OECD Reviews of Risk Management Policies

Assessing Global Progress in the Governance of Critical Risks

OECD

LAUNCH VERSION

OECD Reviews of Risk Management Policies

Assessing Global Progress in the Governance of Critical Risks

OECD
BETTER POLICIES FOR BETTER LIVES

Please cite this publication as:
OECD (2018), *Assessing Global Progress in the Governance of Critical Risks*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris.
https://doi.org/10.1787/9789264309272-en

ISBN 978-92-64-30926-5 (print)
ISBN 978-92-64-30927-2 (pdf)
ISBN 978-92-64-30928-9 (HTML)
ISBN 978-92-64-30929-6 (epub)

Series: OECD Reviews of Risk Management Policies
ISSN 1993-4092 (print)
ISSN 1993-4106 (online)

Photo credits: Cover Illustration © Jeffrey Fisher.

Corrigenda to OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*.

Foreword

This report presents an assessment of countries' progress in the governance of critical disaster risks. Governing risks is essential to ensuring national security, and to achieving economic and social resilience and sustainable development. Resilience is the ability to plan and prepare for, withstand and absorb, recover from and adapt to adverse events. Disasters can cause significant economic, social and political damage. Citizens generally have high expectations of governments to protect them from risk. When a disaster strikes, the public loses its trust in government if it is not well prepared. An investment in risk governance can prepare countries, through a holistic approach, to minimise the consequences of disasters, and increase resilience.

Through the community of risk managers in its High-level Risk Forum, the OECD has worked to advance strategic thinking in this policy area. The 2014 OECD Recommendation of the Council on the Governance of Critical Risks offers a strategic framework for benchmarking country progress in the area.

After providing an overview of trends in critical risks (chapter 1), this report analyses progress along the five dimensions of the 2014

OECD Recommendation, including all hazard and transboundary risk governance (chapter 2), critical risk assessments and financing frameworks (chapter 3), critical risk reduction, prevention and communication (chapter 4), strategic crisis management (chapter 5) and transparency, accountability and lessons learned (chapter 6).

The report finds that progress remains uneven. In particular:

- While countries generally have adopted national strategies with an integrated vision and some form of institutional leadership, relatively few countries set priorities and allocate resources through a risk informed process and only few set performance targets.
- Two-thirds of countries have developed a horizon-scanning exercise, but only half possess the formal elements of a national risk assessment and use the results to inform emergency planning.
- Most countries deploy risk communication efforts and most have strategies to manage risk in some of the critical infrastructure sectors, but few map any interdependencies across sectors, and few provide incentives to small and medium-sized enterprises to encourage business continuity.
- Many countries have updated crisis management frameworks, but only half have the capacity to identify novel, unforeseen or complex crises. In countries with designated lead bodies for critical risks, in only half of those can the body report directly or through a minister to the head of government.
- Nearly all OECD countries use the results of risk assessment to inform the public about its exposure to natural hazards, but fewer do so about technological accidents. Nearly all countries try to conduct post-disaster policy assessments, but few show how the results were used to revise risk management policies.

This report is based on a unique cross country survey covering 34 countries carried out through the High Level Risk Forum in 2016. While the report offers a general overview of the results, detailed information and data on specific countries has been made available on the OECD High Level Risk Forum website (www.oecd.org/gov/risk). The survey included 34 of the 39 countries that adhered to the Recommendation, including 32 OECD members as well as Costa Rica and Colombia.

This report is meant to contribute to broader OECD work on promoting resilience. This assessment of global progress in risk governance also contributes to assessing country efforts to build integrated strategies for disaster risk reduction

Acknowledgments

This report was prepared under the auspices of the OECD High Level Risk Forum by the OECD Public Governance Directorate, led by Marcos Bonturi.

The report presents the results of the work of OECD High Level Risk Forum to analyse and assess country progress in the governance of critical risks, through monitoring the implementation of the Recommendation of the Council on the Governance of Critical Risks. This report was led by Jack Radisch (Senior Project Manager), with the guidance of Stephane Jacobzone (Acting Head of the Reform of the Public Sector Division). Contributions to individual chapters were drafted by Cathérine Désirée Gamper, policy analyst (Chapter 1 and Chapter 4), Jack Radisch (Chapter 2, Chapter 3 and Chapter 6), Charles Baubion, policy analyst (Chapter 5), Roberto Schiano Lomoriello, junior policy analyst at the time of writing (Chapter 1) Stephane Jacobzone (Chapter 6) and John Roche policy analyst at the time of writing (Chapter 3). Valuable research assistance throughout the project was provided by James Drummond, Teresa Maria Deubelli, Roberto Schiano Lomoriello and Ariadna Anisimov.

The Secretariat gratefully acknowledges the many officials who responded to the OECD survey on Governance of Critical Risks, and who assisted in the survey design. The secretariat is also grateful to all the experts and participants in the High Level Risk Forum, practitioners from the private sector and civil society, and experts from think tanks and academia who supported the process by identifying and sharing good practices. Special thanks go to the Chair of the High Level Risk Forum, Ms. Tina Gabbrielli for all her valuable insights. Special thanks also go to Bengt Sundelius, Strategic Advisor at the Swedish Civil contingencies Agency, and to Alex Wittenberg, Executive Director, and Richard Smith Bingham, Director Global Risk Center, Marsh & McLennan Companies (Marsh, Guy Carpenter, Mercer, Oliver Wyman).

Liv Gaunt, Raquel Paramo and Stéphanie Lincourt prepared the report for publication. The team is very grateful for assistance provided by Elisabeth Huggard throughout the project.

Table of contents

Tables

Figures

Boxes

Executive summary

The successful governance of critical risks is a strategic investment in preventing deaths, in preserving economic competitiveness and sustainable growth, and in ensuring better lives for the future. This report, based on 34 country responses to an OECD survey, is the first evidence-based analysis of country implementation of the OECD Recommendation of the Council on the Governance of Critical Risks. In developed and developing countries alike, citizens and businesses expect governments to be prepared for a wide range of possible crises and global shocks.

The annual average damages from disasters over the past 30 years amounts to less than 0.2% of gross domestic product (GDP) in all OECD countries combined. More recent extreme events, however, have caused damages in excess of 20% of GDP. The increasing complexity and magnitude of both natural and man-made risks often reveal inadequate co-operation across government, with the private sector and across borders. Analysis of these governance gaps in a wide range of countries yields broad global lessons concerning where to invest in strengthening institutional capacities.

Implementation of the OECD Recommendation remains patchy, and progress is uneven across countries. This report highlights a number of good practices, such as investments made across the risk management cycle, which generally enable impacts of disasters to be kept under control without disrupting the economy as a whole. The report identifies areas with further room for governance improvements in terms of the institutional, policy, administrative and regulatory aspects of risk management.

Key findings

Implementing all-hazards and transboundary country risk governance

Almost all countries adhering to the Recommendation have adopted a national strategy with an integrated vision for the complete risk management cycle – risk identification and assessment, prevention and mitigation, preparedness and response, and recovery and reconstruction. Most countries have also established institutional leadership to drive the implementation of policies pursuant to these strategies. These bodies coordinate the management of critical risks across government agencies and across different levels of government. There is room for improvement, however, as less than half of them set priorities and allocate resources, and just over a third set performance targets. Further, many lead institutions do not have a role in designing policies, nor in monitoring policy effectiveness.

Anticipating risks in order to reinforce preparedness

Preparing society for critical risks requires projecting for a future state that is often different than experiences of the past. Two-thirds of OECD member countries conduct horizon-scanning exercises to forecast the environment in which future risks and threats will occur. Over half of the countries now possess formal elements of a national risk assessment that identify and assess major risks and use the results to inform emergency planning. The analytical approaches to preparing for and anticipating persistent threats − such as illicit trade and its consequences on public safety, health and finances – are less

transparent than those for disaster risks. However, several are advanced in their efforts to understand the linkages between such persistent threats and man-made risks such as terrorism.

Governing disaster risk reduction

Most countries show significant advances in risk communication to inform their populations about exposures to major risks, though the impacts of these efforts are hard to gauge in terms of stimulating investment in self-protection and resilience measures. Also, most countries have enacted strategies and toolkits to manage risks in critical infrastructure sectors. This is important to minimise disruptions to the supply of goods and services due to extreme events. Room for improvement remains to build the capacity for business continuity needed to ensure economic and social resilience. For example, more countries should map interdependencies between different sectors of critical infrastructure, and few countries provide incentives to small and medium-sized enterprises to encourage business continuity development.

Managing crises strategically

Many OECD countries have revised their crisis management frameworks following major disasters. This trend confirms both that the governments recognise the increased complexity of crises and that standard operating procedures in crisis management plans, while fundamental, are not enough to manage "black swan" events. The challenge of managing modern crises is the uncertainty of their consequences. In this respect, nearly all countries have established inter-agency co-operation mechanisms to help make sense of the unknown during crises. However, only one-half of countries have a department or agency responsible for identifying novel, unforeseen or complex crises. Governments need to build the capacity to understand the direction a crisis could take, beyond the immediate and obvious impacts, and communicate this quickly to decision makers. Yet, only one-half the countries with designated lead bodies for critical risks can report directly, or through a minister, to the head of government.

Assuring transparency and continuous learning

Nearly all countries practice transparency with the results of risk assessments, and some even use them to help inform the public about its exposure to major natural hazards. This practice is less common concerning exposures to potential technological accidents. Nearly all countries had conducted post-disaster policy assessments within the previous three years as a tool for continuous policy improvement. In fact, over half the countries communicated these results to the public, but relatively few countries showed how the results were used to revise risk management policies. Most countries support scientific research to improve policies for managing critical risks.

In conclusion, many country strategies are enacted to guide development of risk management policies for all hazards. The effectiveness of these policies is a work in progress. But many examples show that governments do attempt to follow participatory processes and to foster transparency and accountability in the disaster risk management policy cycle. OECD countries are expanding efforts and experimenting heavily, which reflects the strategic importance and growing concern over managing critical risks. Nonetheless, many countries struggle with implementing policies where risk governance cuts across administrative and territorial borders, signalling scope to foster joined-up approaches across government departments. Significant pockets of vulnerability remain, particularly for populations in many of the highly exposed areas. Governments will need

to partner more with civil society and the private sector in the future, if they are to truly ensure safer lives and build more sustainable futures.

Chapter 1. Overview trends in critical risks

This chapter provides a general overview of the global trends in the governance of critical disaster risks. It highlights the context in which countries adhering to the OECD Recommendation on the Governance of Critical Risks have been reforming their policies. The chapter addresses the increasing frequency of natural and man-made disasters which challenges the economy and increases the vulnerability of populations.

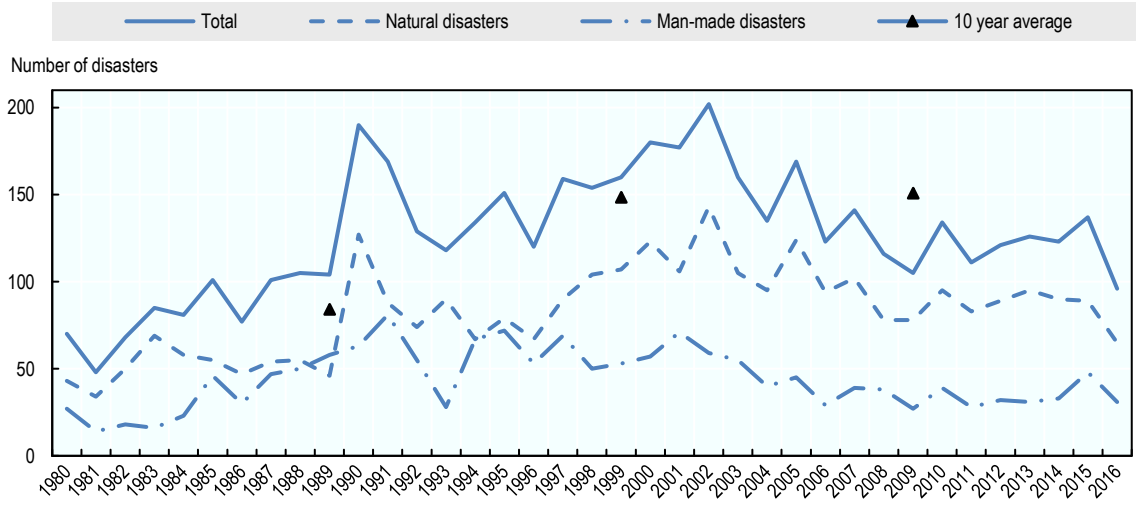
New forms and increasing levels of economic and social vulnerability

The OECD Recommendation on the Governance of Critical Risks recognises significant increases in the frequency of disaster events, the magnitude of their economic impacts, and most importantly the novel forms and transboundary nature of crises that have emerged due to interconnectedness. Quantifying disaster impacts helps analyse these underlying trends over time and reveals the value proposition of effective risk management measures. Between 1980 and 2016, there were 126 disaster events per year on average across the territories of the 34 countries that adhere to the Recommendation and responded to the OECD Survey on the Governance of Critical Risks. The rise has accelerated over each ten-year period (Figure 1.1).[1] Further details regarding the methodology of these metrics can be found in Annex A.

