of Things on mobility patterns, public sentiment streams, environmental factors (such as water height, wind speed, temperature), stockpile

levels and the movement of key goods, and response capabilities.⁹⁴

Leveraging private-sector data would provide the NSC with a more holistic and dynamic dashboard representation of the risk landscape, response capabilities, and societal capacities that might better anticipate cascading impacts in times of crisis. By collecting, cleaning, and integrating such datasets over time, trend analysis could also support the development of early-warning signals for emerging threats and help resource allocation in preparation for and during events.

Such a capability would also be foundational for exploring different planning scenarios that would better ensure the continuity of societal functions. Moreover, improvements to data availability, matching, and standardisation would support national risk assessment work by compiling a national data taxonomy to help identify data gaps that might be filled by further research. Such efforts would also allow for the provision of intelligence to the private sector, especially critical infrastructure sectors such as health, transport, and food, generating enhanced insights into emerging supply-chain risks and demand surges.

Existing analogue(s): In the wake of the COVID-19 outbreak, many countries have integrated diverse and highly granular data streams to better target social protection measures, understand the effectiveness of lockdowns, and model virus spread through microsimulations.⁹⁵ Australian banks provided the Australian Bureau of Statistics with the detailed spending data of businesses and consumers to help it better understand the impact of COVID-19 on consumption and investment.⁹⁶ In the UK, open banking

models allowed HM Revenue & Customs to access the income information of those in financial need to fast-track their applications for welfare entitlements, while NHS and supermarket data helped the government prioritise grocery deliveries to the vulnerable.⁹⁷

Broader examples are also plentiful. Singapore's Land Transport Authority monitors platform crowds in real time to manage train supply; social media data is increasingly used globally to identify and map natural hazard events; and ambulances in Estonia have on-the-fly access to the personal medical data of patients en route to hospital.⁹⁸ On a broader scale, the US National Aeronautics and Space Administration runs a Fire Information for Resource Management System that offers near real-time global active fire data within three hours of satellite observation.⁹⁹

Key considerations: It would be vital to arrive at the right balance of incentives and rules by which to engage the private sector on integrated data-sharing arrangements that can deliver intelligence in a timely, efficient way in times of crisis. Careful thought is needed to avoid potential blind spots in the NSC's database, especially regarding vulnerable populations or assets that might represent stress points within the national resilience network. Other technical issues include questions about how best to build out the Centre's data collection, centralisation, and standardisation capabilities as well as those relating to what standards the Centre might adopt in curating and maintaining data. It bears noting that this initiative would be greatly supported by streamlined and simplified data-sharing regulations agreements (see Opportunity 4.1).

 [To return to summary of opportunities, click here](#)

4.4. Critical national infrastructure interdependency stress testing

Context: The complexity of the infrastructure and services that maintain societal functions and economic activity is continually increasing, especially with an accelerating trend towards digitalisation and the growing dependency of utility networks on information and communications technology. However, the UK possesses no centralised capacity at present to understand and test interdependencies between such networks, the failure thresholds of individual assets, and the cascading consequences of specific outages across those networks. Emerging capabilities in this space, such as the Data & Analytics Facility for National Infrastructure (DAFNI), the Centre for Digital Built Britain (CDBB), and the recently announced plan for a CNI Knowledge Base, would benefit from being integrated, fast-tracked, and refined to explicitly expect private-sector involvement.

Idea and value: Government could facilitate sector-wide and cross-sector stress testing of CNI assets and their supply chains against major contingencies. Regulators would need to coordinate efforts and design scenarios that tested the collective strength of the UK's critical networks against extreme and compound threats.

Periodic stress testing would allow CNI owners and operators to understand what and how much is at risk, including from external dependencies, as well as examine how to enhance preparedness and resilience through targeted measures for critical network elements. A government-led forum could facilitate dialogue to share learnings in a non-competitive setting.

Such complex stress testing would involve the development of CNI simulation modelling capabilities by integrating public and private data on networks, dependencies, supply chains, and failure thresholds in a centralised national repository to be used by operators for vulnerability assessments. These capabilities would enable threat scenarios to be analysed, losses and damages to be estimated, and mitigation actions to be designed and tested. A centralised approach to modelling and stress testing would enable enhancements over time to benefit operators.

Existing analogue(s): Stress-testing strategies are well integrated in the financial sector. The Bank of England's 2021 Climate Biennial Exploratory Scenario is designed to test the resilience of the business models of large banks, insurers, and the national financial system to physical and transition risks from climate change.¹⁰⁰ Meanwhile, modelling capabilities for physical infrastructure are already in progress via DAFNI and CDBB, along with extensive scientific efforts to simulate disruptions to CNI in a more granular way.¹⁰¹

In the US, the annual Dodd-Frank Act Stress Tests and Comprehensive Capital Analysis and Review exercise provide a regime for regular stress testing in the banking sector. The former evaluates all banks' resilience under hypothetical recession scenarios nine quarters into the future, with results informing the annual individual capital requirements for all large banks; the latter assesses the capital levels and risk management capabilities of large banks.¹⁰² The European Banking Authority (EBA) also facilitates biennial EU-wide stress tests as the first stage of the European Central Bank's Supervisory Review and Evaluation Process, albeit with a bottom-up approach

wherein banks generate their stress-test projections using their own models, based on a macro-financial scenario set by the EBA.¹⁰³

Key considerations: Regulators would require stronger mandates and technical capabilities to make this happen, as this would provide a greater emphasis in some sectors on system resilience (vs. competition, price, and consumer protection). New capabilities would include advanced simulation modelling skills, system designers and access to high performance computing resources, along with the skills to deploy them.

