

# Building national resilience

Aligning mindsets, capabilities, and investment

By Richard Smith-Bingham and Alex Wittenberg

# Contents

## 04 **Introduction**

## 06 **Determining the most material risks**

A strategic framework  
Risk characterization and “sense-making”  
Impact analyses

## 12 **Mobilizing government capabilities**

Centralized ownership  
A smooth-running and nimble ecosystem  
Authority, oversight, and accountability

## 18 **Implementing strategic initiatives**

Fiscal and financial resilience  
Infrastructure investment  
Broader policy opportunities

## 24 **Innovation, agility, and leadership**

# Five takeaways

## 01

Building preparedness for risks

that may threaten national security, economic prosperity, and societal wellbeing is a critical function of government

## 02

The constantly evolving risk context

demands greater ambition, innovation, and agility from country-level resilience frameworks

## 03

Enhanced protections for critical national infrastructure and measures that reduce the fiscal impact of disasters must be at the top of the agenda for any government

## 04

Greater leverage of new data and analytics will support the business case and momentum for intervention

## 05

A senior-level risk champion empowered to bring together key stakeholders for lasting solutions will amplify the mandate of national risk units

# Introduction

Effective country-level risk management is of paramount importance in light of the extraordinary pace of global change, hugely costly disasters, and volatile political conditions.

Building preparedness for risks that may threaten national security, economic prosperity, and societal wellbeing is a critical function of government. Robust provisions, well evidenced and communicated, project confidence to citizens, the business and investment community, and international partners alike. Conversely, failing to prepare for long-term challenges, along with the poor handling of periodic crises, raises questions about national resilience and leadership competence.

However, establishing or sustaining an effective response framework at the center of government isn't easy and demands significant bureaucratic and political commitment. Analyses must accommodate an array of very different risks and their complex interactions with risk-absorbing systems. Initiatives have to balance near-term and long-term requirements. Investment needs to work within competing government priorities and resource constraints. And processes must formally engage a wide range of stakeholders.

Against this backdrop, many practitioners acknowledge the importance of taking a "holistic" view of the risk landscape and a "systems-based" view of impacts. There is widespread acceptance of the merits of adopting an

"all-of-government" approach to the challenge and the need to mobilize an "all-of-society" response. And, of course, compelling approaches are vital at all phases of the risk-management life cycle – from observation and assessment, through prevention and preparedness initiatives, then response and recovery capabilities, to learning and improvement.

And those generic principles are not the sole challenges to managing country risk.

Arguably, the goal of country-level resilience has rarely been as multifaceted as it is now, and the stakes have seldom been higher. The pressure for greater effort and sophistication is intensified by four complicating factors:

- The increasing economic cost of disasters in recent decades, with governments absorbing an ever-larger share of that burden, especially at a time of fiscal weakness
- The extraordinary pace of change in the world, where numerous forces are intersecting in unexpected ways with complex reverberations to threaten new shocks and surprises
- Volatile political conditions in many countries – characterized by low levels of popular

trust in democratic leaders, authoritarian leaders vesting even more of the national story in their own decision-making, and weaker international collaboration on a range of critical agenda

- A host of governments pursuing major economic, political, or societal transformations to future-proof their countries against long-term scenarios

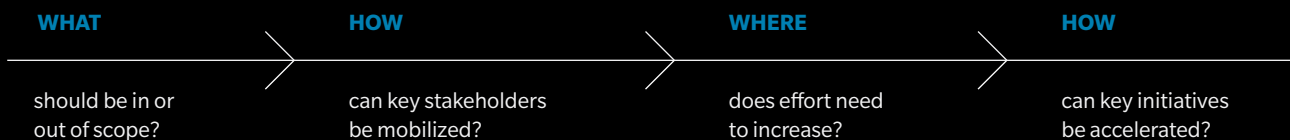
On the plus side, however, many new practices are available to be leveraged, and new analytical capabilities offer opportunities to rethink old solutions that may have run their course.

This report explores the key issues for national and sub-national governments (see Exhibit 1). The first section sets out ways of framing the evolving risk landscape that help allocate resources to the most material concerns. The second reviews options for organizing and coordinating risk management activities within government, while the third explores some of the

key policy levers and solutions that will yield desired outcomes. The final section examines what is required for continuous improvement and the value of an overall “risk champion” within government to drive the agenda forward.

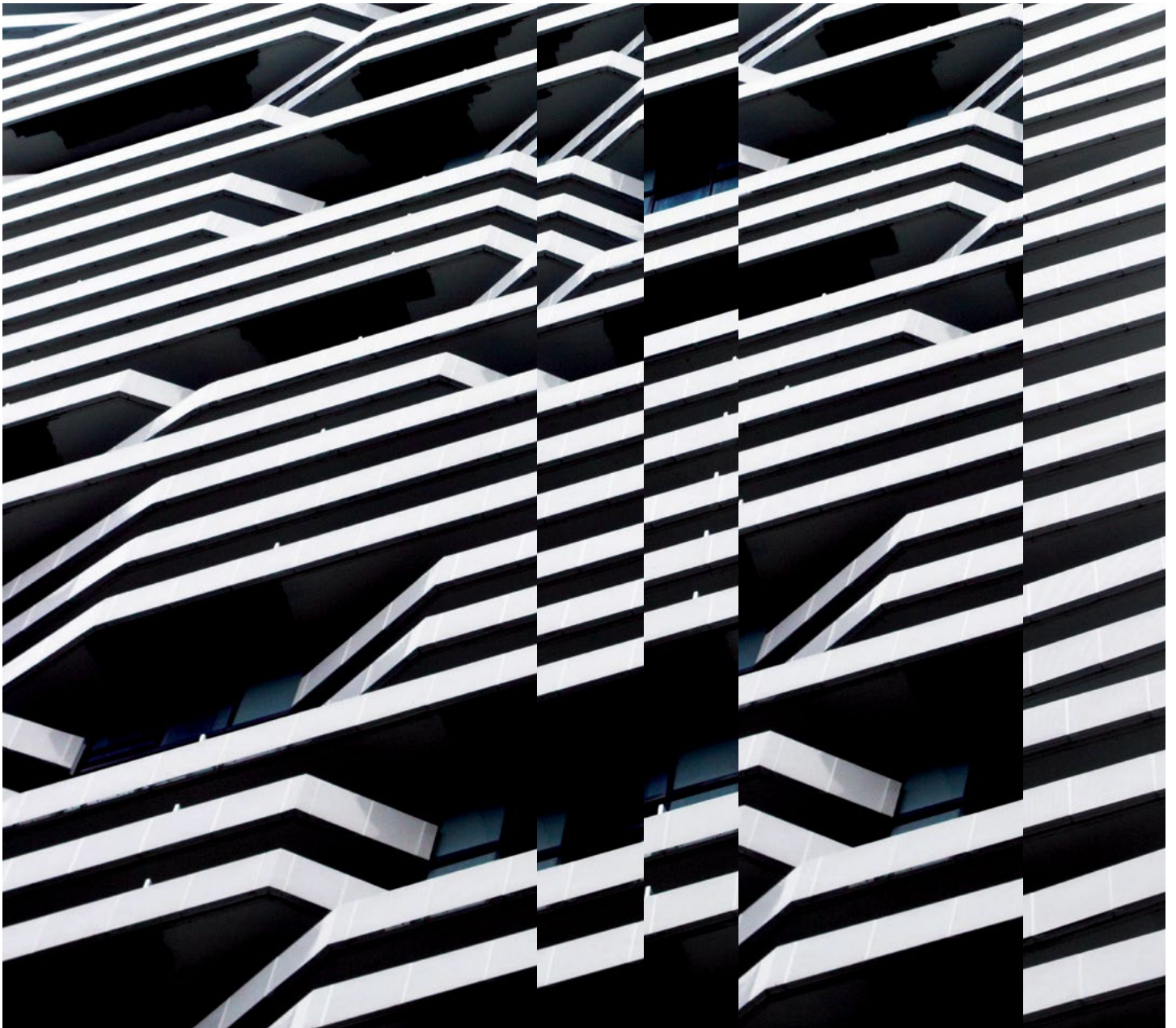
Top risk concerns differ between countries due to geographic, demographic, and other circumstances; institutional setups vary according to constitutional necessity or political decree; and solutions are more or less viable due to economic capacity, cultural acceptance, and enforcement ability. Moreover, government maturity levels in this field inevitably vary. While most advanced economies have been developing and refining approaches for decades, emerging and developing countries are increasingly mindful of their exposures to large risk events and the value that disciplined, evidence-informed decision-making can bring to the apparatus of government.