Some of the increase in disaster frequency might simply reflect better monitoring and reporting of the events. Advances in the capacity to map the magnitude, geographic extent and duration of extreme natural phenomena provide important data for a range of disaster risk management stakeholders. The sustained rise in the number of climate-related disasters, however, does coincide with drivers of increased vulnerability such as population and asset concentrations, and infrastructure networks in advanced stages of their life cycle. The average annual economic losses for all countries over the period 2000-10 was USD 77 billion, or nearly triple the losses recorded in the period 1980-99 of USD 27 billion (Figure 1.2).

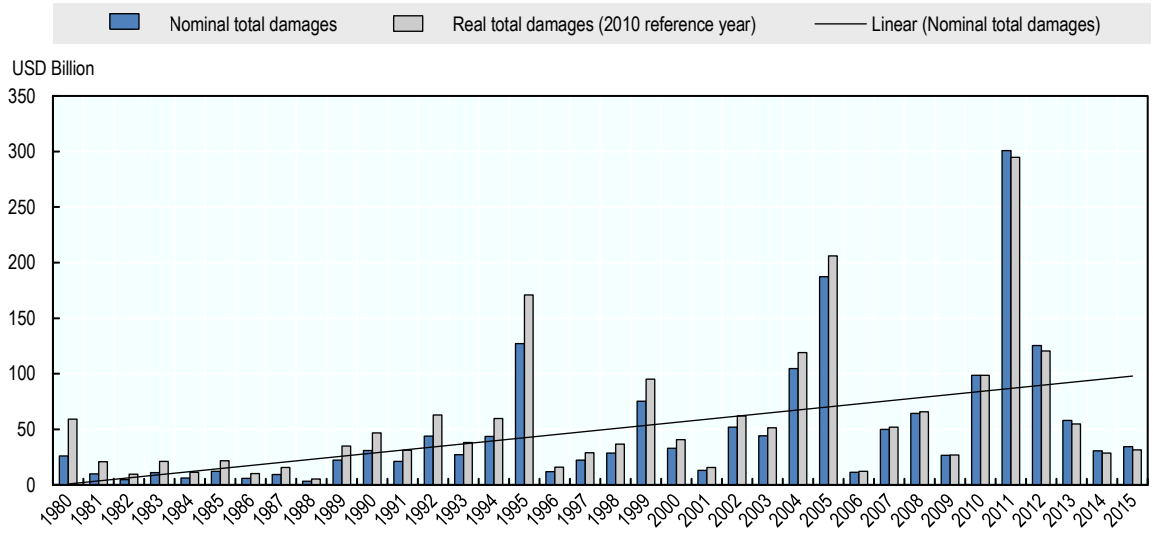
For most countries a high proportion of the total value of annual economic losses every year is caused by just a few largest loss events, which surpass the capacity of local authorities to manage. The cumulative losses from low-impact, high-frequency events are almost negligible in comparison. This finding is key to understanding the need for a whole-of-society approach to risk governance, in which different levels of government, the private sector and civil society co-operate both in scaled-up responses to large-scale events and in efforts to reduce such risks.

Figure 1.1. Number of annual natural and man-made disasters, 1980-2016



Note: Data covers 37 out of the 39 adhering countries: Morocco and Tunisia are missing.
Source: EM-DAT (2017), *The Emergency Events Database*, www.emdat.be; START (2016), *Global Terrorism Database*, https://www.start.umd.edu/gtd.

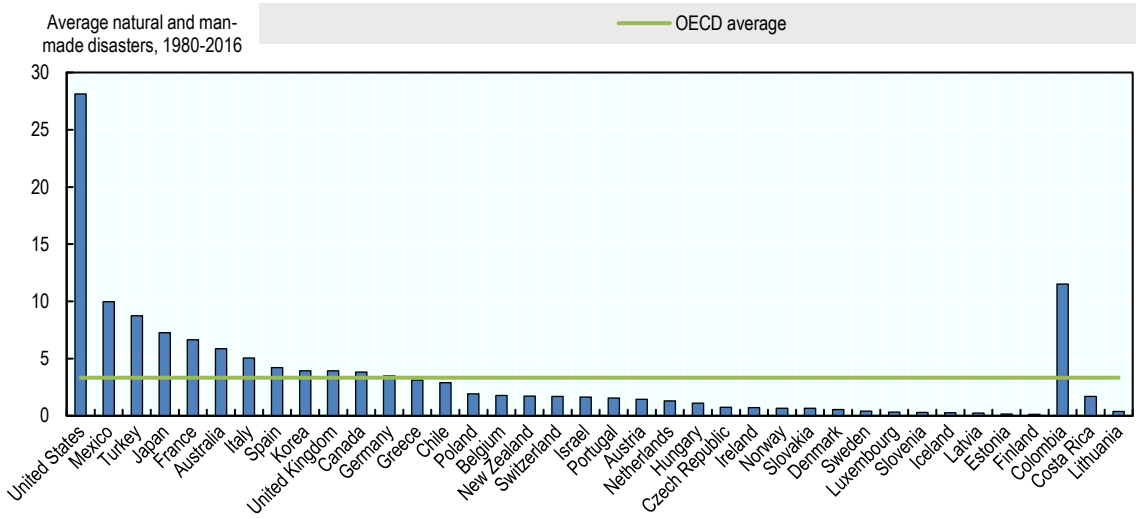
Figure 1.2. Total annual economic damages in nominal and real 2010 USD prices, 1980-2016



Note: Data covers 37 out of the 39 adhering countries: Morocco and Tunisia are missing.
Source: EM-DAT (2017), *The Emergency Events Database*, www.emdat.be.

The aggregate measures of disaster frequency and losses in Figures 1.1 and 1.2 reveal an overall trend upward since 1980. In the last ten years the average number of disasters has decreased, but the average losses have increased, meaning losses are now rising faster than the number of disasters. The high variability from year to year in both measures accurately depicts the uncertainty and unpredictability surrounding such extreme events. These aggregate figures do not, however, convey the variance in disaster occurrence and losses found between countries, between regions and within countries. Among the countries most frequently affected are the Unites States, Mexico, Japan and Turkey (Figure 1.3). For natural disasters, this can be attributed to their large and heterogeneous geography as well as their densely populated urban regions in seismic and coastal areas. Controlling for differences in population size and income levels, for example, helps provide a more refined picture of impacts across countries. Likewise, controlling for exposures to a range of hazards and threats would provide a rough measure to compare progress in managing risks.

Figure 1.3. Average number of natural and man-made disasters per country, 1980-2016

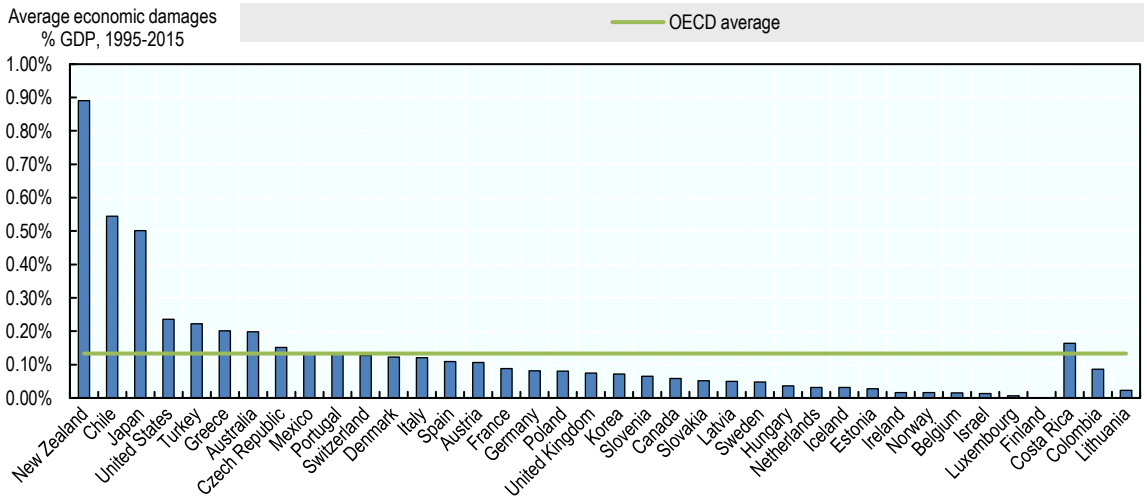


Note: The OECD average is the unweighted average of the 35 OECD member countries. Data covers 37 out of the 39 adhering countries: Morocco and Tunisia are missing.
Source: Author's calculation using data from EM-DAT (2017), *The Emergency Events Database*, www.emdat.be, and START (2016), *Global Terrorism Database*, https://www.start.umd.edu/gtd.

Average annual economic losses due to disasters in a high number of countries are modest relative to aggregate gross domestic product (GDP), but specific major disasters have had large-scale economic consequences, especially in the smaller economies. Over the period 1995 to 2015,[2] the countries with the highest average annual losses due to disasters, in absolute terms, were the United States (about USD 30 billion) and Japan (about USD 20 billion). A different picture emerges when looking at the relation of economic losses to national income (Figure 1.4). The countries with significant seismic activity such as Chile and New Zealand, where urban centres were recently struck by major earthquakes, have the highest average ratio of damage to income. Damages from the earthquakes in Chile in 2010 and in Christchurch, New Zealand, in 2011 equalled around 20% of annual GDP.

If the losses proportionate to national incomes are lower in the larger national economies such as Japan and the United States, the impacts on local communities are nonetheless devastating. From a broad perspective, hurricanes like Katrina caused damages equivalent to only 0.1% of annual GDP, but the estimated USD 125 billion in losses was felt disproportionately in the geographic area and the directly affected population. Moreover, local economic impacts can lead to a considerable drop in regional economic output following disasters, causing substantial negative impacts on regional public finances as well as sectoral imbalances and negative impacts from drops in consumer and business confidence.

Figure 1.4. Average economic damages across countries (% of GDP), 1995-2015



Note: Data covers 37 out of the 39 adhering countries: Morocco and Tunisia are missing. For information on the calculation of economic damages as a percentage of GDP, refer to the technical notes in Annex A.
Source: Authors' calculation using data from EM-DAT (2017), *The Emergency Events Database*, www.emdat.be, and OECD (2017), "Gross domestic product (GDP)" (indicator), http://dx.doi.org/10.1787/dc2f7aec-en.

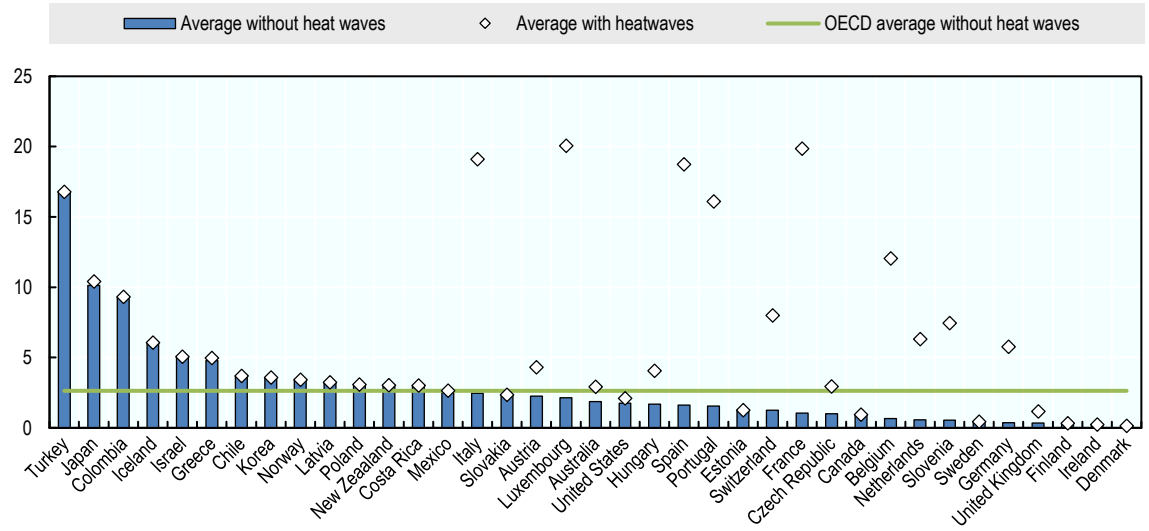
Policies to focus more on economic challenges instead of humanitarian crises

The overall mortality risk due to natural hazards in European countries had diminished significantly until the 2003 European heatwave. This tragic event illustrates the dangers of underestimating risk, as the lack of public awareness and preparedness that partly explains the high number of victims could have been rectified at low cost.

