Building National Resilience

Preparing the UK for Extreme Risks

INTRODUCTION

> The Government's current strategy of centralised and opaque risk assessment and risk management, which fails to make adequate preparations, has left the UK vulnerable.
>
> The UK must adopt a whole of society approach to resilience [...] Risk and resilience are not solely the concern of central Government policymakers; they have the capacity to alter the lives of millions. The Government must ensure it properly accounts for and involves all elements of society in its risk assessment and planning.
>
> - House of Lords Select Committee on Risk Assessment and Risk Planning, *Preparing for Extreme Risks: Building a Resilient Society*, HL Paper 110, December 2021

Before the pandemic, the UK's approach to risk assessment and risk management was widely lauded around the world for its rigour. The 2019 Global Health Security Index even placed the UK as among the best-prepared countries in the world for a pandemic, ahead of Japan or South Korea. With Covid-19, however, the UK's risk management system was shown to be inflexible and deficient for protecting national needs.

Background to this white paper

During the pandemic in December 2020, the House of Lords Risk Assessment and Risk Planning Committee called for written contributions to its inquiry into the UK's preparations for what it called "extreme risks and disruptive national hazards". In particular, the committee examined how the UK can ensure that it is as resilient to extreme risks and emergencies as possible.

As the voice of the UK's corporate risk management community, Airmic responded to the call as part of the national debate about how the UK manages risk. To facilitate a representative submission, Airmic convened a roundtable of its Enterprise Risk Management Special Interest Group. Participants in that discussion and their respective comments remain anonymous; however, the sum of their views formed the basis of Airmic's submission to the committee.

In the government's response in March 2022 to the committee's report, it reaffirmed its commitment to learning lessons from the pandemic, recognising that effective and meaningful risk management must be an integral part of informed decision-making. The government accepted many of the committee's recommendations and committed to considering others. In that same month, furthermore, the government presented the '2022 Post Implementation Review of the Civil Contingencies Act' in Parliament – a five-yearly assessment of the framework for emergency preparedness in the UK. The review made recommendations to improve the legislative framework around the role of local resilience forums (LRFs) and resilience structures, and on assurance and accountability.

This paper presents the key points of Airmic's submission in the context of the committee's inquiry and subsequent report titled *Preparing for Extreme Risks: Building a Resilient Society*, which was published in December 2021.

Yet, there are many other risks that the UK could face – and possibly more extreme ones – aside from the pandemic. The UK has also had to reckon with severe supply chain disruption and threats to its fuel supply during this time. This has brought concerns about the fragility of the just-in-time networks on which the UK's food, fuel and essential services rely. The fall of Afghanistan to the Taliban in August 2021 increased fears about regional security and the renewed threat of global terrorism. Russia's invasion of Ukraine in February 2022 brought the spectre of war to Europe's doorstep.

All of this has called for the UK to assess and strengthen its national resilience, to ensure it is better prepared for the next crises.

1. WHAT EXTREME RISKS DOES THE UK FACE?

Typically, an extreme risk is considered to be an event that would impact the achievement of the strategic objectives of an organisation, or an event that would impact at a global, regional or national infrastructure level.

There is no commonly accepted definition of extreme risk, and it does not form part of the International Organization for Standardization (ISO) Guide 73 risk taxonomy. Consequently, it is important for every organisation to consider a definition of extreme risk to ensure the approach and communication of managing risk across the organisation is consistent with the strategic, tactical and operational objectives of the organisation and its risk appetite.

Examples of extreme risk include:

- Disruption to the national infrastructure caused by failure of the supply of water, power, and information and communication networks
- Flood caused by extreme weather
- Denial of access to business locations caused by political or social unrest
- Cyber security failure and loss of or denial of access to data or information caused by a cyber-attack
- Contamination by activists or other criminal activity, leading to failure in service delivery
- Disease caused by a material variant of Covid-19, failure of vaccines or a new virus
- Lack of innovation and long-term planning caused by economic uncertainty
- Failure of a stable trading environment in which investment is hesitant, caused by social erosion
- Inability to finance the risks caused by the unavailability of insurance cover for some extreme or systemic risks
- Continued widening of the political void caused by the pandemic, Brexit and the negative impacts/side effects of social and click-driven 'media' (spreading of disinformation)
- Scaling back on CapEx (capital expenditures), which could have wide societal impacts on issues such as the need for sustainable investment to transition to a low or no carbon economy, caused by the response to Covid-19 and the need for organisations to conserve cash to support corporate survival.