Exhibit 1: Key questions for every level of government



Our views derive from a range of sources. We have helped individual governments enhance risk governance and crisis preparedness capabilities, assisted national and international authorities in their handling of banking crises, and advised multinationals and critical infrastructure providers on how to underpin their strategic ambitions with appropriate risk management arrangements. Moreover, we have for many years been deeply involved with the OECD’s High-Level Risk Forum, which works with risk managers at the center of government to explore critical risk challenges and effective national-level responses; and we are also a long-term partner with the World Economic Forum on the annual Global Risks Report.

# Determining the most material risks



Deciding where to prioritize risk-management efforts is fraught with difficulty. To understand what might be most damaging, it's crucial to examine threats through different time frames, appreciate the dynamics of each risk, and incrementally build analytical sophistication.

## A STRATEGIC FRAMEWORK

Governments should seek a full, candid view of the critical risks to which their jurisdiction is exposed, regardless of whose responsibility it is to manage them and the challenges of aligning on, and implementing, an effective response.

Categorizing risks both by their origin and by their attributes provides transparency on the diversity of risks and acts as a useful counterweight to the pressures of recent events and political agenda that can skew resources excessively towards particular risk types (see Exhibit 3 on the next page). It helps balance the urgent with the strategic: in other words, near-term concerns for citizen safety and business disruption against longer-term considerations relating to national security and economic competitiveness; or, from

another perspective, unique local challenges against international commitments (such as the Sustainable Development Goals).

To develop context around these risks, advanced economies (such as the US and the UK) often conceptualize their risk agenda over three timelines (see Exhibit 2 below). They have a national security strategy with an outlook of between five and 20 years (or more), a national risk assessment exercise with a time horizon of between one and five years, and a crisis anticipation function that briefs on critical concerns for the coming months. In principle, this enables governments to formulate a long-term investment agenda, build capabilities and strategies for priority known concerns, and respond promptly to sudden shocks or rapidly deteriorating conditions.

Exhibit 2: Risk assessment timescales

	<b>CONTINGENCY PREPAREDNESS</b>	<b>NATIONAL PLANNING ASSUMPTIONS</b>	<b>NATIONAL SECURITY STRATEGY</b>
<b>OUTLOOK</b>	<0.5 year	0.5 - 5 years	5 - 20+ years
<b>RISK MANAGEMENT OUTPUT</b>	Situational awareness warnings	National Risk Assessment	Horizon scanning and foresight

OUTCOME

**PLANS, PRIORITIZATION, INVESTMENT, CAPABILITY MATCHING**

Source: Marsh & McLennan Advantage



Exhibit 3: A taxonomy of common national-level risks

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

Source: Marsh & McLennan Advantage, building on national risk registers. Placement of risks may vary according to national circumstances

## RISK CHARACTERIZATION AND “SENSE-MAKING”

Each of these three time horizons demands a different approach to defining risks and giving shape to plausible unwelcome scenarios.

Foresight and horizon-scanning exercises play a vital role in appraising the evolution of the long-term risk environment and slow-burn issues (as in Singapore). Analyses often take the form of extrapolating current, known risks over longer time periods against expected demographic, climatic, and other changes – seeking to identify potential inflection points, runaway effects, or the crossing of thresholds of acceptability. An alternative approach involves envisaging new risks and shocks triggered by the convergence of different megatrends, then working back to the underlying drivers or conditions.

For more immediate contingencies, including fast-onset events, the effort often centers on making sense of multiple weak signals or one or two strong data points that lack proper contextual validation. In these situations, the challenge is to balance the desire to construct a story as a platform for response with the need to be wary of assumptions that may misconstrue how the emerging crisis might evolve.

The methodology of national risk assessments falls somewhere in between. In this central pillar of national risk frameworks, strong risk characterization is an essential foundation for assessing potential impacts, determining materiality, and analyzing response options. The exercise needs to embrace the deep uncertainty, innate variability, and systemic nature of many national-level risks.


Risks should be unpacked in several ways:

1. Delineate the different possible manifestations of the risk – for example, large cyberattacks may take many different forms
2. Identify which parts of the population or economy might be most affected by incidents, via first- or second-order effects

3. Appreciate for each manifestation the likely trajectory of a crisis – how fast it might materialize, how long it might last, what might accelerate arrival or amplify impacts
4. Consider the factors that may make the risk increase or subside in the coming years

Constructing “reasonable worst-case” scenarios makes these risks more tangible. Although scenarios may not cover every eventuality, they aid in sizing the potential damage and enable a more rigorous exploration of spillover effects. They are also helpful for communications purposes and can underpin the tabletop testing of responses. While persistent “what-if” questioning is vital for thinking through transboundary impacts, highly elaborate scenarios can generate modeling challenges for quantification efforts. Nonetheless, it’s often worth considering the correlation between possible risk events; at the very least, never assume that two crises can’t happen at the same time or that bad things only happen when the economy is doing well.