Considering loss of life in relation to the size of a population, for the period 1995-2015 the most affected countries were Luxemburg, Italy, France, Spain, Turkey, Portugal, Belgium and Japan; i.e. they suffered relatively high disaster fatalities as a proportion of the size of their population. In Japan and Turkey, the average number of fatalities were driven up by a few extreme tsunami and earthquake events such as the GEJE (Great East Japan Earthquake), which led to almost 20 000 deaths, and the Marmara Earthquake in 1999 in Turkey, which led to about 18 000 deaths.

Analysing a broader sample of countries shows a trend between lower GDP per capita and a higher mortality rate in disasters. On the other hand, countries with a higher GDP per capita, such as OECD member countries, have seen larger economic impacts, but fewer fatalities (OECD, 2014). This is explained by the investments of wealthier countries in preparedness and prevention countermeasures, such as early warning systems and higher standards for building safety. However, countries with higher income levels tend to have higher asset concentrations in hazard exposed areas, especially coastal regions, which results in a much higher level of economic damages on average per disaster event.

Figure 1.5. Average deaths due to disasters per 1 million inhabitants across countries, 1995-2015



Note: Data covers 37 out of the 39 adhering countries: Morocco and Tunisia are missing.
Source: Authors' calculation using data from EM-DAT DAT (2017), *The Emergency Events Database*, www.emdat.be, START (2016), *Global Terrorism Database*, https://www.start.umd.edu/gtd, and OECD (2017), "Gross domestic product (GDP)" (indicator), http://dx.doi.org/10.1787/dc2f7aec-en.

Conclusions

Many countries are grappling with recurrent and increasingly costly disasters. The risk landscape is changing with increased occurrence of man-made risks and deadly climate related risks such as heat waves. As a result most OECD countries have developed strategic policy frameworks for risk management, and developed new tools and policies to support the governance of critical risks. They have established institutions at a central level to co-ordinate the wide range of actors responsible for identifying, mitigating, preparing for and responding to the complex risks that pervade interconnected economies. These achievements are highlighted in the subsequent chapters.

Gaps in policy implementation remain, however, touching on some of the more advanced and technical aspects of risk assessment, risk reduction, and crisis management. These gaps are identified also in the subsequent chapters. Often these relate to the efforts that sub-national levels of government could make to engage citizens and civil society, but they also involve the private sector, particularly with regards to strengthening business continuity. Therefore, it is important to continue investing in the areas where risk management can yield results, particularly promoting the Recommendation both at central and sub-national levels of government.

Notes

[1] The average number of disasters between 1980 and 1989 was 84; it was 140 between 1990 and 1999, and 150 between 2000 and 2009.

[2] Only data from 1995 until 2015 were taken into account, as GDP data are not available for all countries before 1995 and for 2016.

References

EM-DAT (2017), *The Emergency Events Database*, Université catholique de Louvain (UCL) - CRED, D. Guha-Sapir, Brussels, Belgium, www.emdat.be (accessed March 2017).

OECD (2017), "Gross domestic product (GDP)" (indicator), http://dx.doi.org/10.1787/dc2f7aec-en (accessed 10 April 2017).

OECD (2014), "Boosting resilience through innovative risk governance", http://pac-files.oecd.org/acrobatebook/4214081e.pdf.

START (2016), *Global Terrorism Database*, National Consortium for the Study of Terrorism and Responses to Terrorism, https://www.start.umd.edu/gtd (accessed March 2017).

Chapter 2. All-hazards and transboundary risk governance

This chapter examines the implementation of the first key OECD Recommendation of the Council on the Governance of Critical Risks. The chapter presents policies and practices to promote a comprehensive, all-hazards and transboundary approach to risk governance. It looks at key trends across the countries. Ways to improve risk management and policies appear in the chapter's conclusions.

Good practices and policy tools

Develop a national strategy for governing critical risks

National risk governance strategies are important planning documents that set out how a society as a whole will deliver an agreed vision for the protection and prosperity of its people and values. Of the 34 respondents to the OECD Survey on the Governance of Critical Risks, 28 provided information about their national strategies. The strategies support all stakeholders with responsibilities related to functions of the risk management cycle: risk identification and assessment, risk prevention and mitigation, preparedness and response, and recovery and reconstruction (see Table 2.1). These strategies serve functional governance purposes, for example to articulate, monitor and evaluate risk management policies, as well as to promote the development of emergency plans further to statutory responsibilities.

National strategies for the governance of critical risks can be found under many different titles, and are developed by a variety of central government bodies: from departments located within the offices of a prime minister (e.g. France, Ireland, Italy, Japan, New Zealand, Spain and the United Kingdom) to line or portfolio ministries with responsibility for national security (e.g. Canada, the Netherlands and the United States) or defence (e.g. Israel and Slovenia). A primary governance question is whether these government bodies have the necessary authorities and support to achieve the stated goals of such strategies.

As a practical matter, the administration of risk management policies is dispersed across several line ministries and sub-national levels of government depending on the nature of the risk and the character of the government action to be taken. Policy direction for the management of security risks may come from ministries of justice for example, whereas health ministries may take the lead on policy for infectious diseases. Both risks are potentially critical risks. The extensive variety of critical risks, and multitude of competent actors raises the challenge interagency coordination when an event entails both, for example security and public health risks, such as the explosion of a chemical, biological, radiological or nuclear device. Who takes the lead in prevention and mitigation planning, who takes the lead in response and recovery actions, what roles do any coordinated agencies play, and what must the lead agency and coordinated agencies budget for? These are among the key questions that many risk governance frameworks try to clarify.

The information collected indicates that the comprehensive character of a national strategy is useful to clarify what ministry has front line responsibility for assessment, prevention and preparedness functions for a range of identified critical risks and to enumerate clearly the mechanisms for leadership and co-ordination across government. The challenge facing governments is to achieve such clarity of leadership, coordination and priority setting when the risks are unknown or clouded in high levels of uncertainty. Some countries have found it useful to establish a central authority or identified convenor of responsible authorities to address emerging risks. Even where high levels of uncertainty impede effective preventive action, coordination mechanisms of multi-agency preparedness can compensate to an extent.

Box 2.1. Public administration in the governance of critical risks: Finland

The Security Strategy for Society in Finland clearly identifies the parts of public administration with risk management functions. Finland's government directs, supervises and co-ordinates the securing of functions vital to society, and each competent ministry does the same within its respective administrative sector. In order to facilitate preparedness and to instigate activities, all competent authorities employ their statutory powers.

The Permanent Secretaries have the task of directing and supervising the activities of their respective ministries. They are responsible for preparing the administrative sector's objectives, monitoring their implementation and ensuring the preparedness and security of the sector. The Head of Preparedness in each ministry assists the Permanent Secretary in implementing preparedness and security related tasks.

The Meeting of Permanent Secretaries and the Meeting of Heads of Preparedness are permanent co-operation bodies. When the matters being dealt with so require, the Secretary General of the President of the Republic participates in the meeting of the permanent secretaries. The Meeting of Preparedness Secretaries assists the heads of preparedness.

Source: Ministry of Defence of Finland (2011), Security Strategy for Society: Government Resolution 16.12.2010.

A main challenge in governance of critical risks is that effective risk management depends on transboundary coordination, which can entail territorial and/ or administrative borders. Administrative silos frequently emerge across the central level of government and impede the setting of evidence based priorities. Silos may also impede policy coherence implementation at sub-national levels of government. Local level officials often lack incentive to invest in risk reduction measures when they jeopardize economic development or job creation objectives.

Table 2.1. National strategic plans for governance of critical risks

Country	Link to national strategy
Australia	www.ag.gov.au/EmergencyManagement/Documents/NationalStrategyforDisasterResilience.PDF
Austria	www.bka.gv.at/site/3503/default.aspx
Canada	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-eng.aspx
Chile	repositoriodigitalonemi.cl/web/handle/2012/1710
Colombia	repositorio.gestiondelriesgo.gov.co/bitstream/20.500.11762/756/1/UNGRD_Plan_Nacional_Gestion_Riesgo_Desastres.pdf
Costa Rica	politica.cne.go.cr/
Denmark	N/A
Estonia	www.siseministeerium.ee/sites/default/files/dokumendid/riskianalyys_kokkuvote_2013.pdf
Finland	www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf
France	www.risques.gouv.fr/
Germany	N/A
Greece	N/A
Iceland	www.innanrikisraduneyti.is/media/blai_bordinn/Almannavarnastefna.pdf
Ireland	www.taoiseach.gov.ie/eng/News/Government_Press_Releases/Government_Publishes_Draft_National_Risk_Assessment_2017_and_seeks_views_on_Strategic_Risks_Facing_Ireland.html
Israel	N/A
Italy	www.protezionecivile.gov.it/jcms/it/home.wp
Japan	www.bousai.go.jp/taisaku/keikaku/pdf/kihon_basic_plan160216.pdf
Korea	www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=60148
Latvia	www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/National_Security_Law.doc; www.likumi.lv
Luxembourg	www.gouvernement.lu/hcpn; https://www.infocrise.lu/fr
Mexico	www.dof.gob.mx/nota_detalle.php?codigo=5415383&fecha=13/11/2015
Netherlands	english.nctv.nl/themes_en/national-security/index.aspx
New Zealand	www.civildefence.govt.nz/cdem-sector/cdem-framework/
Norway	https://www.regjeringen.no/en/dokumenter/meld.-st.-10-20162017/id2523238/
Poland	N/A
Portugal	N/A
Slovak Republic	www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25256
Slovenia	www.sos112.si/slo/page.php?src=sv3.htm
Spain	www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional
Sweden	www.msb.se/en/About-MSB/Crisis-Management-in-Sweden/
Switzerland	www.efv.admin.ch/efv/fr/home/themen/finanzpolitik_grundlagen/risiko_versicherungspolitik.html#1609951231 www.infraprotection.ch
Turkey	National Strategies for Earthquake Risk and Climate Change www.preventionweb.net/files/22115_13335nationalstrategy1.pdf; www.preventionweb.net/files/26236_eqstrategyturkeysmall.pdf
United Kingdom	www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
United States	https://www.fema.gov/national-planning-frameworks

Note: N/A = not applicable.

Several common goals are observed across national strategies for the governance of critical risks, in particular the aim to build and maintain national resilience (i.e. ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions). In addition, an analysis of the national strategies shows that they are comprehensive in scope, i.e. they do not focus just on emergency response but cover all phases of the risk management cycle. To this end they promote development of the skills and means needed to prevent, protect against, mitigate, respond to and recover from critical risks. Several national strategies emphasise the need to move toward a broader distribution of

responsibility for public safety; they state the need to move away from public reliance on a top-down, central government driven approach to building resilience (e.g. Canada and the United Kingdom). This signals recognition of the limits of central government capacities to manage all aspects of critical risks on their own, and seems to imply that individuals and local communities need to take an increased share of costs.

National strategies guide the design of risk management policies and programmes across government, and at different levels of government, with the aim to attain policy coherence. Among the most frequently found objectives within national strategies are: to strengthen the capacity to reduce disaster risks, to improve critical infrastructure protection, to strengthen the government's crisis management architecture and, consistent with the above mentioned national goal, to increase community resilience to threats and hazards. In addition, and in line with the notion of preparing for transboundary risks, many countries claim that the provision of support to overseas partners to develop their resilience and preparedness is an important objective. This includes being able to respond more effectively, and even collectively, to the impacts of conflict and crises.

Assess critical hazards and threats, invest in new research and tools, and set aside resources

A key function of a comprehensive, all-hazards and transboundary approach to country risk governance is to identify the hazards and threats that could pose critical risks. All respondents identified the hazards and threats that are assessed as critical risks. It is important to note that respondents had the possibility to write in a critical risk that did not appear on a set list of options. Thirty-three respondents consider sudden on-set, natural hazards (such as earthquakes, floods and forest fires) as a potential critical risk. The respondents selected these more than any other type of hazard or threat.