It would be important to explore which modelling approaches would be most suitable for supporting CNI operators' stress-testing exercises. Over time, it would be valuable to develop a methodology that adequately accounted for interdependency complexities and helped CNI resilience leaders comprehend the nuances of cross-asset interactions and potential weak connections within their network. Moreover, it would be useful to recognise the increasing availability of evermore granular data that might inform modelling as technical possibilities unfold. A clear view should be formulated on how the data can best be used in aggregate, with appropriate checks and processes to maintain the privacy and confidentiality of data integrated into a national repository.

 [To return to summary of opportunities, click here](#)

4.5. Public-private sector exercises across the crisis cycle

Context: Successful responses to, and recoveries from, crises have often benefited from extensive cross-sectoral exercises, with agencies coming together, practising their responses, and honing their capabilities. The UK has extensive exercising programmes at multiple levels of government designed to validate plans, develop staff capabilities, and test procedures across agencies. However, beyond Local Resilience Forums that unite sectors to run exercises on controlling major accident hazards or managing localised flooding events, private-sector engagement is rarer in larger efforts such as Civil Contingencies Committee exercises.

This is a missed opportunity given government's heavy reliance on private actors before, during, and after crises — as evinced by its efforts on testing, tracing, vaccine development, PPE manufacturing, and logistics in response to COVID-19. Moreover, insights from multi-agency exercises are typically not shared with the private sector, preventing takeaways for individual firms and with possible impacts for national resilience.

Idea and value: Public agencies could more actively invite relevant private-sector businesses, particularly those operating critical infrastructures and systems, to participate in joint crisis exercises for preparedness, response, and

recovery. In certain instances, there may be a case for mandating involvement. These exercises might focus on validating emergency plans, developing staff capabilities, testing procurement procedures, and other critical activities. To enable this, private-sector involvement would need to be explicitly included in relevant doctrines such as the Resilience Capabilities Programme and associated guidance on emergency planning and preparedness.

The inclusion of actors from different sectors (discussion-based or tabletop exercises being less burdensome) would provide more opportunities for public-private interaction and mutual learning. Not only would this likely reveal unanticipated vulnerabilities and operational snags, it would also strengthen relationships and trust, enhance an understanding of different capabilities and working styles, and develop muscle memory that can be accessed in the future. Companies participating in these exercises would gain a better understanding of their own exposure to crises and business continuity weaknesses.

Existing analogue(s): In 2020, a wide range of organisations in the south of England — ports, port authorities, freight operators, logistics firms, and local authorities — participated in exercises in advance of the UK's departure from the European Union. This examined pinch points for the supply of goods and workarounds in anticipation of delays and other consequences of new border controls and customs arrangements.

In 2018, the Bank of England, in partnership with the UK's most systemically important financial firms and other financial authorities, required participants to respond to a cyber-attack scenario.¹⁰⁴ The test was overseen by the Cross Market Operational Resilience Group, which has a standing brief on strengthening the ability of the sector to respond to incidents. More than 10 years earlier, the financial sector undertook an exercise to explore the consequences of an influenza pandemic.¹⁰⁵ Global resilience exercises with wide uptake have also been used to explore how organisations and government agencies respond to and recover from globally catastrophic events.¹⁰⁶ Sweden has a long history of mass mobilisation exercises, with a focus on military reservists.¹⁰⁷

Key considerations: The mandate and expectation in the financial sector of participation in exercises does not exist elsewhere, so it would be important to create that mandate and determine the circumstances under which it might best be deployed. In other words, it would be useful to specify which types of exercise would benefit most from private-sector participation, what the end objectives are, and how the effort would benefit participating firms as well as the nation as a whole. Separately, it may be interesting to investigate the barriers and impediments to scaling up the currently successful Local Resilience Forum efforts to the national level for tackling broader, more strategic threats.