Being able to access and harness the wealth of available asset, risk, and incident data strengthens the case for policy decisions in both crisis and non-crisis situations. Of course, scanning, aggregating, and synthesizing data of different types requires not only the right information technology framework, but also an organizational culture receptive to the insights derived and committed to using them quickly and effectively.



Constructing  
reasonable worst-case  
scenarios makes risks  
more tangible and  
acts as a framework  
for decision-making

## IMPACT ANALYSES

The mission of government requires the materiality of risks to be examined through various lenses. Damage criteria can range from the physical suffering of individual citizens through to a decline in international influence; it may also include outcomes that undermine the fabric of society, impede economic activity, and erode environmental sustainability (see Exhibit 4). These criteria and sub-criteria implicitly reflect both the values of a country's leadership and the nation's strategic priorities.

Putting this framework into practice in risk assessment exercises is often challenging, given likely data shortages, analytical impediments, resource constraints, and conflicting perspectives. Analyses should calculate or assign probability to each reasonable worst-case scenario, but avoid hastily dismissing improbable (but still plausible) narratives as history provides evidence of many such shock events having actually come to pass. Impact assessment work must not only facilitate the scoring of each risk against the different subcriteria, but also permit scores to be aggregated across the framework. Weighting subcriteria or assigning materiality thresholds may feel invidious, but it's usually preferable to omitting types of impact that may not be of top concern. The presence of these issues in the assessment framework can be useful for response planning at individual sectoral or local levels.

Assessments need to look through the behavior of the major risks to the vulnerability of what might be affected. This requires the mapping of critical infrastructure facilities and systems, understanding the dependencies between different infrastructure systems, and appreciating how failures might compromise vital services, economic activity, and the general functioning of society. This is as applicable to the capacity and preparedness of healthcare facilities to deal with major disease outbreaks as it is to large-scale power outages or a wide-ranging cyberattack.

Of course, vulnerability does not always equal risk, as some infrastructure assets are more critical than

---

### Exhibit 4: Criteria for assessing risk impacts on vital national interests



#### HUMAN SUFFERING

- Deaths, injuries, and illness
- Evacuation from homes
- Psychological stress



#### SOCIETAL DISRUPTION

- Supply failure for key goods and services
- Public disorder or instability
- Infringement of rights and liberties



#### ECONOMIC SHOCK

- Damage to assets and infrastructure
- Reduction in business activity and growth
- Investor and lender uncertainty



#### ENVIRONMENTAL EROSION

- Long-term ecological harm
- Decline in agricultural etc. productivity
- Loss of cultural assets



#### POLITICAL WEAKNESS

- Breach of territorial security
- Dwindling capacity to govern
- Deterioration in international credibility

---

Source: Marsh & McLennan Advantage, reflecting on national risk assessments

others. Even among those with the “critical” label, distinctions must be made: It’s not always the assets that serve the largest number of people or key societal or industrial functions that are of most concern, it’s those that can’t easily be substituted in a crisis. To prioritize resilience efforts, countries often grade their infrastructure, either by asset importance (Switzerland) or by the consequences of failure (the Netherlands). In France, an objective review of infrastructure resulted in a very significant reduction in the number of assets designated “critical.”

Assessments should acknowledge the likely change in exposures over time: Clearly, a situation in which, over a period of years, risk is likely to increase while resilience is likely to decline should raise alarm bells. In the context of specific scenarios, for some risks it’s important to anticipate actions (such as mass flight or panic buying) that groups of people might take both in the run-up to an incident, during a crisis, or in the aftermath – which may mitigate damage or exacerbate it. Moreover, analyzing the likely time to recovery (defined in different ways) is key to being able to contain the fallout and re-establish normality.



Governments seeking to improve their risk assessment activities often need to make trade-offs between the range of risks covered, the degree of analytical sophistication, and the ability to easily repeat analyses at desired intervals. However, capacity can be built over time. Risk assessment roadmaps that start with a broad view of risks and initially shallow analytics are good for stimulating cross-government discussions but will ultimately lack traction in budget allocation processes due to insufficient financial rigor. Those that target specific areas, with a view to expanding scope over time, may achieve rapid acceptance at an early stage but find themselves exposed to unconsidered risks or the implementation of parallel, unconnected processes elsewhere in government. Foresight capabilities should be used to challenge national assumptions and aspirations, not just to highlight opportunities.



# **Mobilizing government capabilities**

Governments need an effective ecosystem focused on resilience to critical risks. A centrally positioned national risk unit can engage stakeholders across government, set expectations for risk assessment and mitigation, help resolve uncertainty in public policy, and galvanize expert resources in times of crisis.

## CENTRALIZED OWNERSHIP

A risk unit at the heart of government can generate a coherent view of different risks, types of impact, time horizons, responsibilities, and response planning. With a strong remit, operating model, and relationships across the public sector and beyond, it can blend rigor, consensus, and agility in the pursuit of national resilience.

In their narrowest incarnation, national risk units focus on civil contingencies, especially natural disasters. In this model, security matters are wholly reserved for counterintelligence agencies, law enforcement bodies, and defense forces; economic risks are retained by the Ministry of Finance (or equivalent), central banks, and regulatory bodies; strategic sectoral challenges are the responsibility of individual line departments. This approach has advantages for managing the flow of sensitive information and an operational logic that aligns risk oversight responsibilities with departmental mandate. At the same time, taking this siloed approach to the extreme often leads to narrow thinking and stovepipe solutions.

In many advanced economies, governments have recognized that national risk units with a broader mandate stimulate richer analyses of causality, interconnectedness, and consequence, and this gives rise to a more thorough appreciation of mitigation options. This is valid even when the primary focus of the national risk unit remains citizen welfare and the general

functioning of social and economic infrastructure (see Exhibit 5 on the next page). Preparedness for malicious human acts remains in scope, even if the specifics of upstream, threat-based intelligence remain confidential. Moreover, units in some countries actively reflect on issues beyond national borders – for example:

- The safety of citizens abroad in the face of life-threatening situations (as in Sweden);
- The vulnerability of dependent infrastructure in partner countries (Switzerland);
- The possible consequences for national security of crises in neighboring or distant fragile states (the UK);
- The resilience of international regulatory and legal frameworks (the Netherlands).