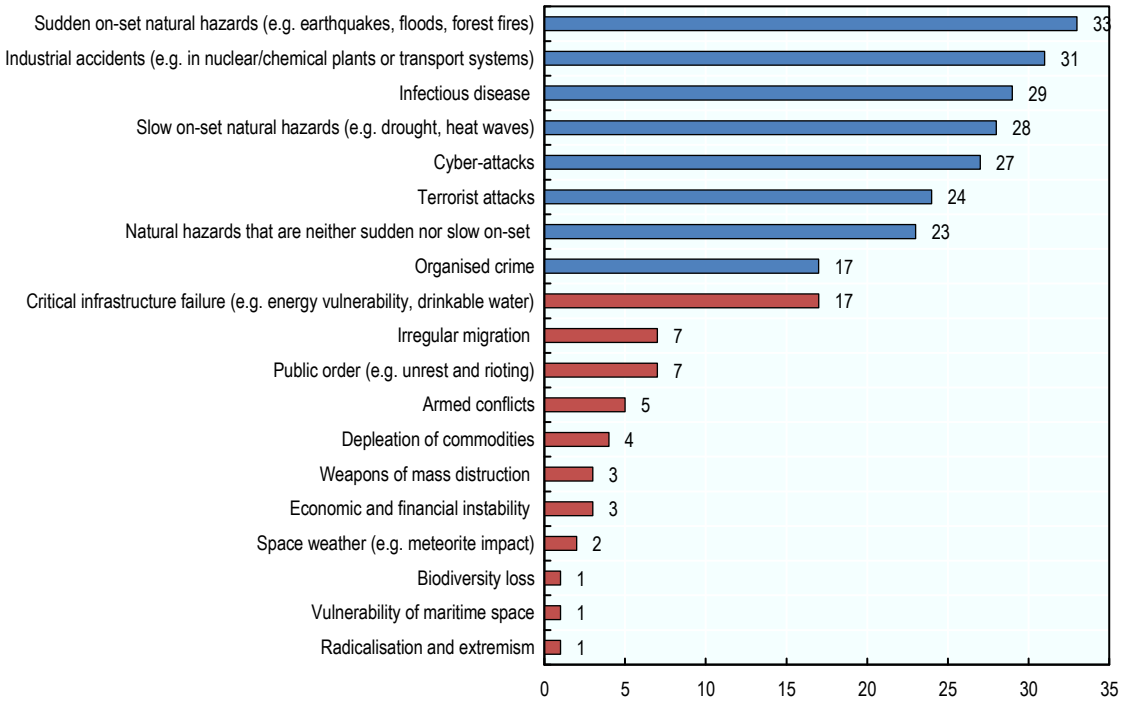
Infectious diseases also figure high on the list of critical risks that respondents identified. Since the outbreak of severe acute respiratory syndrome (SARS) in 2003, which caused 775 deaths worldwide and 44 deaths in Canada alone, there have been at least 7 outbreaks of infectious disease that affected more than one continent. These include dengue, mumps, the 2009 seasonal flu (14 286 deaths worldwide), Middle Eastern Respiratory Syndrome (449 deaths as of 2015), Ebola (11 300 deaths worldwide), Chikungunya and Zika.

The Ebola epidemic of 2013-16 was unprecedented in its scale and reach, revealing numerous societal and institutional vulnerabilities, but also opportunities to learn about the virus itself. Several medical care workers who had been identified as infected were flown for treatment in secure facilities in Europe and North America; however, others returned home during the incubation period without knowing they were infected. Despite precautions, for the first time an Ebola related casualty occurred in an adhering country (the United States), and for the first time a human-to-human transmission of the Ebola virus occurred in an adhering country.

Cyber-attacks generally do not lead directly to human casualties, yet 27 respondents consider them a critical risk. The frequency and sophistication of cyber risks continue to grow. Targets of Distributed Denial of Service and ransomware attacks now include critical infrastructure systems, such as electricity and gas distribution, healthcare facilities, transportation systems, cloud-based networks, financial institutions and payment systems. The Internet of Things will bring interconnectivity to new levels and multiply networks. Some countries anticipate cyber-attacks on everything from implanted

medical devices to clothing accessories and vehicles, which would raise new challenges for regulatory approvals of hitherto innocuous consumer products.

Figure 2.1. Types of hazards and threats identified as potential critical risks



Notes: Hazards and threats in red reflect information provided in response to "other" in the survey. Answers were received from all 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

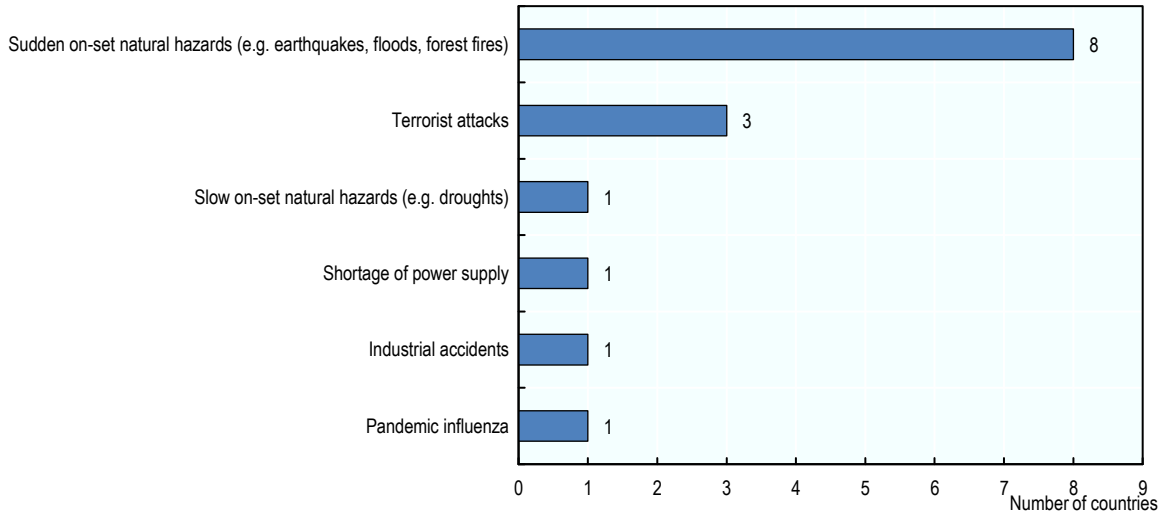
More than half of respondents consider organised crime a critical risk, which may also be a reflection on recent trends in national security related to the illicit markets these groups supply (narcotics, humans, counterfeits, arms and wildlife). These "steady-state" risks are not discrete, "extreme" events in probabilistic terms; rather their endemic nature has important cumulative impacts that make them relevant to a comprehensive national strategy to govern critical risks. Additional steady-state risks, such as air pollution, traffic accidents or ingestion of carcinogens were not considered as critical risks by countries, despite the large number of fatalities and illnesses that these steady-state risks result in every year. This reflects an understanding of "critical risks" as generally large discrete events that surpass the capacity of sub-national authorities to manage their consequences, and exceptionally as steady-state risks that significantly impact a national security interest sufficient to justify attention under a central government led strategy.

It is noteworthy that nearly half the respondents indicated on their own initiative that critical infrastructure disruptions are a potential critical risk (i.e. the survey did not provide this risk as an optional answer, but respondents provided this information in a blank space for this purpose). Likewise, seven respondents indicated at their own initiative that social unrest and irregular migration are seen as critical risks.

Three respondents consider discrete events from the perspective of their longer-term potential as critical risks. The United States Strategic National Risk Assessment, the

United Kingdom National Strategic Risk Assessment and the National Risk Profile in the Netherlands analyse discrete events both as they could occur now and in light of longer-term developments. These analyses show that risks may accumulate slowly over time, reach a point of no return and become a strategic consideration, because the impacts can no longer be remedied efficiently. Such risk analyses help to justify taking action now to reduce high-frequency, low-impact risks in the immediate term as a longer-term preventive action, similar to the countermeasures employed for steady state risks described above.

Figure 2.2. Critical risks singled out as "the most important"



Notes: Answers were received from 14 out of 34 responding countries. The figure adds up to 15 because one country ranked two risks as the most important.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

It is more accurate to state that all national strategies assess multiple risks rather than promote an all-hazards approach. According to the respondents, most national strategies follow an all-hazards approach, but four countries have opted specifically not to (Chile, Estonia, Japan and Turkey). In some cases this is due to a preference to treat the terrorist threat within a separate, non-integrated strategy. Several countries continue to develop hazard- or threat-specific strategies, for example on pandemic preparedness, critical infrastructure protection, counterterrorism and transnational organised crime. Some of the single theme strategies are aligned to an all-hazards strategy and share a common planning architecture to integrate and synchronise plans across the whole of society. This promotes unity of purpose and a foundation for setting priorities without carving out exceptional treatment for one type of critical risk.

A high number of respondents reported that terrorism is a critical risk, but the threat is frequently treated separately from the scope of all-hazards national strategies for the governance of critical risks. This raises the question whether terrorist events are so different in character that the capacities developed to manage their impacts are too specific to be of broader use to all hazards.

Box 2.2. National strategies governing critical risks: Australia, New Zealand and Spain

The national strategies for the governance of critical risks in Australia, New Zealand and Spain illustrate good practice in a whole-of-society approach with clear responsibilities, priorities and guidance for the governance of all critical risks.

Australia's National Strategy for Disaster Resilience provides high-level guidance on disaster management to federal, state, territory and sub-national governments, businesses, communities, and the non-profit sector. The Strategy recognises that disaster resilience is the collective responsibility of the whole society. It co-ordinates efforts and provides practical directions to all relevant national and sub-national stakeholders. While the Strategy specifically outlines guidance for critical risks emerging from natural hazards, the approach can also apply to governing other disasters such as pandemics and terrorist events.

Through its National Security System, **New Zealand** has adopted a comprehensive security guidance that embraces a whole-of-society perspective. The strategy outlines how government and other agencies should work together to plan for and respond to security issues, following the principle of subsidiarity. The strategy aims to improve the effectiveness of governance, strategic planning and management before, during and after a security challenge. Embracing an all-hazards approach, the framework seeks to address all significant risks New Zealand may face.

Spain's National Security Strategy promotes and facilitates a whole-of-society approach that assigns leadership at the national level and aligns the engagement of the various stakeholders through a national co-ordination platform. Taking an all-hazards perspective to risk, the strategy provides a comprehensive overview of the current security environment. It identifies objectives and lines of action for the entire spectrum of threats and risks, ranging from natural disasters to human induced threats.

Sources: OECD (2016b), Toolkit for Risk Governance, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/; New Zealand Department of the Prime Minister and Cabinet (2011), "New Zealand's National Security System", www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf; Departamento de Seguridad Nacional (2013), "Estrategia de Seguridad Nacional", www.dsn.gob.es/en/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional; Council of Australian Governments (2011), "National Strategy for Disaster Resilience: Building our nation's resilience to disasters", www.coag.gov.au/node/81.

Adopt an all-hazards approach that identifies interdependencies between critical systems

An all-hazards approach does not mean spreading limited resources to prevent and/or mitigate all possible hazards, but rather allocating resources to risks that are the most likely to have a national significance. Fundamentally, this approach is meant to address not only known risks, but also the challenges that arise from "known unknowns" and "unknown unknowns". While all countries make efforts to identify critical risks, the mapping of interdependencies in critical systems that can lead to widespread vulnerabilities is still at its beginning stages in only a few countries.

A good practice is found in the United States where the Department of Energy has supported research to map interdependencies with electricity infrastructure and potential cascading impacts due to disruptions they may cause. The research identifies systems'

vulnerabilities and helps to prioritise measures that address potential failure points that would have the most severe consequences.

Identify core capabilities to preserve against the harmful impacts of critical risks

The aim of the OECD Recommendation is to support countries in the preservation of public safety, sustainable economic growth, market integrity and the environment. No two emergencies or disasters are identical, but in each situation, regardless of cause, the emergency preparedness capabilities and skills that first responders need to possess are essentially the same. The direct consequences of critical risks often include injuries or deaths, property damage and environmental contamination. But these risks also produce second order effects such as the failure of infrastructure networks vital to the delivery of essential goods and services.

Past events reveal that core capabilities are key to manage both the different types of social and economic consequences seen in recent crises and disasters (such as closure of air-traffic to ash clouds) and the increased tendency of transboundary consequences (e.g. the SARS, Ebola and H5NI viruses). These comprise human capital, equipment, financial resources and administrative capacities needed to ensure the last line of defence, i.e. to rescue people, protect property and restore lifelines and livelihoods.

A high number of countries have identified and designated core capabilities, however relatively few respondents provided clear evidence that these have been implemented and tested as part of their all-hazards strategy. Among the respondents that did provide examples of good practice are the United Kingdom and the United States (see Box 2.3).