 [To return to summary of opportunities, click here](#)

5. GOVERNMENT CHEERLEADING BUSINESS INITIATIVES

5.1. Metrics for asset resilience and disclosure

Context: Maintaining the adequacy of existing privately owned infrastructure is vital for societal and financial resilience. Although considerations regarding climate change and other systemic threats can be built into the design of new assets, upgrading and maintaining existing ones in line with a changing risk profile can be more challenging. Such efforts are often fraught with inertia due to a lack of available capital or bankable return on investment. As an illustration, the United Nations Environment Program (UNEP) has forecast that adaptation costs in developing countries will reach almost \$300 billion by 2030, about 13 times the amount of international private sector funding available today.¹⁰⁸

Idea and value: To incentivise timely asset upgrading and maintenance, government could advocate for the inclusion of metrics on asset resilience and risk governance

— including design standards, maintenance records, and risk-engineering reports — in outputs from rating agencies and investment data providers. Additionally, government could also lead by example and publish such metrics on its own assets to encourage more widespread adoption and ultimately induce a paradigm shift towards a convention of asset resilience reporting and disclosure.

More granular metrics and improved reporting would help long-term investors direct capital towards assets that are better managed for resilience, thereby raising questions for owners and operators of less resilient assets. As rating agencies adopted such metrics, the underlying data could also inform the cost and design of loans, which would yield cost savings for private firms and hence create financial incentives for better asset management in the long run.¹⁰⁹ Such metrics could also be used as the key trackable KPIs required for ongoing access to sustainable and transition-linked finance. The net outcome would be greater trust in the reliability of critical societal functions.

Existing analogue(s): ESG-related indices and metrics are increasingly used by both investors and rating agencies, with the latter providing concessional loans and better

credit terms and conditions for green investments and companies with good ESG practices.¹¹⁰ This movement has in turn shifted capital toward green initiatives and improved awareness of ESG considerations, while at the same time prompting enhancements to private firms' risk management efforts.

Key considerations: Aside from deciding what should or should not be included by way of assets or systems, significant technical hurdles would need to be overcome for the specification of metrics to ensure an appropriate rating could be allocated. This challenge includes determining which risks to include in any metric scheme and where to draw the boundary on materiality. To achieve momentum, the government might need to not only lead by example but also deploy market-based incentives.

 [To return to summary of opportunities, click here](#)

5.2. Private-sector code(s) of crisis conduct

Context: National emergencies not only disrupt business-as-usual activities, but also create uncertainty for the private sector, especially regarding how they should respond vis-à-vis their peers or the rest of the industry. Although crises often bring out the best in organisations, mismatched expectations can undermine national resilience as businesses may be deterred from contributing to recovery and preparedness efforts at an optimum level.

Even where individual crisis codes of conduct exist and are deployed, these may not be fit for purpose during every type of emergency. Where firms only engage in damage limitation discussions in the absence of any consensus on expected behaviours, inadequate and short-sighted provisions and a lack of flexibility can hinder the private sector's ability to respond.

The COVID-19 crisis precipitated a wave of emergency antitrust measures. For example, the UK Competition and Markets Authority issued a warning against exploitative sales and pricing practices as well as non-essential collusion, while the Australian Competition and Consumer Commission prioritised temporary authorisations for coordination between competitors as well as watching out for affordability issues and price-gouging activities.¹¹¹ Instead of developing responses in real time, having formal

guidelines in place prior to the onset of crises might better forestall confusion and prevent undesirable practices.

Idea and value: Government could encourage industries to develop crisis codes of conduct that would help establish and clarify expectations as to reasonable behaviour by private firms during contingencies that trigger a State of Emergency declaration or during other extraordinary circumstances.¹¹² Any such code should include 'best-practice' provisions — developed by those industries with government input — on critical issues including data sharing, pricing, intellectual property rights, treatment of employees and suppliers, and capacity management. For example, a code of conduct for biopharmaceutical companies might include guidelines on licensing and supply agreements for essential drugs during a pandemic.

Successful implementation of any private-sector crisis code of conduct, particularly for firms providing critical services, would bolster societal resilience as private firms would be better placed to more seamlessly and efficiently allocate resources and capabilities during crises. This would accelerate private-sector responses under emergency circumstances, resulting, for example, in shorter procurement timelines. A formal code that helped clarify expected behaviours and was widely adopted would empower individual firms to cooperate without fear of being disadvantaged relative to their peers.

Existing analogue(s): The City Code on Takeovers and Mergers defines how listed companies in the UK are required to act during certain conditions, with enforcement by a board of senior executives.¹¹³ Elsewhere, the European trade association for the medical technology industries, MedTech Europe, recently updated its code of conduct to include additional guidance on how the industry can better support governments' COVID-19 responses.¹¹⁴

Key considerations: Such an effort would need to be industry-led and the culmination of extensive dialogue across business and sector leaders, with government as a key stakeholder playing a key role in identifying desired outcomes and sharing views on interdependencies. One model might be to have a single overarching industry-wide code with built-in contingency and flexibility mechanisms for particular applications; alternatively, there might be high-level principles or guidelines that then inform sector-specific or even crisis-specific codes. It would be necessary to determine applicability of provisions to smaller firms as well as larger ones. Clearly, it would need to be well promoted via industry associations — who might have been instrumental in its development — to achieve widespread adoption.