Siloed responsibilities for major risks can result in a narrow understanding of impacts and sub-optimal solutions

---

Exhibit 5: The focus of national risk units



**National defense and counterterrorism**

- Military capabilities
- Intelligence services
- Specialist threat response



**Physical infrastructure/ services reliability**

- Energy and water
- Transportation
- Communications
- Financial operations
- Healthcare
- Food supply



**Business and citizen resilience**

- Strategic sectors
- Large employers
- SMEs
- Stable households
- Disadvantaged/ at risk groups



**Economic stability**

- Fiscal, trade, and monetary policy
- Prudential regulation
- Long-term investment

Source: Marsh & McLennan Advantage

---

What does this more coherent approach look like operationally?

While merely receiving and compiling the outputs of work done elsewhere is less than satisfactory, it's rarely sensible or realistic for risk units to seek a remit for all risk assessment and response planning efforts. Not only would they lack expertise and data on the different risks but also buy-in from line departments (who necessarily own the risks). More viable is a middle ground that involves setting standards for assessments; training risk leads in line departments to build capacity; convening discussions to enrich analyses and responses; and facilitating ways forward where there are competing perspectives.

## **A SMOOTH-RUNNING AND NIMBLE ECOSYSTEM**

Good coordination between key participants at all levels of government is critical for achieving country-level resilience. At the very least, the national risk unit or

equivalent should align the roles and interactions of risk leaders in different government departments, specialist agencies, and emergency response providers (see Exhibit 6 on the next page).

Often national risk units are mandated to draw on a broader network through ad hoc or standing forums that engage local authorities, critical infrastructure operators, non-government experts on individual risks, and providers of risk finance. For example, confidential exchanges on attack trends between government cybersecurity experts and critical-infrastructure operators (individually and as a group) help counter some of the information asymmetries associated with state-affiliated advanced persistent threats. And in an emerging pandemic crisis, it can be essential to know the key people to draw in to discuss the possible trajectories of the virus and the capacity of medical facilities to cope.

Engaging diverse views enhances both the national-level risk view and ownership at departmental, sectoral, and local levels. Experts and stakeholders

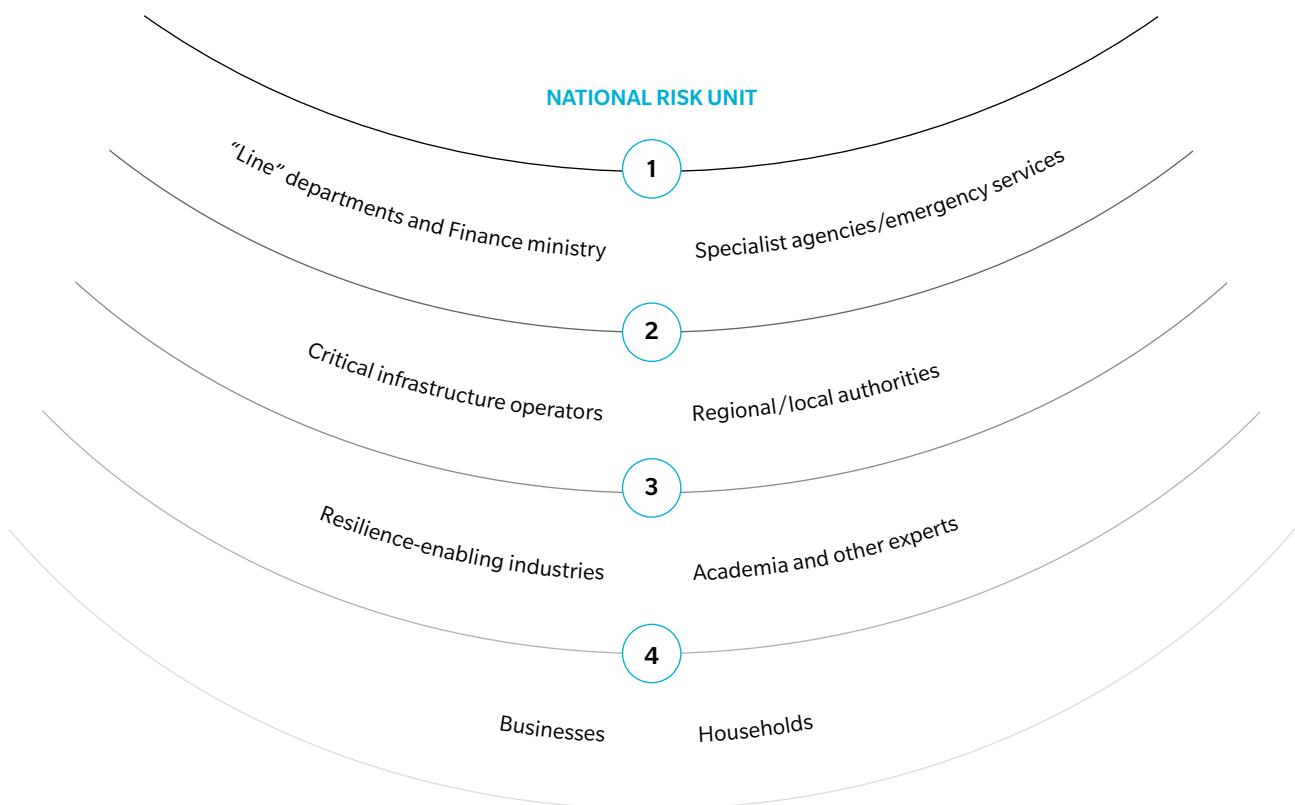
should inform risk assessments and scenario generation, appreciating how different groups might be impacted. They can also support response choices, validating expected benefits and flagging possible collateral damage or unintended consequences over time. Different vantage points also enrich sense-making exercises in emerging crises, thereby averting premature lock-in to instinctive courses of action.

An ecosystem view of national and societal resilience capabilities is integral to developing investment and mitigation priorities. In the first instance, this means analyzing the (mis)match between the risk

exposure of different entities and their current or likely future resilience, based on the availability and affordability of effective solutions. This leads to some fundamental questions:

- What can or must be done by the public sector (at a national or local level), and where can or must the private sector support, or even deliver?
- Where should the government avoid creating moral hazard, and how can it wean entities away from unsustainable assumptions of unlimited or repeated government support?

Exhibit 6: National resilience stakeholder ecosystem



Source: Marsh & McLennan Advantage



A capabilities-based approach is important for ensuring adequate crisis response, and several leading economies are currently analyzing the adequacy of national capabilities (whether centrally or locally situated) to address the common consequences of priority hazards and threats. The effort includes exploring the capacity of emergency services to respond to defined crisis scenarios and the scale or type of event that would overstretch them. Subordinate challenges range from the ability to deploy the right technical expertise in specialist crises (chemical or biological, for example) to the speedy recovery of essential services (such as power, water, and communications) following extreme weather events. Assessments should also acknowledge the scope for leveraging volunteer enthusiasm, which often proves invaluable in the aftermath of disasters.