Extreme risks do not operate in silos and can impact others. Indeed, there is frequently a cascading effect. Cumulative risks may impact multiple stakeholders, caused by connected risk failure such as in the supply chain. Systemic risks at the

level of an organisation could trigger severe instability or collapse an entire industry or economy.

So far, threats from the commercial sector do not appear to be well considered. For example, the recent pandemic demonstrated the reliance of supermarket chains to provide food to society. Had supermarkets closed – for instance, due to the refusal of staff to come to work – or had their logistics failed, the resulting societal breakdown could have been catastrophic for the UK.

Airmic believes that the UK is particularly vulnerable to or is poorly prepared for the following risks:

- The absence of whole or cross-system thinking and risk assessment across sectors and organisations essential for the strategic infrastructure
- The limitations in the use of data and AI to enhance the understanding of supply chains
- The economic dominance and the political centre of power in London, which makes the UK vulnerable to an extreme event in London
- The electoral process and associated turnover of government, which create risk to thinking and investing long term
- The extreme effect of the pandemic on the UK, which will require national funding for many years, putting other potential extreme risks out of vision and placing the treatment of these on the risk back burner
- The UK's diminishing influence on the global stage – the lack of direction for financial services, and a transfer of authority and capital in the insurance industry away from the UK and London is a tangible example.

On the upside, the UK has demonstrated a 'can do' culture not bound by general convention or community. Nevertheless, in looking back at the experience of the pandemic, politics and the science community could have been more joined up.

2. THE GOVERNMENT'S APPROACH TO RISK ASSESSMENT

The UK government's Orange Book – a guidance produced by HM Treasury's Government Finance Function, which establishes the concept of risk management – and the associated family of guides such as the National Risk Register, produced by the Cabinet Office, are widely respected. They should form part of the 'bible' for corporate risk professionals.

However, they are infrequently updated. Like other guides, they have typically not kept pace with developments in practices used by corporate risk professionals. This means that organisations using the Register as a benchmark will not be synchronised with their reality, nor aware of the velocity of change, which could act as a lag on their developing and using a shared understanding.

Knowledge of these guides is also not effectively communicated to the commercial world; yet despite some shortcomings, they would add value as guidance and as a benchmark for government suppliers on how the government manages risk.

Key to effective and efficient risk assessment is the gathering, analysis and application of data using consistent taxonomy, data sets, metrics and methodologies. The government appears to use a range of approaches, which can inhibit the ability to aggregate and analyse data from different risk assessments.

Engaging professionals with commercial risk management experience to join those who

educate government risk management professionals, and taking part in exercises such as horizon scanning, scenario analysis and risk assessments, would help the embedding of current commercial good practice.

Introducing commercially experienced professionals into non-executive roles as part of government committees could increase the diversity of these groups and improve the bandwidth of government risk governance.

Risk is typically viewed in government as something negative to be minimised or avoided. There is a focus on strengthening risk frameworks and processes, tightening risk assessments, reinforcing oversight arrangements, and improving monitoring and reporting processes, with an emphasis on compliance and prudence. This can be to the exclusion of the upside or value creation aspects of risk and associated opportunities. This approach makes the assessment of long-term risks more difficult.

An understanding of enterprise risk management (ERM) does not appear to be at the heart of government, and there is a disconnect between governance and intent.

There appears to be limited capability in government in managing emerging risks. Emerging risks demand a different approach. In practice, although a robust discussion of key or principal risks would also likely capture emerging risks, a formal process for identifying emerging risks is required. While the approach for emerging risks should be analytical, it should also be creative and pragmatic, reflecting the complexity of uncertainties to secure buy-in and actionable results.

The approach to developing the National Risk Register requires enhancement to address risk connectivity and the application of the Register to an integrated controls environment – for example, developing a linkage between national risks and the role of the government as 'insurer of last resort' in supporting solutions for systemic risk, which the insurance industry is not equipped to provide.

A sense of the timescales associated with the risks in the National Risk Register may also help enhance the approach. Threats that can arrive immediately – for instance, a terrorist act – may need to be considered differently to threats that evolve over time – for instance, poor air quality.