Box 2.3. Building core capabilities to manage critical risks: United Kingdom and United States

The **United Kingdom** identifies generic capabilities that underpin the country's resilience to disruptive challenges, regardless of whether those emergencies are caused by accidents, natural hazards or man-made threats. Capability to respond to emergencies encompasses a number of interdependent and interrelated factors including appropriate numbers and types of personnel, the right types of equipment and supplies, relevant and sufficient training and exercises, clear emergency plans, etc. The Cabinet Office Civil Contingencies Secretariat manages a capabilities programme that identifies and monitors the current levels of capability in each of the areas covered by 22 defined work streams. The information gathered on how much capability each work stream has delivered is then used to provide assurance to ministers on how ready the United Kingdom is to respond to civil emergencies. Each of the 22 work streams is the responsibility of a lead government department.

In the **United States** the National Preparedness Goal identifies 32 core capabilities, each of which is tied to a capability target. These targets recognise that every organisation needs the flexibility to determine how they apply their resources, based on the threats that are most relevant to their communities. A city, for example, may determine it is at high risk for a catastrophic earthquake. As a result, the city could set a target to have a certain number of buildings retrofitted to meet modern building codes. The same applies across all potential risks, understanding that each risk is different; therefore, each target is different. The core capabilities are categorised according to five mission areas: prevention, protection, mitigation, response and recovery. Some fall into only one area, while others apply to several.

Sources: United Kingdom Cabinet Office (2014), Guidance: Preparation and planning for emergencies: the National Resilience Capabilities Programme; https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme FEMA (2016), National Preparedness Goal, Core Capabilities website, https://www.fema.gov/core-capabilities.

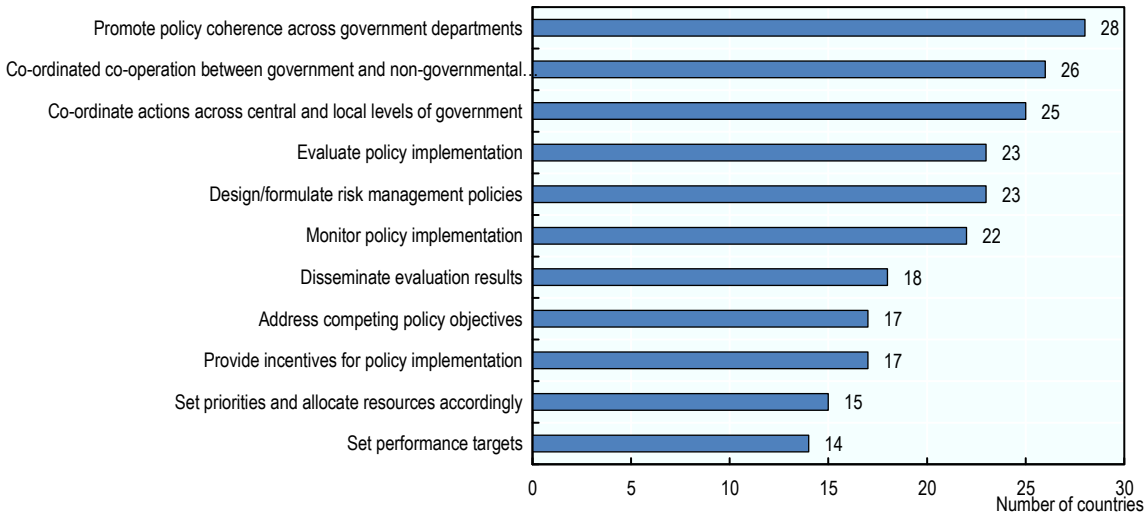
Assign leadership at the national level

National leaders should be selected to drive policy implementation, connect policy agendas and align competing priorities across ministries and between central and sub-national levels of government. In a traditional emergency management context, local emergency services handle incidents without involvement by central government. Critical risks concern incidents that by definition involve an impact of national significance and entail co-ordination between a lead line ministry and potentially several line ministries, departments or agencies, and levels of government.

Containment measures during an infectious disease outbreak, for example, may require co-ordinated actions with a health, environment and/or agriculture ministry as well as authorities responsible for tourism, education and transport. This may happen when animal to human or plant transmission is a risk, food security is at risk, or culling animals is considered as a policy response. In such cases, a single local community could undermine a broadly agreed containment strategy by refusing to close schools, inoculate livestock or implement quarantine measures as directed.

When asked whether they had assigned leadership at national level, 31 respondents answered that a central government institution or body had been given responsibility to co-ordinate the management of critical risks. This does not necessarily mean that key governance functions are not carried out, but rather the roles are distributed to a mix of ministries and agencies, which could complicate the objective of connecting policy agendas and aligning competing priorities. It is noted that the government administrative structures of a few countries place primary authority for implementing disaster risk reduction policies and emergency management at the sub-national levels of government. Nonetheless, establishing leadership to drive a national strategy is key to address the risk governance gaps in transboundary crises, where sub-national authorities are overwhelmed and national institutional responses involving multiple agencies are uncoordinated or undercut each other's efforts by pursuing their individual interests.

Figure 2.3. Lead institution governance functions



Note: Answers were received from 29 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Respondents pointed to various functions and responsibilities of designated lead institutions for the governance of critical risks that enable them to co-ordinate joint efforts between multiple ministries and agencies, realign incentives to achieve the aims and priorities of the national strategy, and drive co-operation between governmental and non-governmental organisations. Figure 2.3 indicates risk governance functions where implementation across countries is relatively developed and also areas in need of further improvement. Twenty-eight respondents reported that institutions aim at establishing an inter-agency approach in order to identify interlinkages and to promote policy coherence, as well as connecting policy agendas across levels of government and with the private sector. A high number of respondents also pointed to functions to co-ordinate across government at different levels and with non-government entities. About half of the countries provide incentives for implementing policies to manage critical risks. Relatively few, however, go so far as to define priorities for risk management actions or to set performance targets.

Box 2.4. Functions of lead institutions: United Kingdom

In the United Kingdom, the Cabinet Office Civil Contingencies Secretariat (CCS) provides the central focus for the cross-departmental and cross-agency commitment, co-ordination and co-operation necessary to deal with disruptive challenges and crises. This focus goes beyond first response and consequence management and applies to systems for identifying new challenges, for assessing risks, for anticipating, planning, preparing and conducting exercises for crises, for building up resilience to them, and for systematically applying the lessons learned from particular incidents.

In the event of an emergency of a large scale or of a kind identified by the lead government as requiring central involvement, the CCS engages in a way designed to enable the department's ministers and senior officials to concentrate on strategic decisions. Key objectives will be smooth collaboration between organisations and a seamless transition to central co-ordination if required.

Working closely with the department concerned, the CCS:

- assesses immediate needs and support their provision; establish possible scenarios up to worst cases and plan for scaling-up, logistical management and evacuation (see Chapter 5)
- ensures that the centre of government and other interested departments are kept informed and are prepared to act
- helps establish structures, rhythms, routines and data flows for managing the response – in particular increasing the department's resources and public information systems
- connects the department with agencies able to provide specialist advice and information
- decides whether and when to approach the chairman to convene a meeting of Civil Contingencies Committee, thereafter providing ongoing support from the centre.

The CCS works closely with pre-designated lead ministries to:

- enable and protect their own decision makers develop their own early warning systems
- prepare plans against various eventualities and make sure those plans are properly integrated with those of other departments and agencies
- identify the training and exercises needed to test the plans and enable continuous improvements
- build up the necessary management and professional expertise to maintain and activate the plans and to know where to turn for reinforcement
- learn from experience and share their knowledge with other departments
- align competing priorities across government departments.

Source: CCS (2011), "The role of lead government departments in planning for and managing crises", United Kingdom Civil Contingencies Secretariat, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61356/lead-government-department-framework.pdf.

Respondents noted that synergies can arise through building coherence across different thematic strategies, in particular climate change adaptation strategies which are increasingly linked to disaster risk management. This presents a clear opportunity to

exercise central leadership in the governance of risk reduction policies, which are mainly implemented at sub-national levels of government. Good practice examples can be found in Poland and Portugal where risk assessment expertise and preparedness capacities for hydro-meteorological risks feed into the design and planning of climate change adaptation policies. This is of particular importance, since hydro-meteorological risks are the most susceptible to climate change and account for a majority of disaster damages on an average annual basis.

Institutional leadership is useful to achieve policy coherence and co-ordinate responsibilities between line ministries and sub-national levels of government, but co-operation requires backing from political leaders. Respondents were asked whether the institution identified as leading the national strategy on governance of critical risks reports to the head of government and/or a cabinet-level minister on actions to further the strategy and performance of its authorities. Twenty-five countries have established a systematic formal process for reporting to the highest level of government, with 17 respondents reporting at least once per year and 5 reporting more than once per year.

Table 2.2. The risk governance functions of the lead organisation on the management of critical risks, 2016

	Design/formulate risk management policies	Set priorities and allocate resources accordingly	Set performance targets	Provide incentives for policy implementation	Monitor policy implementation	Evaluate policy implementation	Disseminate results of evaluation to the public	Promote policy coherence across government departments	Address competing policy objectives	Co-ordinate actions across central and sub-national levels of	Co-ordinate co-operation between government and non-
Australia	●	●	X	●	●	●	X	●	●	●	●
Austria	○	○	○	○	○	○	●	●	○	●	●
Canada	●	●	●	●	●	●	●	●	●	●	●
Chile	●	○	○	●	○	○	○	●	●	●	●
Denmark	X	X	X	X	X	X	X	X	X	X	X
Estonia	●	○	○	○	●	●	●	●	○	●	●
Finland	○	○	○	○	●	●	○	●	○	○	●
France	●	○	○	○	○	○	○	●	○	○	○
Germany	○	○	○	○	○	○	○	●	○	○	●
Greece	●	○	○	●	●	●	○	●	○	○	●
Iceland	○	●	●	●	○	○	●	●	●	●	●
Ireland											
Italy	●	○	○	○	●	●	●	●	●	●	●
Japan	●	○	○	○	○	○	○	●	○	●	○
Korea	●	●	●	●	●	●	●	●	●	●	●
Latvia	○	○	○	○	●	●	○	○	●	●	●
Luxembourg	●	●	●	●	●	●	●	●	●	●	●
Mexico	●	●	●	●	●	●	●	●	●	●	●
Netherlands	●	○	●	●	●	●	●	●	●	●	●
New Zealand	●	●	○	○	○	○	○	●	●	●	○
Norway	●	○	○	●	●	●	●	●	○	●	●
Poland	●	○	○	○	●	●	●	●	○	○	○
Portugal	X	X	X	X	X	X	X	X	X	X	X
Slovak Republic	X	X	X	X	X	X	X	X	X	X	X
Slovenia	○	○	○	●	○	●	●	●	○	●	●
Spain	●	●	●	●	●	●	●	●	●	●	●
Sweden	●	○	●	●	●	●	●	●	●	●	●
Switzerland	●	●	○	○	●	●	○	●	○	●	●
Turkey	○	●	●	○	●	●	○	○	○	●	●
United Kingdom	●	●	●	●	●	●	●	●	●	●	●
United States	●	●	●	●	●	●	●	●	●	●	●
OECD total											
● Yes	20	12	11	15	19	20	16	25	15	22	23
○ No	8	16	17	13	9	8	12	3	13	6	5
x Not applicable	3	3	3	3	3	3	3	3	3	3	3
Costa Rica	●	●	●	●	●	●	●	●	●	●	●
Colombia	●	●	●	●	●	●	●	●	●	●	●

Note: ● = yes, ○ = no and x = not applicable.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Include a range of stakeholders in policy-making processes

Risk governance requires balancing and co-ordinating a range of stakeholders in processes that are open to public participation and especially at the policy formulation stage. All national and sub-national government actors should engage in this effort. An inclusive, whole-of-society approach to risk governance not only helps allocate risks, it establishes a public record that clarifies accountability for decisions which might otherwise obscure complex trade-offs.

Consistent with the overall objectives of Open Government and the Open Government Partnership, citizen engagement is meant to achieve a shared vision of critical risks and the division of responsibilities for shouldering the management burden. Ultimately the aim of such multi-stakeholder processes is to reach an optimal balance of trade-offs that results in more resilient communities. From this inclusive growth perspective, stakeholder engagement creates the buy-in from stakeholders and citizens needed to ensure sustainable benefits.

Box 2.5. Engaging the whole of society in the policy-making process: Germany and the United States

In **Germany**, the federal government regularly analyses the risk landscape and includes all relevant federal and sub-national departments in the process. The risk analysis work is considered a continuous process to enable need-based and effective protection against disasters. Since 2009, the Federal Ministry of Interior is legally obliged to share the results of the annual risk analysis, as well as deliver a comprehensive report on the current status of ongoing risk analyses with the national parliament (Bundestag). The Internal Affairs Committee of the Bundestag discusses and comments on the findings of the risk analysis and supports inter-departmental and interdisciplinary risk analysis efforts. To date, five risk analyses have been conducted focusing on the following: flood events and pandemics in 2012, winter storms in 2013, storm surges in 2014, nuclear accidents in 2015 and chemical spills, as well as gas scarcity, in 2016. The results of the risk analysis are compared and harmonised with the available civil protection and crisis management capacities.