Well-founded, well-coordinated, and well-communicated crisis response arrangements are vital for both delivering effective solutions and securing public confidence. Decision makers must demonstrably engage with expert intelligence; optimistic viewpoints should be challenged hard by contrarian perspectives and standard plans by the exploration of possible second- and third-order effects. Regular updates should establish authoritative sources of information in the face of misinformation and disinformation that may

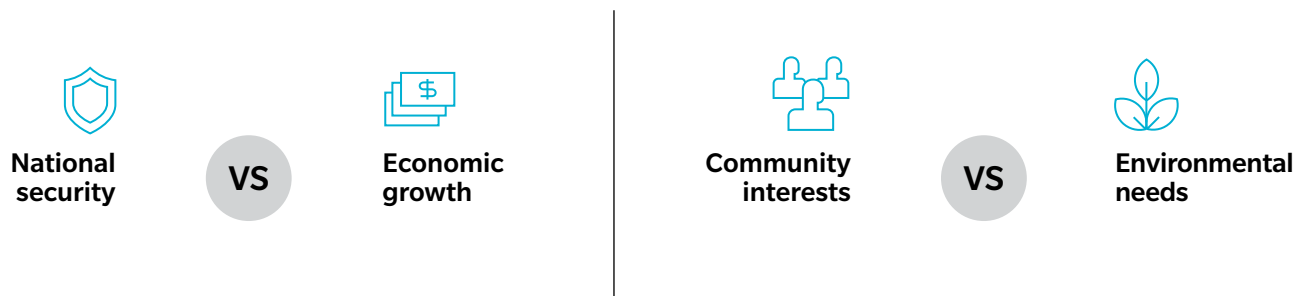
be spread through social media. While leaders should not fear adjusting response strategies in the light of new information, they will be more convincing if they do so within the context of a clear set of principles or framework.

Impacts that cascade across sectors and dependencies that cross national jurisdictions can be particularly difficult to anticipate. Crisis management drills (whether tabletop or on the ground, and sometimes with the participation of national leaders) can deepen trust between different participants and indicate where operational interfaces, protocols, and information flows may need refining. Recent European Union exercises have used this approach to explore novel cyberattacks and hybrid threat scenarios instigated by foreign states.

## **AUTHORITY, OVERSIGHT, AND ACCOUNTABILITY**

Notwithstanding their ability to build buy-in, national risk units have little inherent power to define national risk management priorities, set targets, and hold other parts of government accountable. The active support of senior bureaucratic and political leadership structures is essential for overcoming departmental differences and marshaling effort.

Exhibit 7: Common decision trade-offs



Source: Marsh & McLennan Advantage

Strategic policy conundrums take different forms (see Exhibit 7 on the previous page). For example, many governments are struggling to reconcile the competing imperatives of national security and economic growth – this is playing out in dilemmas about the use of foreign technology providers in critical national infrastructure. Elsewhere, it’s necessary to make trade-offs between community interests and environmental exigencies – often in the context of planning for floods and drought. Other quandaries may focus more on the quantum or source of investment in resilience – for protections (barriers to protect coastal cities against storm surges), contingency planning (stockpiling medicines against emerging pandemics), and preparedness (resources for the intelligence agencies to support counterterrorism).

At the same time, governments should also regularly assess the effectiveness of national resilience capabilities and measures, especially against the backdrop of an evolving risk landscape. This is inevitably easier when

backtested against historic incidents that have severely tested the country (such as a major terrorist attack or flood). Evaluations that can be publicly undertaken and reported on are helpful for justifying expenditures and acting as a foundation for adjusting policy frameworks and response capabilities, as well as potentially supporting national healing processes.

All the same, stress tests may struggle in the face of novel, technology-based risks (from pervasive fake news to poorly controlled artificial intelligence) or even traditional-sounding risks (such as public health emergencies or food security challenges) that may manifest very differently to previous instances.

Moreover, while planning efforts may focus on the nation at large, today’s more complex risk environment also warrants fresh thinking about scenarios that threaten the continuity of government operations and the viability of response plans should government employees or infrastructure (or both) be incapacitated.



National risk units are invaluable for helping governments take a holistic view of the most significant threats to citizens’ wellbeing and striking an appropriate balance between challenging departmental assumptions and building trust, consensus, and commitment on the path forward. By shedding light on the gap between current and required responsive capabilities, they can catalyze the innovation and momentum required to build resilience to both near and long-term risks. National risk units must also engage early on difficult emerging risk topics, even those that may at first seem to be outside their remit.

# Implementing strategic initiatives



Working towards sustainable resilience requires both meaningful investment and cultural change. Progress involves finding new ways to share responsibility across national and local government entities, public and private sectors, and asset owners and users.

## **FISCAL AND FINANCIAL RESILIENCE**

Many of the hazards and threats listed earlier in Exhibit 3 present significant fiscal and financial risks to nations, businesses, and households. Although broadly recognized, this knowledge doesn't reliably inform decision-making by these entities, leading to a persistent reliance on disaster recovery financing at the expense of up-front measures that would lessen impacts.

Government accounting for critical risks is often less than systematic. Many processes often assess the direct losses from historic disasters rather than the longer-term economic impact, and report on payouts for specific incidents or by specific authorities rather than expected longer-term liabilities from those events. At the same time, few countries attempt to quantify future disaster scenarios as economic outcomes, and fewer still use such analyses to inform fiscal risk assessments and financial planning. This can result in inadequate budgeting for contingent liabilities, sometimes resulting in the public purse paying an ever-higher share of the costs of increasingly expensive disasters (as with windstorm events in the US over the past 30 years) and event impacts that are much more consequential for national stability than anticipated (as with drought and floods in Argentina in 2018). Moreover, the ability of many jurisdictions to cushion fresh crises is constrained by historic high levels of public and private debt.