 [To return to summary of opportunities, click here](#)

5.3. Employee engagement for resilience

Context: Individuals and households represent a huge resource for furthering the resilience of homes and communities. However, it is often hard outside moments of clear crisis to galvanise their strengths towards clear goals. Given the relatively high levels of trust employees have in the businesses they work for, employers represent a key channel for strengthening employee awareness of resilience issues, encouraging them to take learning points back into their private lives and consequently bolster community resilience.¹¹⁵

Idea and value: Government could encourage companies, especially large employers, to enhance the disposition and capabilities of their workforces. A multi-pronged strategy might blend the inclusion of a resilience dimension into health and benefits offerings, educational opportunities on risk mindfulness, employer-based training for actions

to be undertaken in the event of specific contingencies, and support for local resilience-related community and charitable organisations — such as through offering employees paid leave to undertake community-based volunteering activities.¹¹⁶

Expanding these efforts would benefit employees as individuals in major life choice decisions, contribute to a stronger corporate risk culture, and deepen employee loyalty. More broadly, it would help foster a ‘whole-of-society’ culture-oriented approach to national resilience that would reduce the need for government intervention.

Existing analogue(s): Employers already support employee resilience in various ways — from health and safety requirements, through fire incident training, through to the lifestyle choices promoted via health and benefits programmes. More strategically, in all phases of the COVID-19 crisis, employers were a vital lodestone for

their workforce regarding employee behaviours — home working, social distancing, mask wearing, and vaccination — in support of both business continuity and employee wellbeing, but also with broader community benefits. Many employers also have active volunteering programmes, that encourage their employees to share their skills and experience with others.

Key considerations: Many companies have considerable experience in designing and implementing programmes in the areas identified above and would find it relatively easy to introduce more explicit resilience goals. Government, in all its constituent parts, is also a major employer and could adapt its own practices in these areas. Should there be a desire to consolidate such practices, the government could consider how workforce resilience-focused metrics might be integrated into non-financial reporting.

 [To return to summary of opportunities, click here](#)

Endnotes

- 1 UK Cabinet Office. (2021, March). [Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy](#).
- 2 Marsh McLennan Advantage. (2020, April). [Building national resilience](#).
- 3 Foster, P., & Neville, S. (2020, May 2). [How poor planning left the UK without enough PPE](#). Financial Times. Retrieved 12 October 2021. Harari, D., & Keep, M. (2021, September 24). [Coronavirus: Economic impact](#). Briefing Paper Number 8866. House of Commons Library.
- 4 Health and Social Care, and Science and Technology Committees. (2021, October 12). [Coronavirus: Lessons learned to date](#). HC 92. House of Commons.
- 5 Giles, C. (2021, July 1). [COVID pandemic masks Brexit impact on UK economy](#). Financial Times. Retrieved 12 October 2021. Pilling, D. et al. (2021, March 27). [New Suez crisis: A global economy creaking under the strain](#). Financial Times. Retrieved 12 October 2021. Jones, C. (2021, September 7). [The sunk cost of shipping to the UK](#). Financial Times. Retrieved 12 October 2021. Ambrose, J. (2021, September 21). [What caused the UK's energy crisis?](#). The Guardian. Retrieved 12 October 2021. O'Carroll, L. (2021, September 24). [What is causing the UK crisis in petrol supplies?](#). The Guardian. Retrieved 12 October 2021.
- 6 [Critical Infrastructure Ransomware Attacks](#). (2021, August 31). Cybersecurity in Application, Research, and Education Laboratory. Retrieved 12 October 2021. UK Finance. (2021). [Fraud – the facts 2021](#). US National Security Agency et al. (2021, July). [Russian GRU conducting global brute force campaign to compromise enterprise and cloud environments](#). Ofcom. (2021, January 27). [Understanding online false information in the UK](#).
- 7 Climate Change Committee. (2021, June 24). [Progress in reducing emissions: 2021 Report to Parliament](#). Climate Change Committee. (2021, June 24). [Progress in adapting to climate change: 2021 Report to Parliament](#).
- 8 Environment Agency. (2021, October). [Living better with a changing climate](#).
- 9 Gowing, N., & Langdon, C. (2018). *Thinking the Unthinkable: A New Imperative for Leadership in a Disruptive Age*. John Catt Educational Limited. Martin, P., & Giddings, J. (2020, December). [Building better resilience](#). National Preparedness Commission. Deloitte & Cranfield University. (2021, May). [Resilience reimagined: A practical guide for organisations](#). National Preparedness Commission.
- 10 The Prince's Responsible Business Network. (2020, December 3). [500,000 people supported through COVID-19 by businesses](#). Retrieved 12 October 2021.
- 11 Business Roundtable. (2019, August 19). [Business roundtable redefines the purpose of a corporation to promote 'an economy that serves all Americans'](#). Retrieved 12 October 2021. [The company of the future: Profit and purpose](#). (n.d.). Financial Times. Retrieved 12 October 2021.
- 12 Adamczyk, A. (2021, May 21). [Millennials spurred growth in sustainable investing for years. Now, all generations are interested in ESG options](#). CNBC. Retrieved 12 October 2021.
- 13 Dimon, J. (2021, April 7). [Chairman & CEO letter to shareholders](#). JPMorgan Chase & Co. Retrieved 12 October 2021. UK Corporate Leaders Group. (2021, June 23). [Bridging the gap: UK business and policy leadership for net zero](#). Retrieved 12 October 2021.
- 14 [Business Alliance to Scale Climate Solutions](#). (n.d.). Retrieved 12 October 2021. [Cyber Peace Institute](#). (n.d.). Retrieved 12 October 2021. [Ellen MacArthur Foundation](#). (n.d.). Retrieved 12 October 2021.
- 15 Edelman. (2021). [Edelman Trust Barometer 2021 – UK media deck](#).
- 16 Edelman. (2021, August 31). [2021 Edelman Trust Barometer special report: The belief-driven employee](#).
- 17 The Insurer. (2021, February 18). [Enoizi: Pool Re must retain "independence of thought" as a government body](#). Retrieved 12 October 2021. Meyer, D. (2021, April 7). [If a COVID-19 vaccine does turn out to be dangerous, who's on the hook?](#). Fortune. Retrieved 12 October 2021.
- 18 HM Treasury. (2020, March 11). [Government as insurer of last resort: Managing contingent liabilities in the public sector](#). As a follow-up, the government has recently announced the establishment of the Contingent Liability Central Capability (see HM Treasury. (2021, August 17). [Contingent liability approval framework](#).
- 19 Department for Business, Energy & Industrial Strategy. (2021, July 20). [Reforming competition and consumer policy](#). Retrieved 12 October 2021.
- 20 UK Regulators Network. (n.d.). Retrieved 12 October 2021. [Digital Regulation Cooperation Forum](#). (n.d.). Retrieved 12 October 2021.
- 21 Quest, L. et al. (2021, July 19). [4 ways regulators must keep up with the global digital economy](#). World Economic Forum. Retrieved 12 October 2021. Gambling Commission. (2021, September 22). [Gambling Commission responds to independent inquiry into BetIndex](#). Retrieved 12 October 2021.