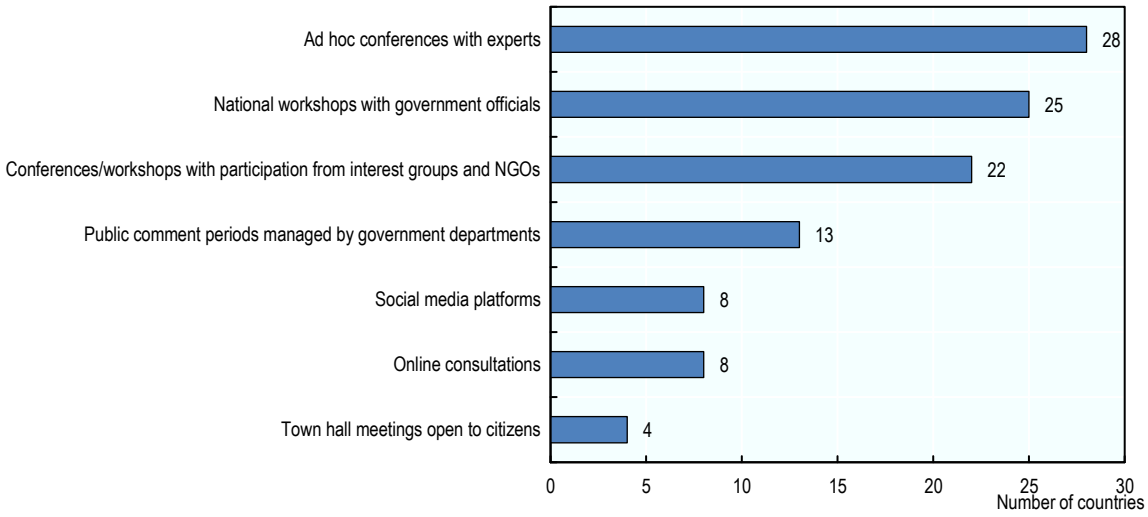
In the **United States**, the Secretary of Homeland Security develops and submits the national preparedness goal to the president, through the Assistant to the President for Homeland Security and Counterterrorism. The Secretary co-ordinates this effort with other executive departments and agencies and consults with state, local, tribal and territorial governments, the private and non-profit sectors, and the public. The national preparedness goal is informed by the risk of specific threats and vulnerabilities – taking into account regional variations – and includes concrete, measurable and prioritised objectives to mitigate that risk. The goal is meant to be reviewed regularly to evaluate consistency with these policies, evolving conditions and the National Incident Management System.

Source: Deutscher Bundestag (2016), "*Unterrichtung durch die Bundesregierung, Bericht zur Risikoanalyse im Bevölkerungsschutz 2015*" [Briefing issued by the German Government, Report on risk analysis in civil protection 2015], dip21.bundestag.de/dip21/btd/18/072/1807209.pdf.

Twenty-nine respondents reported that the lead institution responsible for governance of critical risks consults with a broad range of stakeholders in the policy-making process. When asked what forms of consultation they undertake, 28 respondents pointed to ad hoc conferences to engage with national experts. Twenty-five countries have established national workshops series to promote dialogue among government officials, and 22 countries also engage with non-governmental organisations (NGOs) and interest groups through conferences, which is a proven means to test new ideas. A small minority of countries have put in place mechanisms to foster more granular citizen engagement such as social media platforms, online consultations and town hall meetings.

Overall, these results indicate a propensity among countries to consult with experts, rather than openness to a broad set of stakeholders who represent a variety of interests. A lack of participatory process in risk management decisions in some past instances has led to public protest and even civil unrest, for example concerning where to locate new dams.

Figure 2.4. Mechanisms used to engage national and sub-national stakeholders



Note: Answers were received from 29 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Though countries were not asked specifically, no information was offered concerning whether these consultations occur at an early stage and involve all citizens concerned, including the most rural, excluded and special needs population groups. As disaster risks tend to have a disproportionate impact on these groups, further research is needed to ascertain whether and how effectively interactions could take place directly with these citizens. Social media and virtual platforms can enable governments to increase access to a broader range of stakeholders at lower costs. Such efforts are beginning to be used by river basin authorities, which in many countries have responsibility for designing flood risk management policies.

River basin authorities in the European Union are a good example of transboundary governance bodies accustomed to involving stakeholders in policy dialogue across sub-national administrative boundaries. This governance mechanism enables inclusive dialogue at the policy formulation and evaluation stages to foster co-operation between government and industrial, agricultural, recreational and energy sector stakeholders. The

experience has shown to achieve higher regulatory compliance rates and clearer accountability.

As a core part of Mexico's National Civil Protection System (Sistema Nacional de Protección Civil, SINAPROC), the National Board of Civil Protection (Consejo Nacional de Protección Civil, NBCP) is the key forum for strategic co-ordination between the president, the heads of federal ministries, all state governors and the head of government of the Federal District, as well as the boards of civil protection commissions of the Senate and House of Deputies. Since 2013, the NBCP holds annual meetings to define cross-cutting policies and guidelines for civil protection and disaster prevention. Through the NBCP, all relevant national and sub-national stakeholders have a gateway for involvement in the process of civil protection and disaster risk reduction policy making. The NBCP also serves as a platform for dialogue with relevant non-governmental stakeholders and seeks to implement a whole-of-society approach.

Establish partnerships with the private sector

Government partnerships with the private sector are meant to achieve responsiveness and shared responsibilities aligned with the national strategy. The private sector possesses a wealth of expertise, core skills and competencies to support disaster recovery and reconstruction to "build back better". Relatively few respondents provided information to show that they engage the private sector in disaster risk reduction actions, emergency preparedness, response and recovery.

The Recommendation calls for the creation of models for public-private partnerships (PPPs) to develop trusted information-sharing networks that help identify where disruptions to critical infrastructure and supply chains could lead to knock-on effects across borders and to cascading effects. The United States provides a good practice example of this in the Critical Infrastructure Partnership Advisory Council.[1] The Council convenes critical infrastructure owners, operators and trade associations to engage in intra-government and public-private co-operation, information sharing and collaboration across the entire range of critical infrastructure protection activities.

Use the private sector for technologies, infrastructure and financing

Countries should integrate private sector capability and expertise to develop new technologies, build resilient infrastructure and deliver financial mechanisms. Japan presents a good practice model of public-private partnership through the Bosai Platform. This network of companies and associations offers goods and services ranging from research, technology, training and finance solutions for all phases of the disaster risk management cycle.[2]

Key trends and self-assessment

Almost all countries have adopted national strategies for the governance of critical risks in response to the increasing frequency and magnitude of such risks, but also due to deficiencies identified in the planning, co-ordination and implementation of disaster risk management capacities. Generally, these strategies promote a comprehensive policy framework comprising the essential phases of the risk management cycle under one cohesive plan. The framework is addressed not only to government agencies but to all relevant stakeholders, i.e. the whole of society. The most recently adopted national

strategies tend to call for preparedness for all-hazards approaches to support capacities required for managing "unknown unknowns" or "black swan" events.

Most national strategies establish the development of national resilience as their central goal, but they focus on objectives of pre-event preparedness and prevention actions. Consistent with the all-hazards approach to risk management, a few national strategies set out guidance on the core capabilities commonly required to manage the harmful impacts of major disasters (such as evacuation routes and transportation services, debris removal and fatality management services). These are considered the main capacities and resources needed post-event to bounce back quickly from disasters.

Almost all countries have identified a lead institution to co-ordinate actions pursuant to their national strategy. Lead institutions are tasked with a range of governance functions related to the national strategies, from ensuring policy coherence to providing policy guidance across government departments and agencies, whether at central or sub-national levels of government. National strategies are seldom used to align competing priorities. In terms of driving policy implementation, the access of these lead institutions to senior levels of government demonstrates some degree of policy push from leadership that encourages stakeholders to co-operate in the participatory processes made available.

Greater use of digital platforms to actively engage stakeholders in formulating risk management policies is beginning to take hold for a small number of hazards, especially floods. Such tools have proven useful to overcome some cost barriers to broader participation in public debates on risk management policies, just as in different areas of public policy.

In many cases the lead institution operates in close proximity to the centre of government and co-ordinates with the lead ministries responsible for policy design. A few lead institutions have conducted internal reviews to monitor and evaluate the results of risk management policies and specific risk management policies aligned to the national strategy. In a few cases, countries have even conducted an OECD risk management policies peer review.

Countries have clarified the roles of government agencies for managing different major risks, by identifying who takes the lead for specific risks and/or various phases of the risk management cycle: risk assessment, prevention, preparedness, response and recovery. Nonetheless, a high number of countries' national strategies focus on natural hazards, and a significant number continue to address terrorist threats, industrial accidents and pandemics in a separate strategy document. Consequently the domestic debates and programme planning in these countries tend to operate in thematic silos, which may not be suited to identify where investments in capabilities can converge to address multiple risks.

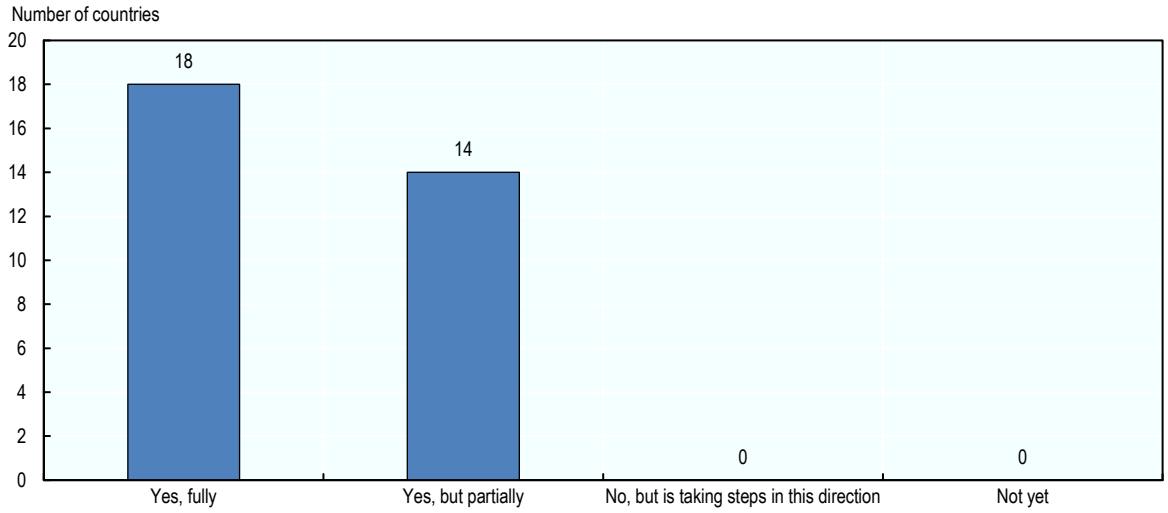
National strategies emphasise the importance of a whole-of-society approach to risk governance and advocate unifying efforts between multiple organisations in support of disaster risk management policies. The role of civil society seems to be most developed in the volunteer organisations that support civil protection services. The various non-government actors that constitute the "whole of society", including private sector operators of critical infrastructure, are sometimes better positioned to manage consequences of critical risks than government bodies.

A central corollary to the goal of developing national resilience in a few countries is that central government cannot be expected to bear all risks; a greater share of the costs for

prevention, preparedness, recovery and reconstruction have to be borne by the private sector, households and local communities. Relatively few national strategies articulate extensive expectations of what the whole of society is expected to contribute toward national resilience, beyond the need to conduct local risk assessments, implement risk informed land-use policies and urban codes, and provide leadership and support to local first responders. Long-term engagement of local volunteers and non-governmental actors in policy design, monitoring and implementation is a noted challenge due to lack of resources.

When asked about fulfilling the first key recommendation, countries rated themselves relatively high (Figure 2.5). More than half of the countries consider that they have fully met its provisions, while less than half report that they have partially fulfilled it. No country reported that it had not yet fulfilled this key recommendation.

Figure 2.5. Self-assessment on implementing the first key recommendation



Note: Answers were received from 32 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Conclusions

In line with the Recommendation, countries that have already adopted a national strategy for the governance of critical risks should ensure that they provide for a comprehensive and transboundary approach to risk management, and those that have not adopted one should do so. Most countries have adopted such strategies, and in general these strategies aim to strengthen co-ordination of disaster risk management planning and operational responses, which have increased due to the frequency, magnitude and complexity of extreme events. The contents of these national strategies build on existing national disaster preparedness plans and fulfil the provisions of the Recommendation to varying degrees.