The government should determine its risk appetite. The Orange Book supplement on risk appetite, published in October 2020, assists in that regard. An understanding of risk appetite will help to drive the level and prioritisation of assurance the government should be seeking. The government must understand key priorities at all levels in order to implement a strategic response to disruptions – key indicators will inform resilience performance and decisions.

3. INTEGRATING RISK MANAGEMENT INTO NATIONAL FRAMEWORKS

Risk management should be part of all government activities and processes, including strategic planning, operational, financial, legal, IT, and project and change management. It should be integrated into processes where decisions are made and discussions are held, to enable the government to grasp new opportunities whilst reducing the risk of threats, in a controlled manner.

Risk management should be integrated into a consistent framework to ensure that robust assurance can be provided on the effectiveness of the controls in place. The 'Three Lines Model'[1] is an example of a framework used globally, primarily

1 See for instance: Chartered Institute of Internal Auditors, 'Application of the Three Lines Model.' https://www.iia.org.uk/resources/corporate-governance/application-of-the-three-lines-model/

in financial institutions, but which can be modified to suit all organisations including the government. Used as a tool, rather than as a standard, this can help organisations to identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management, through:

- Adopting a principles-based approach, which should be adapted to the organisation
- Focusing on the contribution risk management makes to achieving objectives, and protecting and creating value
- Understanding the roles and responsibilities represented in the model and the relationships between them, and
- Implementing measures to ensure activities and objectives are aligned with the interests and prioritisation of stakeholders' front of mind.

The government should consider adopting a more corporate approach to managing risk, and learn from the knowledge and experience of corporates. The National Risk Register could provide the agenda for a national conversation about risk.

Ways of characterising risks

Current ways of characterising risk have not worked effectively with the pandemic, where a worst-case scenario should be adopted and constantly updated – current practice has erred towards optimism. Preparing for the less serious is not preparing for the worst.

The challenge to any model, and especially those with predetermined 'scores', is the loss of flexibility at the expense of consistency. An extreme event such as the pandemic does not conform to the pattern of many other extreme events – it has not been a 'text book' crisis, it has been an 'event' with multiple crises and recoveries operating concurrently.

Any scoring should be supplemented by intelligent risk management involving informed people from across all stakeholders who are constantly considering scenarios in concert with the other risk management systems informing the process.

The interconnectedness that one event may have on other risks should be taken into account when assessing the overall threat.

Communicating national contingency plans

The communication of contingency plans is patchy. Without a consistent process, it is difficult to comment on whether plans are understood. It is worth examining whether accepted good contingency practice is adopted, as this would include communication and feedback, and the cascading of lessons learnt across all stakeholders.

Contingency planning should form part of an integrated approach to risk management and, as such, should form part of scenario planning exercises involving a range of scenarios conducted by professionals from all disciplines. There is a tendency in some organisations and in some professions to ring-fence this process. Without agreed consistent metrics and communication of performance against these, how can those who govern in government or business have confidence that this process is effective?

4. THE ROLE OF THE INDIVIDUAL AND THE PUBLIC IN NATIONAL CRISES

The Global Health Security Index released in November 2019, cited in this paper at the outset, examined whether countries

across the world were prepared to deal with an epidemic or a pandemic. The index analysed preparation levels by focusing on whether countries have the proper tools in place to deal with large-scale outbreaks of disease. Measured on a scale of 0 to 100, where 100 is the highest level of preparedness, the United States came first, followed by the UK and the Netherlands. By March 2020, the UK appeared to lose this leadership position. Some businesses that were relying on guidance from the government to tailor their disease response strategies underestimated the potential impact of the eventual pandemic and generally were too slow to respond.

Business leadership has been challenged by a lack of useful intelligence and data to support business decisions during the pandemic, leading to some knee-jerk, short-term reactions. Some supply chains were caught off guard, with limited contingency plans for strategic sourcing options in an interconnected global crisis. At an operational level, the processes of many businesses were found wanting around the long-term business impacts to office spaces – for example, the ability to supply home workers with laptops, monitors and basic office furniture to make working at home possible, safe and healthy.

Crisis management has not been set up to deal with long-term crisis. The pandemic should modify crisis management practice. Government and businesses will need to be comfortable dealing with increased uncertainty, allowing them to better identify opportunities and threats, and rise to the extreme long-term event.