- 22 Rosenberg, S., & Fried, I. (2021, August 26). [The government-industry cyberdefense dance](#). Axios. Retrieved 12 October 2021.
- 23 London First. (2020, September). [Data for London](#).
- 24 National Cyber Security Centre. (2021, June 17). [Financial sector cyber collaboration centre \(FSCCC\)](#). Retrieved 12 October 2021.
- 25 O'Sullivan, D. (2021, July 16). [White House turns up heat on Big Tech's COVID 'disinformation dozen'](#). CNN. Retrieved 12 October 2021. Espinoza, J. (2020, December 10). [EU to tell Big Tech to police internet or face large fines](#). Financial Times. Retrieved 12 October 2021. Department for Digital, Culture, Media & Sport. (2021, May 12). [Draft Online Safety Bill](#). CP 405. Department for Digital, Culture, Media & Sport & Department for Business, Energy & Industrial Strategy. (2021, August 9). [A new pro-competition regime for digital markets](#). CP 489.
- 26 Pegg, D. et al. (2020, May 7). [Revealed: The secret report that gave ministers warning of care home coronavirus crisis](#). The Guardian. Retrieved 12 October 2021. Booth, R. (2021, October 7). [Coronavirus report warned of impact on UK four years before pandemic](#). The Guardian. Retrieved 12 October 2021.
- 27 BBC News. (2021, September 27). [Fuel supply: UK suspends competition law to get petrol to forecourts](#). Retrieved 1 October 2021.
- 28 [Australian Data Availability and Transparency Bill 2020 \(Cth\) pt 4.2 div 1](#).
- 29 Lovegrove, S. (2021, September 16). [Sir Stephen Lovegrove speech at the Council on Geostrategy](#) [Speech transcript]. Cabinet Office.
- 30 Joint Committee on the National Security Strategy. (2021, September 13). [The UK's national security machinery: First report of session 2021-22](#). HC 231/HL 68. House of Commons & House of Lords. Health and Social Care, and Science and Technology Committees. (2021, October 12). [Coronavirus: lessons learned to date](#). HC 92. House of Commons.
- 31 Department for Business, Energy & Industrial Strategy. (2021, March 15). [Competition law exclusion orders relating to coronavirus \(COVID-19\)](#). Retrieved 12 October 2021. Competition & Markets Authority. (2020, March 25). [CMA approach to business cooperation in response to COVID-19](#).
- 32 OECD. (2016, June). [The changing face of strategic crisis management](#).
- 33 Foster, P. & Neville, S. (2020, May 2). [How poor planning left the UK without enough PPE](#). Financial Times. Retrieved 12 October 2021.
- 34 Department of Energy & Climate Change. (2015, February). [UK emergency oil stocks](#).
- 35 Department of Business, Energy & Industrial Strategy (2019, March 1). [Capacity market](#). Retrieved 12 October 2021.
- 36 OECD. (2020, June 24). [Stocktaking report on immediate public procurement and infrastructure responses to COVID-19](#). Retrieved 12 October 2021.
- 37 [Civil Contingencies Act 2004](#), c. 36.
- 38 Walker, C. (2014). [The governance of emergency arrangements](#). *The International Journal of Human Rights*, 18(2), 211-227.
- 39 [The US Defense Production Act of 1950, as Amended](#), 50 U.S.C. § 4501 *et seq.* (2018).
- 40 [The Network and Information Systems Regulations 2018](#) (2018/506).
- 41 Department for Digital, Culture, Media and Sport. (2020). [General data protection regulation keeling schedule](#).
- 42 [Critical Infrastructure Ransomware Attacks](#). (2021, August 31). Cybersecurity in Application, Research, and Education Laboratory. Retrieved 12 October 2021.
- 43 Fitch Ratings. (2021, April 15). [Sharply rising cyber insurance claims signal further risk challenges](#). Retrieved 12 October 2021.
- 44 Murphy, H. (2021, July 4). [Russia-linked hackers target IT supply chain with ransomware](#). Financial Times. Retrieved 12 October 2021.
- 45 [Australian Data Availability and Transparency Bill 2020 \(Cth\) pt 4.2 div 1](#).
- 46 The White House. (2021, May 12). [Executive Order on Improving the Nation's Cybersecurity](#). Retrieved 12 October 2021.
- 47 Cabinet Office, & Lord Agnew. (2021, June 7). [Firms must commit to net zero to win major government contracts](#). Retrieved 12 October 2021.
- 48 Pope, T. et al. (2021, January 15). [The cost of coronavirus](#). Institute for Government. Retrieved 12 October 2021.
- 49 National Audit Office. (2020, November 26). [Investigation into government procurement during the COVID-19 pandemic](#).
- 50 Federal Emergency Management Agency. (2021, August 5). [Advanced contracting for goods and services](#). Retrieved 12 October 2021.
- 51 Stronger Christchurch Infrastructure Rebuild Team. (n.d.). [Competitive collaboration](#).
- 52 Marsh McLennan Advantage. (2021, May). [Harnessing technology convergence](#).
- 53 British Business Bank. (n.d.). [National Security Strategic Investment Fund](#). Retrieved 12 October 2021.
- 54 Department for Business, Energy & Industrial Strategy. (2021, March 19). [Advanced Research and Invention Agency \(ARIA\): Policy statement](#). Retrieved 12 October 2021.
- 55 Mazzucato, M. (2018). [Mission-orientated research & innovation in the European Union](#). Directorate-General for Research and Innovation.
- 56 Thomas, D. et al. (2021, September 14). [UK chancellor takes taxpayer stakes in more than 150 start-ups](#). Financial Times. Retrieved 12 October 2021.