The survey exercise could not determine whether the national strategies actually result in enhanced co-ordination of risk owners such that transboundary risks are now identified, assessed, reduced and prepared for to a greater degree than before the strategy was adopted. To conduct such analysis would require a more granular level of information

collection and stakeholder engagement capable of assessing the information, for example as can be performed through an OECD peer review.

Countries should update their national strategies as needed to incorporate preparedness for transboundary risks, threats and vulnerabilities. The national strategies of six countries do not follow an all-hazards approach, which may impede fully informed reflection on how the consequences of one type of risk can trigger another.

Significant thematic gaps are observed in the national strategies of countries that reportedly follow an all-hazards approach. For example many strategies cover natural hazards and industrial accidents, but they do not address infectious disease, terrorism or other forms of steady state risks that could be assessed as critical risks. Consequently, even if a leading institution is in place to consider all hazards, its deliberations and decision-making may contain blind spots due to assessments that take place in administrative silos. This could impede an objective and forward-looking comparison of risk analysis results, e.g. of man-made threats and natural hazards as well as near-term and long-term risks, which is necessary to set risk informed priorities.

Countries should enumerate and develop the generic capabilities needed to prepare for the consequences of transboundary incidents. They should do so no matter what the cause, where public safety is jeopardised on a large scale.

Leading institutions should leverage their co-ordination role in policy design, policy monitoring and policy evaluation to engage in a broad range of disaster risk reduction policies. The magnitude of many critical risks surpasses sub-national capacities for emergency response, and many hazards, not only climate risks, are transboundary in nature. The institutions designated to lead national strategies are in a strong position both to map the broad range of hazards and vulnerabilities that stand to be significantly altered by changes to climate and to exercise their competence to connect policy agendas to reduce the associated risks.

Notes

[1] See https://www.dhs.gov/critical-infrastructure-sector-partnerships.

[2] See the Bosai Platform: https://www.bosai-jp.org/en/page/profile.

References

CCS (2011), "The role of lead government departments in planning for and managing crises", United Kingdom Civil Contingencies Secretariat, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61356/lead-government-department-framework.pdf.

Council of Australian Governments (2011), "National Strategy for Disaster Resilience: Building our nation's resilience to disasters", www.coag.gov.au/node/81.

Departamento de Seguridad Nacional (2013), "Estrategia de Seguridad Nacional" [National Security Strategy], Spain, www.dsn.gob.es/en/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional.

Deutscher Bundestag (2016), "Unterrichtung durch die Bundesregierung, Bericht zur Risikoanalyse im Bevölkerungsschutz 2015" [Briefing issued by the German Government, Report on risk analysis in civil protection 2015], dip21.bundestag.de/dip21/btd/18/072/1807209.pdf.

FEMA (2016), National Preparedness Goal, Core Capabilities website, update 07/05/2016 - 09:22, Federal Emergency Management Agency, United States, https://www.fema.gov/core-capabilities.

Ministry of Defence of Finland (2011), *Security Strategy for Society: Government Resolution 16.12.2010*, Helsinki, Finland, www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf.

New Zealand Department of the Prime Minister and Cabinet (2011), "New Zealand's National Security System", www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf.

OECD (2016a), OECD Survey on the Governance of Critical Risks, OECD, Paris.

OECD (2016b), Toolkit for Risk Governance: Good Practices website, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/.

United Kingdom Cabinet Office (2014), Guidance: Preparation and planning for emergencies: The National Resilience Capabilities Programme, https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme.

Chapter 3. Critical risk assessments and financing frameworks

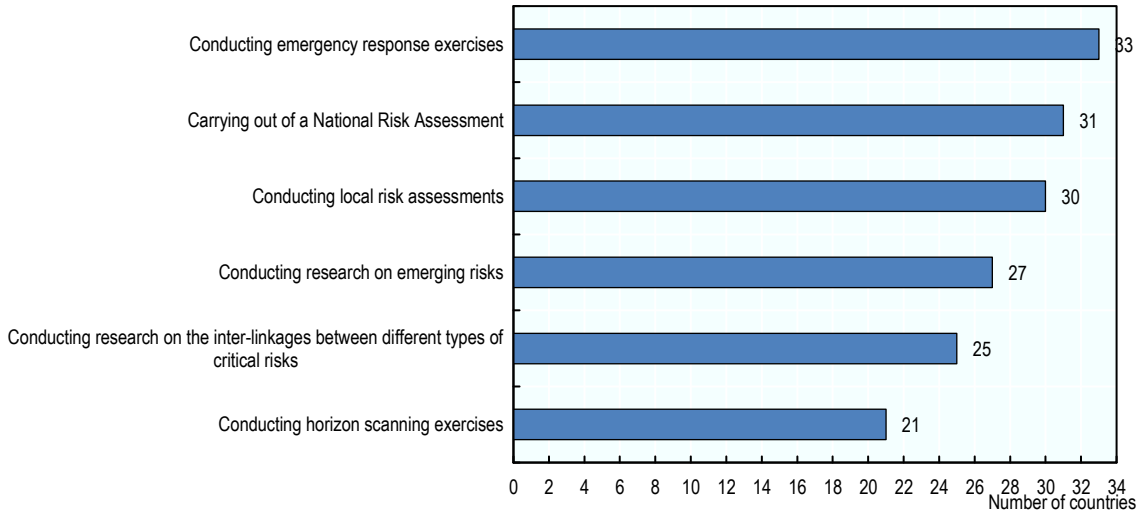
This chapter reviews how countries have carried out the second key OECD Recommendation of the Council on the Governance of Critical Risks. This recommendation calls for building preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impacts. The first section presents examples of good practice and policy tools to prepare for emergencies. The second section analyses key trends among countries attempting to follow the Recommendation. The chapter's conclusions offer ideas for effective next steps to face critical risks.

Good practices and policy tools

Respondents to the OECD Survey on the Governance of Critical Risks identified a wide range of measures and tools used to develop risk anticipation capacity. These include emergency response exercises, national and local risk assessments, research on emerging risks and on the interlinkages between different types of critical risks, and the conduct of horizon scanning.

Thirty-three of the 34 respondents indicated that emergency exercises help to build risk anticipation capacity (Figure 3.1). Respondents commented that exercises inform decisions about where improvements are needed in emergency management capabilities and enable planners to anticipate and prevent shortcomings in future responses. Exercises are not usually conducted with the aim to uncover new types of critical risks, though such insights might arise in the course of an exercise. Relatively few respondents provided information about the conduct of exercises specifically designed to test preparedness capabilities for rare or unprecedented events. Austria, Germany, the Netherlands and the United States demonstrate good practice examples of exercises designed around a simulated emergency situation involving sustained electrical outages in major cities.

Figure 3.1. Tools for risk anticipation



Note: Answers were received from all 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Establish national risk assessments

Thirty respondents reported that they had established a national risk assessment to identify the risks that would have a significant national impact. Ireland (see Box 3.1), the Netherlands, Norway, Sweden and the United Kingdom demonstrate multiple good practices in developing and applying this tool.

Box 3.1. National risk assessment: Ireland

In Ireland both the Department of Taoiseach (Prime Minister's Office) and Department of Defence (Office of Emergency Planning) each conduct a multi-agency national risk assessment with distinct but complementary aims. The latter focuses on events that could lead to civil protection emergencies such as extreme weather, fires and floods and feeds into the national civil protection strategy. The former considers broad geo-political, social and major economic or fiscal trends (both inside and outside Ireland), which could lead to a national level crisis. Since some civil emergencies could develop into crises, the underlying analysis also forms a subset of the annual strategic overview of national risks carried out by the Department of Taioseach (Irish Department of the Taoiseach, 2017).

The national risk assessment of the Department of Defence provides an all-hazards/threat analysis at national level to complement the risk assessments completed at local and regional levels. The process begins by grouping identified hazards and threats into four categories: natural, transportation, technological and civil. Focus groups are formed to consider the overall risks presented by each category by assessing the likelihood of the hazard occurring and examining the potential impact (severity of consequences to life and health, property and infrastructure, and the environment). The impact assessment criteria are designed to reflect emergencies requiring national (rather than regional) co-ordination. Risks are plotted in a five-by-five matrix to enable comparisons, as per the European Commission guidelines (European Commission, 2010). The exercise results are four individual hazard classification risk matrices and a consolidated overall national risk matrix. They have been used to drive key emergency management agenda items at a high level within government to prioritise the mitigation of high risks identified as such. They have also contributed to other emergency management processes.

The Department of Defence's national risk assessment is supported by quantitative analysis where relevant data on hazards is available. Multiple stakeholders contributed to its development, including the Office of Emergency Planning, with guidance from experts at Dublin City University Business School, and in conjunction with all the relevant government departments and state agencies. The process builds in strong transparency and accountability measures; it is noted by government and then submitted to the European Commission as required under its Civil Protection Mechanism, and published on www.emergencyplanning.ie. The document is subject to a three-year review cycle, which commenced in 2015, and to the approval of the Government Task Force on Emergency Planning.

Source: OECD (2016b), Toolkit for Risk Governance: National Risk Assessment in the Netherlands, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/nationalriskassessmentinthenetherlands.htm; OECD (2016c), Toolkit for Risk Governance: Ireland National Risk Assessment 2015 − Overview of Strategic Risks, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/irelandnationalriskassessment2015-overviewofstrategicrisks.htm.

To develop all-hazards national risk assessments, countries include inputs from across different government departments and agencies where the expertise can be found. This practice is important not only to identify a wide range of critical risks in terms of their

potential likelihood, plausibility and impacts, but also to build consensus across government departments concerning the outcomes of the exercise.

About one-third of countries have shown that they established a co-ordination mechanism such as a standing working group or committee comprising policy advisers from responsible government departments. While a high number of countries rely solely on the knowledge of experts in government agencies, in some cases they have opened the process to include expertise from outside organisations when it cannot be found in government ranks. A good practice example can be found in the Netherlands where a formal network of analysts includes experts from government research establishments and the academic sector. Among the countries that take an inclusive approach to national risk assessment, the benefits noted were a more comprehensive understanding of the factors that render populations, assets and economic activities vulnerable to shock events. Finally, survey respondents indicated that such co-operative processes can be leveraged as trusted information-sharing networks that prove useful in a crisis management context.

To develop capacity for risk anticipation, 25 respondents also pointed to support for public research on emerging risks and the practice of following private sector research in this field, such as that developed by insurers and reinsurers.[1] Analysis of emerging risks involves identifying trends and drivers in diverse fields, such as climatology, technology and sociology that point toward the development over time of new risks or that substantially alter existing ones. Among the most common drivers, respondents identified geographic concentrations of assets and populations in hazard exposed areas (especially along coastal zones), climate change, and new vulnerabilities arising from the Internet of Things. These include stealing, distorting or destroying data, holding data for ransom, and disrupting the delivery of essential goods and services.

When asked, 27 respondents reported using local risk assessments as a tool for risk anticipation. This process involves lower tiers of government, at sub-national or regional level down to the local level. A national risk assessment can provide guidance on the national risk picture and, in some instances, on how this may be reflected in regional or local risk assessments to assist authorities to examine and plan for risks. Some respondents pointed to the difficulty in achieving a consistent methodology between top-down and bottom-up approaches. A few respondents with large territories consider it methodologically unsound to aggregate multiple local risk assessments into a national level picture, whereas those with small territories did not identify this as an issue.

Develop capacity for horizon scanning

Twenty-one respondents reported that they conduct horizon-scanning exercises, analysing trends that shape the environment or circumstances under which future risks will occur. While over half of respondents indicated that they carry out horizon scanning, relatively few provided specific information that links horizon scanning and foresight analysis to decision-making. A commonly cited challenge is translating complex and sometimes nebulous future issues into coherent documents that can usefully inform the policy process. Respondents provided examples of horizon scanning to detect early signs of potentially important developments with disruptive impacts on risk management decisions, e.g. climate variance, technology, society, the global economy and political developments. Respondents also pointed to studies conducted on novel risks and unexpected strategic challenges, as well as persistent problems and weak signals.

The United Kingdom was one of the first countries to develop this concept by analysing and anticipating near-term risks as a "Forward Look". This approach has strongly enhanced the country's strategic crisis management capacity (Box 3.2).

The Netherlands also undertook this process in 2007. In contrast to the permanent horizon-scanning systems of the United Kingdom, the Netherlands Horizon Scan 2007 was a single project carried out by a specially established team under the responsibility of the Commission for Consultation of Sector Councils (COS). The COS is a platform for consultation and collaboration of independent commissions consisting of representatives from research, society, industry, government and think-tanks. On the basis of futures studies, it formulated priorities for society-oriented research, focusing in particular on those experts dealing with cross-sector subjects at the interface of policy domains and scientific disciplines (Commission for Consultation of Sector Councils, 2008).