Either from a legal obligation or an implicit commitment, post-disaster financial assistance is often provided to households (and sometimes businesses) whether or not they have taken steps

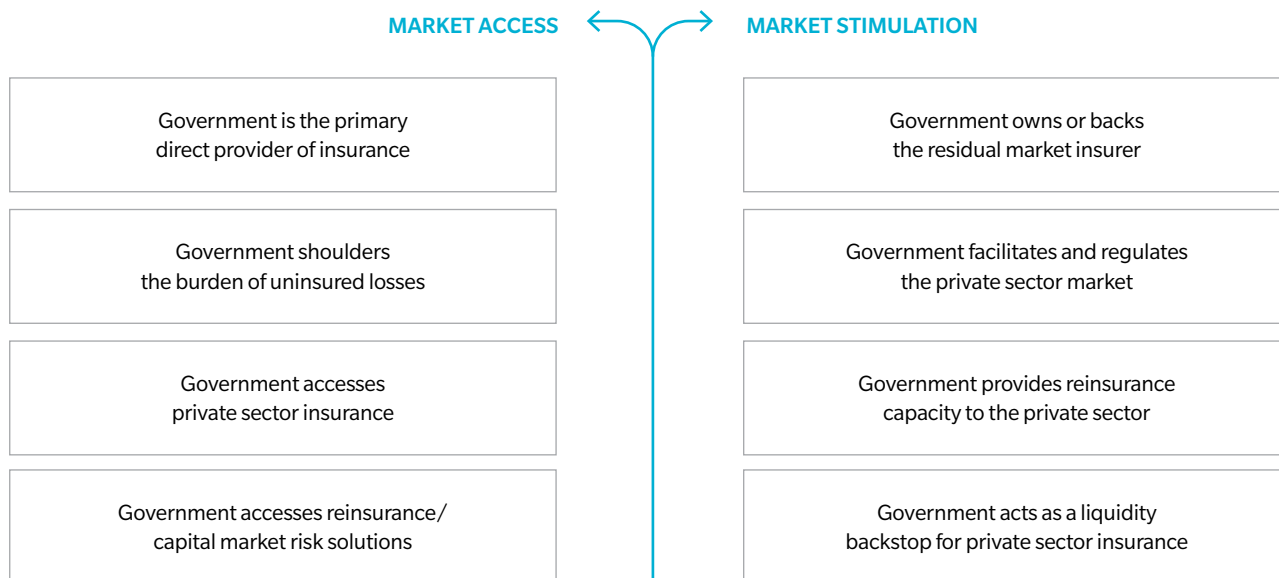
to protect themselves. Moreover, national governments struggle to control liabilities relating to assets and infrastructure in the hands of subnational authorities – cost-sharing responsibilities are often unclear or else constrained financial capacity at the local level renders them unviable.

Nonetheless, a variety of financial measures are in use. Some countries maintain reserve funds (Canada, Chile) or contingency budgets (South Africa, Japan), while New Zealand's strong net debt-to-GDP target seeks to lessen the impact of major events. Governments occasionally reach into private sector markets to insure public assets (the US at local level) or issue catastrophe bonds (Mexico, the Philippines) – often to boost funds set aside for major incidents. Governments promote, mandate, and sometimes provide insurance to enhance responsibility among businesses and households (see Exhibit 8 on the next page). Parametric insurance products are increasingly on radar, while strong public-private partnerships have led to pooled solutions and backstop arrangements for assets (in flood-prone areas, for example) or risk types (nuclear radiation leakage, terrorism) for which it would otherwise be hard to secure coverage.



**Governments have  
many options to  
protect balance sheets  
against contingencies**

Exhibit 8: The role of government in insurance against catastrophic risks



Source: Guy Carpenter, Marsh & McLennan Advantage

However, by underpricing risks and offering low payouts, some government insurance interventions have given households a false sense of security and distorted market capacity without achieving the higher levels of take-up anticipated or customer investments in mitigation. Against this backdrop, an explosion of data on key perils and advanced analytical capabilities are opening the door for new public-private arrangements that can replace outmoded programs.

The advantages of sovereign risk transfer are many. Aside from the benefits of a more diversified funding base, guaranteed access to external funds provides greater budget planning certainty and liquidity in the aftermath of catastrophes (such as earthquakes, wildfires, and floods), thereby mitigating the need to divert national reserves and lightening sovereign rating and foreign exchange impacts. Operationally, it may also speed payouts to affected parties and enable faster rebuilding. By contrast, post-hoc emergency

fundraising (such as national budget reallocation, tax hikes, and loans from multilateral institutions and individual countries) may not only take time to arrive but also spark societal discontent and international political difficulties due to the associated terms and conditions.

## INFRASTRUCTURE INVESTMENT

While mitigating the financial impact of major incidents is important, it's also necessary to take a precautionary approach to physical infrastructure resilience, especially where vulnerabilities are likely to increase over time. Analyses repeatedly suggest that pre-emptive investment in defenses and adaptations is several times more efficient economically than post-incident expenditure on disaster recovery; moreover, such action also helps lessen the suffering and human loss in catastrophic events. Governments that can apply cost-benefit analyses (such as the US and France) will have a stronger view on worthwhile investments (see Exhibit 9).

---

Exhibit 9: Risk-based considerations for targeting infrastructure resilience investment



**OBJECTIVE**

Asset protection?  
Overall system viability?  
Consequence containment?



**VALUE**

Minimization of defined concerns?  
Avoidance of collateral impacts?



**METHOD**

Damage resistance?  
Threat absorption?  
Fast bounce-back?



**TIMING**

In initial design?  
While retrofitting/upgrading?  
During decommissioning?



**IMPLEMENTATION**

Incremental adaptation?  
Transformational effort for lasting impact?



**ALTERNATIVES**

Supply-side redundancies?  
User-oriented resilience?

Source: Marsh & McLennan Advantage

---

Investment must be directed effectively, especially in the context of climate change adaptation. Expenditures that seem worthwhile over a 10 or 20-year perspective may not be justifiable on a longer horizon. Moreover, while enhancing the protection of critical assets remains a clear focus, unavoidable contingencies mean that supply-side systemic redundancies (for example, in the form of capacity markets for electricity generation), national stockpiling (oil and gas), and provisional contracts (with logistics companies for transporting supplies in an emergency) are often essential.

Governments are increasingly calling on citizens and businesses to be prepared and adapt current practices. Actions may take the form of lower water consumption requirements, access to backup generators, and the storage of emergency supplies, among other measures. Low-cost expenditures by households and businesses can yield savings over the long term, especially when coupled with insurance premium reductions.

Physical resilience initiatives often take the form of large-scale projects and involve complex, politically fraught, infrastructure transitions. While some schemes by their nature can be centrally planned and delivered (such as desalination and water reclamation projects in the UAE), others (such as anticipating sea level rise in large coastal cities) face an array of competing vested interests that

impede the development of coherent solutions and delay investment.

Done well, master planning and extensive stakeholder engagement can yield strong results (as with the “room for the Waal” project in the Netherlands, a country that each year invests 1.2 percent of GNP in flood prevention); where key issues remain unresolved and implementation weaknesses abound, outcomes can be deeply unsatisfactory.

The process for financing resilience in new infrastructure is, on the face of it, relatively uncomplicated. Governments can simply embed resilience standards or future-proofing obligations into tender processes, where appropriate. However, while this ensures a level playing field between bidders, government project sponsors may need to balance this expectation with other ambitions – in other words, shifting risk across the life cycle of the asset to the private sector, driving a hard bargain to get value for the public purse in co-investments, and ensuring acceptable price levels for end users in due course. Projects where the relationship between revenue opportunities and costs suggest a poor return on investment are unlikely to prove attractive to potential bidders. Those who persevere may do so with an eye to renegotiating terms, cutting corners on obligations, or underinvesting in maintenance in due course.