- 57 Ofgem. (n.d.). [Strategic Innovation Fund \(SIF\)](#). Retrieved 12 October 2021. Department for Digital, Culture, Media & Sport. (2021, August 9). [Shared Outcomes Fund 5G Testbed and Trials Programme: Fibre in water: Improving access to advanced broadband and mobile services via drinking water mains – application guidance](#).
- 58 Mazzucato, M., & Macfarlane, L. (2019, March). [A mission-oriented framework for the Scottish National Investment Bank](#). Institute for Innovation and Public Purpose.
- 59 Ministry of Defence. (2002, November). [DEFCON 705 – Intellectual property rights – research and technology](#).
- 60 Hutton, G. (2021, September 2). [Research & development spending](#). SN04223. House of Commons Library.
- 61 UK Cabinet Office. (2021, March). [Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy](#).
- 62 [Industrial Strategy Challenge Fund](#). (n.d). UK Research and Innovation. Retrieved 12 October 2021.
- 63 Cheltenham Borough Council. (2020, May). [Gloucestershire cyber and digital sector impact study](#).
- 64 [UK Collaboratorium for Research on Infrastructure and Cities](#). (n.d.). Retrieved 12 October 2021.
- 65 [The Trinity Challenge](#). (n.d.). Retrieved 12 October 2021.
- 66 Israel is the third most represented country on the NASDAQ index, with 2.6 percent of start-ups founded between 1999 and 2014 having achieved annual revenues of over \$100 million. Apolitical. (2017, June 6). [The government venture capital fund that boosted Israel's start-up economy](#). Retrieved 12 October 2021.
- 67 European Insurance and Occupational Pensions Authority. (2021, February 12). [EIOPA staff paper on measures to improve the insurability of business interruption risk in light of pandemics](#).
- 68 Marsh. (2021). [Pandemic Risk Protection Report 2021](#).
- 69 [French natural disasters compensation scheme](#). (2015, February 3). Caisse Centrale de Réassurance. Retrieved 12 October 2021. [US Further Consolidated Appropriations Act, 2020](#), H.R.1865, 116th Cong. (2020).
- 70 Financial Protection Forum. (2017, December). [Financial protection against crises and disasters](#).
- 71 Lloyd's. (2021). [Supporting global recovery and resilience for customers and economies](#).
- 72 Wood, C. (2019, December 11). [QOMPLX, Chaucer launch multi-peril parametric product for SMEs](#). Reinsurance News. Retrieved 12 October 2021.
- 73 SonicWall. (2021). [Mid-year update: SonicWall cyber threat report](#).
- 74 Marsh. (2021, July). [Global insurance markets: Pricing increases moderate in second quarter](#).
- 75 [Flood Re](#). (n.d.). Retrieved 12 October 2021.
- 76 Department for Environment, Food & Rural Affairs. (2021, July 29). [Flood and coastal erosion risk management policy statement: Progress update 2021](#). Retrieved 12 October 2021.
- 77 [Pool Re](#). (n.d.). Retrieved 12 October 2021.
- 78 OECD. (2015, December). [Green Bonds: Mobilising the debt capital markets for a low-carbon transition](#).
- 79 European Investment Bank. (2021, April 28). [EIB issues its first ever digital bond on a public blockchain](#). Retrieved 12 October 2021. HSBC & Sustainable Digital Finance Alliance. (2019, September). [Blockchain: Gateway for sustainability linked bonds](#).
- 80 Environment Agency, Department for Environment, Food & Rural Affairs, and Natural England. (2021, July 14). [Innovative nature projects awarded funding to drive private investment](#). Retrieved 12 October 2021.
- 81 [Safe Drinking Water, Wildfire Prevention, Drought Preparation, Flood Protection, Extreme Heat Mitigation, and Workforce Development Bond Act of 2022](#), A.B. 1500. (2021, May 18).
- 82 Science and Technology Committee. (2021, January 8). [The UK response to COVID-19: Use of scientific advice](#). House of Commons. Retrieved 12 October 2021. Ada Lovelace Institute & The Royal Society. (2021, January 5). [Learning data lessons: Data access and sharing during COVID-19](#).
- 83 The Alan Turing Institute. (2021, June). [Data science and AI in the age of COVID-19](#).
- 84 Department for Digital, Culture, Media & Sport. (2021, July 6). [Digital Regulation: Driving growth and unlocking innovation](#). Retrieved 12 October 2021.
- 85 National Cyber Security Centre. (2021, June 7). [Financial sector cyber collaboration centre \(FSCCC\)](#). Retrieved 12 October 2021.
- 86 Regulation 2020/0340. [Proposal for a regulation of the European Parliament and of the Council on European data governance \(Data Governance Act\)](#).
- 87 [Australian Data Availability and Transparency Bill 2020 \(Cth\) pt 4.2 div 1](#).
- 88 Massachusetts Institute of Technology Technology Review Insights. (2020). [The global AI agenda](#).
- 89 Hall, W., & Pesenti, J. (2017). [Growing the artificial intelligence industry in the UK](#). Department for Digital, Culture, Media & Sport & Department for Business, Energy & Industrial Strategy. World Economic Forum. (2021). [The Global Risks Report 2021](#).
- 90 Department for Business, Energy & Industrial Strategy. (2021, January 21). [UK research and development roadmap](#). Retrieved 12 October 2021.