The concept and application of 'red teaming' should be explored. This helps teams to ask better questions and challenge embedded assumptions. 'Red teaming' refers to applying independent structured critical thinking and culturally sensitised alternative thinking from a variety of perspectives. It uses structured tools and techniques to help us ask better questions, challenge explicit and implicit assumptions, expose information we might otherwise have missed, and develop alternatives we might not have realised existed in order to improve understanding.

The Edelman Trust Barometer is a useful source of trust indicators. As its 2021 report put it, "Government briefly seized the high ground, emerging as the most trusted institution in May 2020, when people entrusted it with leading the fight against Covid-19 and restoring economic health. But Government failed the test and squandered that trust bubble, having lost the most ground in the last six months (down 8 points globally)."

Ineffective information and communication will threaten public engagement and pandemic recovery. Education is the starting point. This topic could be included in the school syllabus as an investment in building and embedding awareness, responsibility and raising the level of trust in stakeholders.

5. DEVELOPING RESILIENCE CAPABILITY

Resilience is a term that is not consistently defined or understood, which inhibits the development of good practice. The 2018 Airmic report *Roads to Revolution* identified eight principles for achieving resilience in an age of advances in technology and digital transformation:

1. Risk radar focused on emerging risks and developments in technology

2. Resources and assets able to take full advantage of developments in technology

3. Relationships and networks that are constantly developed and extended

4. Rapid response supported by excellent communication within the organisation

5. Review and adapt to events to protect and enhance reputation

6. Redesign processes to embrace new technologies and encourage innovation

7. Retain stakeholders during the transformation by analysing big data

8. Reinvent purpose by opportunity awareness, commitment and capabilities.

The report of the House of Lords Select Committee on Risk Assessment and Risk Planning used the United Nations Office for Disaster Risk Reduction (UNDRR) definition of resilience, which notes that resilience refers to emotional and psychological resilience as well as physical or material resilience.

An untested plan is doomed to fail. Exercises should involve all stakeholders, including suppliers and other third parties, who often embed their expectations on resilience standards, event notification and event response within supplier contracts.

The HM Treasury report *Government as insurer of last resort: Managing contingent liabilities in the public sector*, published in March 2020, noted that:

> The UK government has a responsibility to protect the population and provide stability. As a result, the government bears risks, and incurs costs when unforeseen events occur. These risks and costs typically arise because they cannot be adequately insured by the private sector and the government should take them on. This is known as the government's role as insurer of last resort. [...]
>
> Taking on these risks creates liabilities that are uncertain but might lead to future expenditure if specific conditions are met or specific events happen. These liabilities are known as contingent liabilities. These types of contingent liabilities are an increasingly important policy tool to support economic growth and safeguard the economy in times of stress. The risks need to be managed carefully.

Proposals to strengthen national resilience should also be considered in the context of the private sector. There is much to be gained from considering the public and private sectors in concert, as many of the issues, risks, controls and lessons addressed are shared.

Conclusions of the House of Lords Committee report

In considering the 99 submissions it received, including Airmic's, the House of Lords Select Committee on Risk Assessment and Risk Planning concluded in its report that:

- The government's current risk management system is veiled in an unacceptable and unnecessary level of secrecy.

- The government's risk assessment process is unable to encompass the complexity of risks facing the UK, failing to account for interconnected or cascading risks and chronic or long-term risks, and has a bias against low-likelihood/high-impact risks.

- A more dynamic, data-driven risk management system is needed and should be linked directly to preparation, mitigation and response.

- Such a risk management system must be matched by practical measures to ensure

preparedness and resilience – the government must not only anticipate risks, but prepare for and respond to them effectively.

- Competence, capacity and skills are required to manage these crises. Risk plans must be frequently tested, challenged and scrutinised.
- Preparation, mitigation and response plans must be scrutinised, and planners must be accountable both within government and to Parliament, creating a system of audit that is appropriately resourced.
- While prevention is significantly cheaper than response, the government has a traditional disincentive to invest against possible risks, especially low-probability/high-impact risks. Spending policy for risk and resilience therefore needs to be readdressed.

Finally, the report acknowledged that no government can succeed in anticipating every threat or hazard. Therefore, the UK needs to be prepared to recover from shocks to which it is vulnerable. That capacity to recover must be based on a flexible, adaptable and diverse population that appreciates the need for its own resilience.