Securing resilience investments from operators is often more challenging in the context of pre-existing infrastructure. As key risks appear to intensify, governments are seeking to raise standards or advance resilience initiatives that operators would rather defer for commercial reasons, as incurring such costs would likely affect the company's near-term financial performance. Resistance is stronger when an operator is asked to bear costs from which other players in the ecosystem (or interdependent ecosystems) would benefit without charge. Moreover, in regulated sectors there may be little opportunity to pass on additional costs to users.

While some governments are considering tougher regulatory measures where voluntary frameworks seem outdated or unresponsive, others are exploring new partnerships and incentives to increase private sector operator investments. They are also developing new cost-sharing rules and co-financing arrangements with sub-national authorities to strengthen local ownership of the resilience agenda.

## **BROADER POLICY OPPORTUNITIES**

A more complex risk environment is obliging governments to intensify, refashion, reverse, and develop new policy measures to support national security and resilience frameworks. At the same time, the quest continues to nurture resilient societies from the bottom up, an exercise that is all the more pressing when the sense of communal cohesiveness is at a low in many countries.

Well-enforced land-use planning regulations and building code standards remain fundamental to mitigating natural disaster damage, but more radical measures (such as "managed retreat") should be seriously considered when protection or rebuilding measures are no longer viable or affordable options. In other critical areas, such as countering rapidly declining biodiversity, soil quality erosion, ocean cleanliness, and escalating migration crises, reversals of long-held approaches and new forms of international cooperation are necessary.

But it's perhaps with reference to rapid technological advances that the greatest innovation is required. Many countries have introduced, or are working on, measures to curb systemic impacts from large cyberattacks; to prevent undesirable consequences of multiple new technology applications (such as artificial intelligence); to govern the growing concentration of power in the big technology players; and to thwart the ability of foreign states to exploit domestic research and development excellence for their own long-term geostrategic advantage.

1. High levels of uncertainty related to the trajectory of emerging risks mean that action is often delayed until some response options are no longer on the table and the cost of implementation is (or seems) that much greater
2. Many of the responses to risks involve a manifestly acute balancing act between economic, security, and sustainability imperatives in the short term, even if those agenda may align on a more distant horizon
3. More fraught international relations have accentuated tension between the goal of strengthening global public goods and the pursuit of national competitive advantage
4. In some countries, less-centrist political agenda have already removed or deprioritized some policy options and increased lock-in to others
5. New resilience priorities inevitably need to confront not only inertia but also interests vested in existing arrangements

To be properly responsive, government decision-making needs to navigate five challenges or trade-offs.

Seeking broad-based resilience, governments are increasingly recognizing the importance of risk communication that can mobilize the broader population, encouraging a subtle glide from personal or family self-interest to community and national benefit. In the

context of natural hazards, this includes protecting homes against extreme weather events, taking prompt action (such as evacuation) in an emerging crisis, and offering help as volunteers in the wake of a catastrophe. In some countries (such as Japan), this expectation-setting has for a long time begun within the formal education system; and many countries along the “Ring of Fire” around the Pacific now use mobile phone-based early-warning systems to spread word quickly about significant earthquakes and tsunamis without arousing panic at every tremor.

Promoting citizen vigilance against malicious threats is equally important. Well-established measures include expecting people to promptly report suspicious packages on transportation systems and in public places, and in the last decade cyber awareness campaigns have repeatedly alerted individuals to the threats both to their own personal data and financial security, and also to the integrity of the organizations for which they work. Sophisticated disinformation or fake news initiatives instigated by local or foreign agents have presented fresh challenges, given their

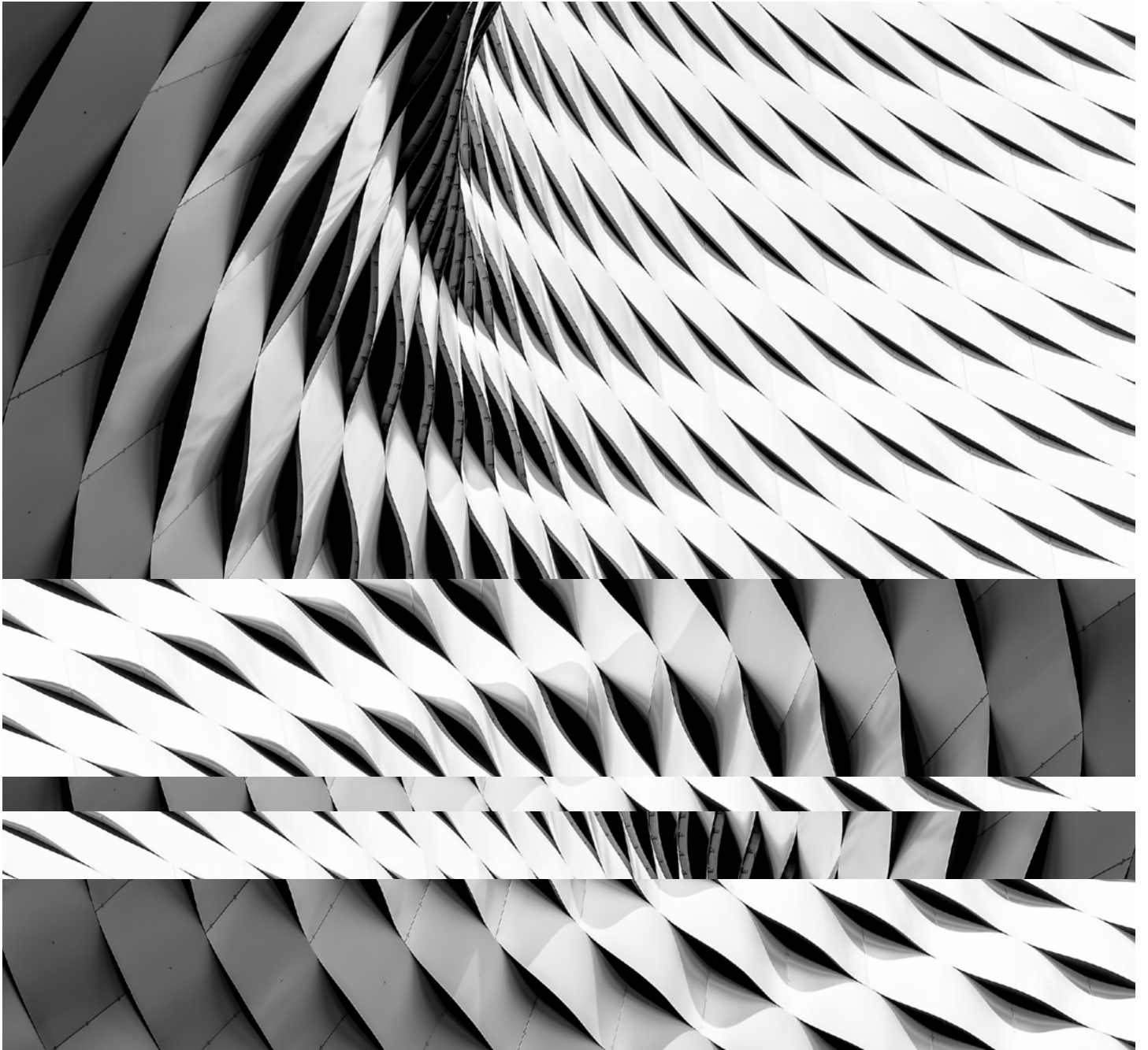
exploitation of the automated protocols of social media platforms to tap into instinctive preferences of users. Despite manifest oversight deficiencies among some key technology players, governments have struggled to identify or deliver interventions that will enhance trust sustainably.