- 91 Basellini, U. et al. (2021). [Linking excess mortality to mobility data during the first wave of COVID-19 in England and Wales](#). *SSM-Population Health*, 14, 100799.
- 92 The White House. (2021, June 10). [The Biden administration launches the National Artificial Intelligence Research Resource Task Force](#). Retrieved 12 October 2021.
- 93 Greater London Authority. (2018, February). [Piloting the London Office of Data Analytics](#).
- 94 The Open Data Institute. (2021, June). [Improving data access in the UK smart meter data ecosystem](#).
- 95 London Data Commission. (n.d.). [Supporting London's response and recovery during COVID-19](#). Retrieved 12 October 2021. The Alan Turing Institute. (2021, June). [Data science and AI in the age of COVID-19](#).
- 96 McIlroy, T., & Cranston, M. (2020, August 16). [Banks hand COVID-19 spending data to the ABS](#). *Australian Financial Review*. Retrieved 12 October 2021.
- 97 Dowden, O. (2020, July 9). [The pandemic has made UK government rethink its relationship with data](#). *ComputerWeekly*. Retrieved 12 October 2021.
- 98 Flood Tags. (n.d.). [Our solutions](#). Retrieved 12 October 2021. Tavra, M. et al. (2021). [The role of crowdsourcing and social media in crisis mapping: A case study of a wildfire reaching Croatian City of Split](#). *Geoenvironmental Disasters*, 8(1), 1-16.
- 99 National Aeronautics and Space Administration. (n.d.). [Fire Information for Resource Management System](#). Retrieved 12 October 2021.
- 100 Bank of England. (2021, June 8). [Key elements of the 2021 Biennial Exploratory Scenario: Financial risks from climate change](#). Retrieved 12 October 2021.
- 101 Thacker, S. et al. (2017). [System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures](#). *Reliability Engineering & System Safety*, 167, 30-41.
- 102 Board of Governors of the Federal Reserve System. (2021, February 12). [Federal Reserve Board releases hypothetical scenarios for its 2021 bank stress tests](#). Retrieved 12 October 2021. Board of Governors of the Federal Reserve System. (n.d.). [Stress tests and capital planning](#). Retrieved 12 October 2021.
- 103 European Banking Authority. (n.d.). [EU-wide stress testing](#). Retrieved 12 October 2021.
- 104 Bank of England. (2019, September 27). [Sector Simulation Exercise: SIMEX 2018 report](#). Retrieved 12 October 2021.
- 105 Financial Services Authority, HM Treasury, & Bank of England. (2007). [Overview of financial sector pandemic flu planning](#).
- 106 EARTH EX, The Resilience Shift, & Electric Infrastructure Security Council. (2019). [EARTH EX@ III 2019: Lessons learned from a global resilience exercise](#).
- 107 Swedish Armed Forces. (n.d.). [Total Defence Exercise 2020](#). Retrieved 12 October 2021.
- 108 S&P Global Ratings. (2018, December 7). [Plugging the climate adaptation gap with high resilience benefit investments](#).
- 109 FTSE Russell. (2021, June 24). [How is corporate ESG data impacting capital flows?](#). Retrieved 12 October 2021.
- 110 OECD. (2020, September 25). [ESG investing: Practices, progress and challenges](#).
- 111 Competition and Markets Authority. (2020, March 5). [COVID-19: sales and pricing practices during coronavirus outbreak](#). Retrieved 12 October 2021. Australian Competition and Consumer Commission. (2020, March 27). [ACCC response to COVID-19 pandemic](#). Retrieved 12 October 2021.
- 112 Ong, Z., & Gerbase, A. (2020). [Public-private partnerships during public health emergencies](#). *Horasis*. Retrieved 12 October 2021.
- 113 The Panel on Takeovers and Mergers. (2021, July 5). [The Takeover Code, thirteenth edition](#).
- 114 Sidley. (2020, April 1). [MedTech Europe releases new guidance altering code of conduct during COVID-19 crisis](#). Retrieved 12 October 2021.
- 115 Edelman. (2021). [Edelman Trust Barometer 2021](#).
- 116 Hariharan, K. et al. (2021, July 13). [How businesses can improve the health of societies](#). *BRINK*. Retrieved 12 October 2021.