Stirring up popular sentiment against perceived foreign aggressors may be a centuries-old ploy by national leaders to distract citizens from domestic problems, but information-sharing can also be a key stimulus for enhancing resilience. Greater governmental openness (especially among European countries) about foreign interference has been vital for encouraging the attentiveness needed to counter the persistent, low-level aggression that seeks to erode trust in government and the effectiveness of national institutions. The Swedish government’s decision to send total defense pamphlets to every household, advising citizens to be prepared in the event of war, attracted significant attention both at home and abroad.



Pursuing an “all-of-society” approach to resilience involves rethinking established practices and expectations within government and the country at large. It certainly can’t be achieved without the concerted deployment of a wide range of policy levers (including some new ones) in support of clear goals. At the same time, high-quality communication and engagement is vital for achieving cultural change.





# **Innovation, agility, and leadership**

**Bold thinking and determined implementation are vital for overcoming inertia generated by deep uncertainties and competing priorities. A senior-level risk champion empowered to bring together key stakeholders to develop and deliver lasting solutions may amplify national risk unit mandates.**

Government resilience frameworks show evidence of significant progress over the past decade. These structures have embraced a wider range of risks, sharpened approaches to risk assessment and analytics, established new strategic resilience initiatives, and strengthened crisis management arrangements. In doing so, they have consolidated expectations across government departments, developed new relationships with the private sector, and deepened peer networks across countries.

But more remains to be done. As noted in the introduction, new risks have come onto the radar while familiar risks are intensifying, and risk interconnectedness has exacerbated the potential for large, or systemic, impacts. Some traditional solutions are declining in effectiveness or affordability, against a backdrop of more febrile political and societal

conditions. Overcoming institutional blind spots and prevarication is essential.

Resilience frameworks in many countries would benefit from greater ambition, innovation, and agility (see Exhibit 10). This involves engaging more forcefully with upstream root causes rather than just downstream effects and getting fully behind larger initiatives that may produce transformational change. In practical terms, this means better use of foresight work and creative risk scenarios to deal faster and more resolutely with emerging challenges and crises; more rigorous risk budgeting, with a clear view on how solutions will be paid for; a more transparent monitoring of progress; the development of new partnerships; and, more generally, stronger ownership of major risks across all stakeholders within government and beyond.

---

Exhibit 10: Delivering on ambition, innovation and agility



---

Source: Marsh & McLennan Advantage

Without a coherent imperative firmly pushed forward, essential infrastructure schemes may remain on the drawing board, opportunities to hold back emergencies will be lost, and communications exercises will fall on deaf ears. Moreover, failure to resolve increasing tensions between the principle of risk sharing (contributions from the many support the affected few) and growing opportunities for risk-reflective pricing (those facing more risks pay more) may trigger new forms of moral hazard and market failure. Indeed, the protection gap (the difference between economic and insured losses) both globally and in key economies hasn't meaningfully closed in recent decades, and fears are rising that climate change could make insurance increasingly unaffordable for significant parts of the population in some locations, with consequences for regional economic stability as well as household financial security.

How have leading private sector firms adjusted expectations of the risk function to strengthen risk management?

The growing need for companies to grapple more effectively with complex uncertainties and strategic emerging threats has required the chief risk officer to become a nerve center for emerging risks, an innovator in how to characterize and assess them, a commercial expert who can appreciate the potential impact on corporate ambitions, and a strong communicator who can quietly educate senior management and the board to ensure this intelligence informs corporate decision-making, even when the data is patchy, contradictory, or contested. This essential expansion beyond a controls and mitigation agenda to one embracing fundamental adaptation and business-case support offers the risk function a larger role in shaping future corporate priorities and how they are taken forward.

A 2009 report co-authored by Marsh & McLennan and the OECD proposed the establishment of country risk officers. While many of the expectations identified in that report have become part of the mandate of stronger national risk units, only some countries have designated singular, visible, influential leadership. A formal champion of the resilience agenda might stand above departmental interests, form a coherent long-term view, set expectations for responsibilities and the interactions of different stakeholder groups, communicate imperatives widely, and make the case for resilience investments or question proposed budget cuts. The person holding this post would have a vital remit to challenge governmental assumptions regarding current and future resilience, and drive new initiatives that can anticipate and address new, emerging challenges.

As national governments not only grapple with a more problematic risk environment but also undertake massive economic transformation programs, seize new technological opportunities, and respond to climate change, the qualities of innovation and leadership are more important than ever before.

## **AUTHORS**

**Richard Smith-Bingham,**  
Executive Director,  
Marsh & McLennan Advantage

**Alex Wittenberg,**  
Executive Director,  
Marsh & McLennan Advantage

## **CONTRIBUTORS**

This report owes a considerable debt to the reflections of risk and resilience experts in national governments who are grappling with challenges old and new. Many thanks also to the following individuals at Marsh & McLennan for their perspectives on this topic: Daniel Kaniewski, Andrea Federico, Crispin Ellison, Anshu Vats, Jonathan Clark, Charles Whitmore, Ruth Lux, Michael Schwarz, Robert Reader, Chaitra Chandrasekhar, Julia Reffell, and John Drzik.

## **ABOUT MARSH & MCLENNAN COMPANIES**

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 76,000 colleagues advise clients in over 130 countries. With annual revenue of \$17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. 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 wellbeing 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](http://mmc.com), follow us on LinkedIn and Twitter @mmc\_global or subscribe to BRINK.

Copyright © 2020 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.