ACKNOWLEDGEMENTS

This paper has benefited from multiple interviews and other discussions with members of the National Preparedness Commission, business leaders, and risk experts from across the public, private, and third sectors — in the UK and abroad — who kindly shared their experience and insights and acted as a sounding board for some of the opportunities discussed in this report. Many thanks to those who participated.

Author

Richard Smith-Bingham

Richard leads a team at the core of Marsh McLennan that [explores](#) critical risks and transformational agenda such as climate resilience, cyber resilience, healthy societies, innovations in infrastructure, transformative technologies, and workforce for the future.

He is a longstanding contributor to, and Advisory Board member of, the World Economic Forum Global Risks Report, a Steering Group member of the OECD's High-Level Risk Forum, and a commissioner on the UK's National Preparedness Commission.

Marsh McLennan contributors

Marsh

James Crask, Graeme Riddell, Bob Sawers

Guy Carpenter

Ruth Lux, Siobhan O'Brien, Jamie Russell, Charles Whitmore

Oliver Wyman

Anthony Charrie, Lisa Quest

Marsh McLennan Advantage

Darrel Chang, Daniel Kaniewski, Deepakshi Rawat

Design

Sujin Lee, Tezel Lim

How to cite this report

Smith-Bingham, R. (2021). Partnering with purpose: Strengthening national-level resilience in the UK through more dynamic public-private interactions. National Preparedness Commission & Marsh McLennan Advantage.

Lord Toby Harris

Chair, National Preparedness Commission

toby.harris@nationalpreparednesscommission.uk

Richard Smith-Bingham

Executive Director, Marsh McLennan Advantage

richard.smithbingham@mmc.com

[Marsh McLennan](#) (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 78,000 colleagues advise clients in 130 countries. With annual revenue over \$18 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. [Marsh](#) provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. [Guy Carpenter](#) develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. [Mercer](#) delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and well being for a changing workforce. [Oliver Wyman](#) serves as a critical strategic, economic and brand advisor to private-sector and governmental clients.

For more information, visit [mmc.com](#), follow us on [LinkedIn](#) and [Twitter](#) or subscribe to [BRINK](#).



This publication was prepared by Marsh McLennan for the National Preparedness Commission.

Copyright ©2021 Marsh & McLennan Companies Ltd, Inc. All rights reserved.

This report may not be sold, reproduced or redistributed, in whole or in part, without the prior written permission of Marsh & McLennan Companies, Inc.

This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report.

We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.