Countries were asked how they make use of risk anticipation. Thirty-two respondents indicated it is primarily used to inform the public about impeding risks and to develop specific training exercises. Moreover, these efforts also widely serve to inform strategic policy decisions and often translate into the prioritisation of government actions aimed at risk treatment. The example of the United Kingdom demonstrates that strategic early warning of events can be achieved with structured and consistent application of a clear methodology and with established information networks to ensure material for analysis.

Box 3.2. Good practice in strategic foresight arrangements: Finland, Sweden, United Kingdom and United States

Finland: The Government Foresight Report (GFR) and Government Foresight Network are the key elements of a broader foresight system. The system also comprises a parliamentary committee for the future, a foresight consortium for labour force, competence and educational needs, an independent public innovation fund (known as SITRA) which inter alia promotes the long-term perspective in Finnish decision-making through a National Foresight Network, and a number of futurists' or futures-oriented peoples' networks of which the largest is the Finnish Society for Futures Studies. There is no unified top-down foresight system in Finland but the GFR and Network, including sectoral reports by the key ministries, are key components of the national system of government.

Sweden: The Swedish Civil Contingencies Agencies Strategic Foresight Analysis focuses on issues within the field of societal security with a time perspective of up to 20 years, with the aim of supporting strategy formulation and long-term planning.

Five future scenarios produced in 2012 (for 2032) covered the following:

- a growing population and deteriorating public health;
- a weak economy, high unemployment and social unrest;
- accelerating climate change and rising oil prices;
- the threat of terrorism in a world of conflict;
- antibiotic resistant bacteria spread across the world.

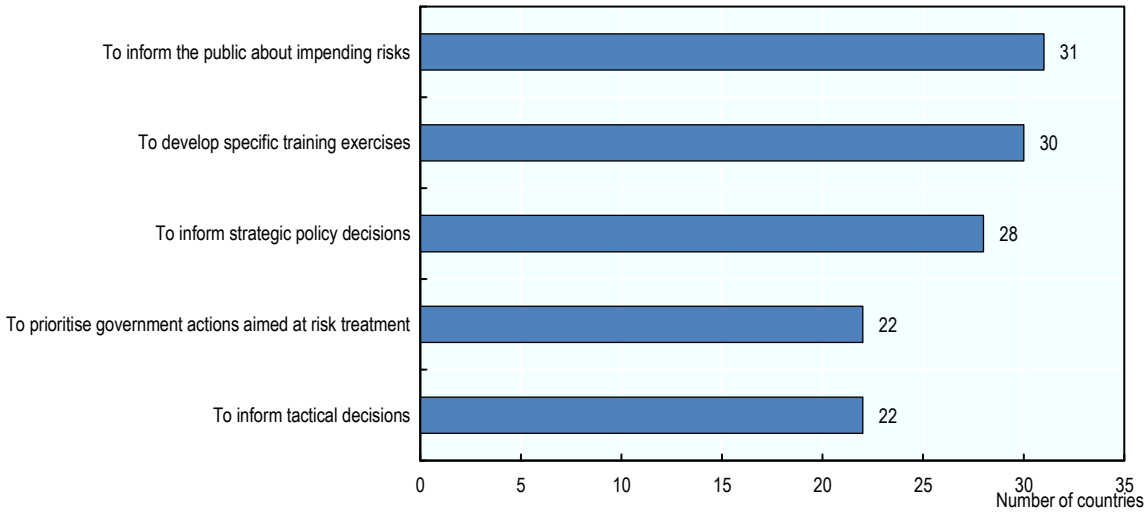
United Kingdom: Horizon-scanning arrangements in government were reviewed in 2012. Recommendations included establishing the Cabinet Secretary as "senior champion" and chair of a cross-government advisory group overseeing new or reinforced machinery for commissioning and discussing the policy implications of foresight/horizon-scanning work. The system in the United Kingdom includes a foresight team under the government's Chief Scientific Adviser, which has been merged with the Cabinet Office's horizon scanning secretariat since 2014.

United States: The Future Strategic Environment (US DHS Quadrennial Homeland Security Strategy) analyses future trends, challenges and uncertainties up to 20 years ahead. It also identifies key interdependencies, across society, technology, the economy, the environment and governance that can impact the ability to achieve homeland security objectives. The study sets the foundation for reflecting on how changes in five homeland security missions are carried out. A 2010 Strategic Foresight Initiative by the Federal Emergency Management Agency (FEMA) was designed to advance understanding of future risk trends and drivers through a three-phase collaborative programme of environmental scanning, scenario planning and aligning findings to strategy.

Source: OECD (2016d), "Preparing governments for long-term threats and complex challenges", www.oecd.org/gov/Preparing-governments-for-long-threats-and-complex-challenges.pdf.

Respondents noted that conducting risk anticipation capacity exercises can help optimally allocate scarce resources to improve efficiency throughout all phases of country risk management. They range from prioritising investments in disaster risk reduction to improving emergency management capabilities. The results of these risk anticipation efforts can also be used to raise awareness about risks and help create the basis for a deeper risk management culture.

Figure 3.2. How risk anticipation efforts are used by policy makers



Note: Answers were received from all 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Inventory exposed populations, assets and infrastructure

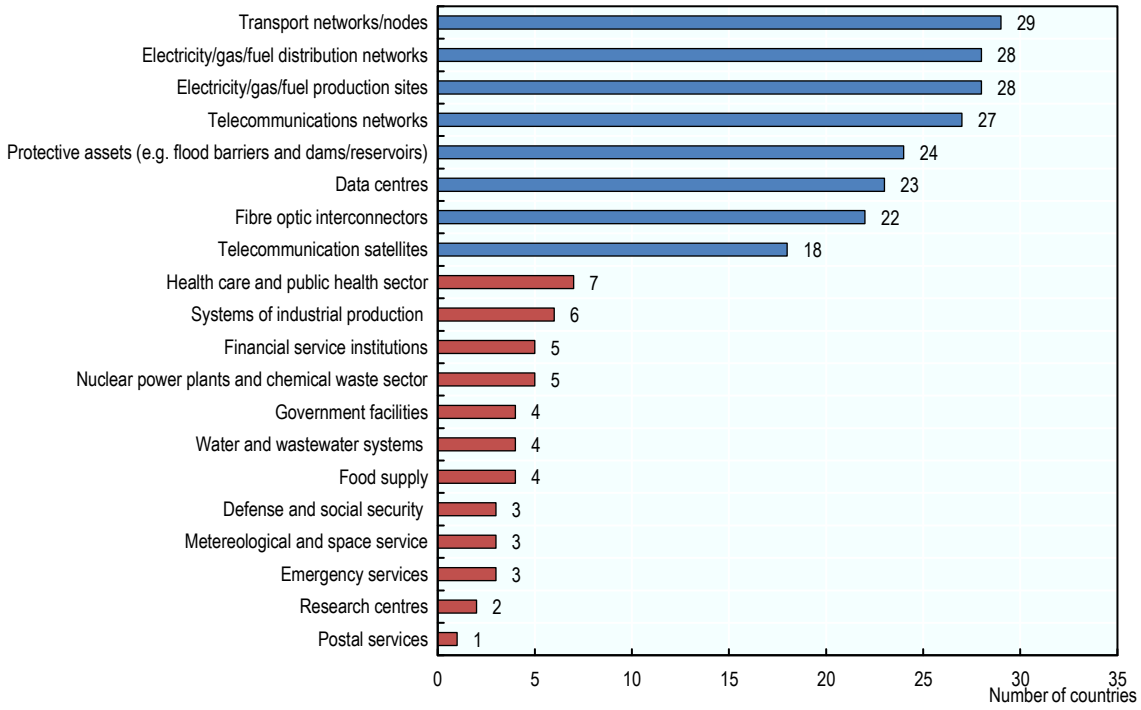
The Recommendation encourages countries to develop location-based inventories of exposed populations and assets, as well as infrastructure that reduces exposure and vulnerability. The assessment process should identify inter-linkages between different types of critical risks and the possible sequencing of hazardous events and cascading effects, which require cross-sectoral and even international co-operation. The rationale behind this provision is rooted in recognition that the security, economic stability and well-being of citizens depend increasingly on critical infrastructure networks and the services they provide to society.

New and complex threats highlight the need for closer co-operation between public and private actors to share knowledge and insights about interdependencies across these different sectors. National and international co-operation is needed, both on the strategic and operational levels, to safeguard critical infrastructure against terrorism, sabotage and natural hazards.

The definition of critical infrastructure and approaches to critical infrastructure protection vary across countries, though a high degree of similarity is observed. When asked, 31 respondents reported that they have designated specific infrastructure sectors as "critical", including for example transport networks, energy supply, dams and reservoirs, data centres, fibre optic interconnectors, and telecommunication satellites (Figure 3.3).

The governance of risk management policies in critical infrastructure systems is particularly challenging since in the majority of countries the private sector owns some 80% of the assets or manages their operations. To address this challenge, numerous countries have established a critical infrastructure protection (CIP) programme to assist owners and operators of critical infrastructure systems to co-operate with the government in site assessments and to address threats such as cyber, accidental or intentional man-made events and natural catastrophes. Typically these programmes identify critical infrastructure sectors and the assets that belong to them, and call for sharing information to strengthen emergency preparedness and public safety. The CIP programme of Canada (Boxes 3.3 and 3.4) can be seen as good practice and an effective template for countries that do not have such a programme.

Figure 3.3. Types of designated critical infrastructure systems



Note: Answers were received from 30 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Box 3.3. Regional Resilience Assessment Program: Canada

The Canadian Regional Resilience Assessment Program (RRAP) is a comprehensive risk assessment programme for owners and operators of Canadian Critical Infrastructure. This programme features site assessments to help organisations measure and improve their resilience to all hazards in Canada, such as cyber threats, accidental or intentional man-made events, and natural catastrophes. These site assessments are voluntary, non-regulatory, free-of-charge and confidential. To enhance critical infrastructure resilience, the RRAP uses three main tools:

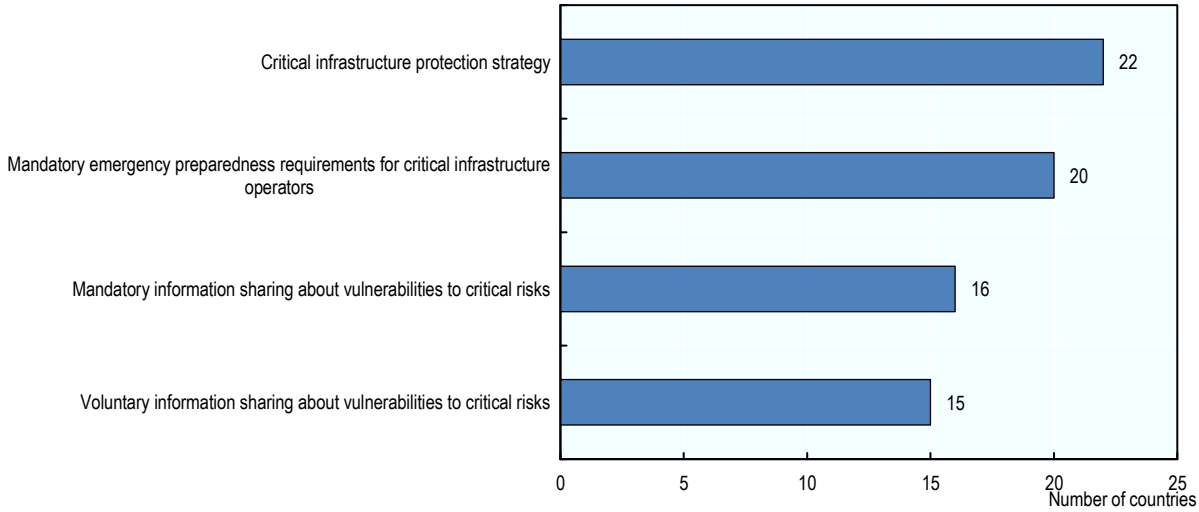
- Critical Infrastructure Resilience Tool: an on-site, survey-based tool that measures the resilience and protective measures of a facility
- Critical Infrastructure Multimedia Tool: a multiplatform software tool that generates an interactive visual guide of a critical infrastructure facility, featuring spherical photography
- Canadian Cyber Resilience Review: an on-site, survey-based tool that measures the cyber security posture of an organisation. The programme may include workshops, meetings, geospatial products and subject matter expert interviews.

Source: Public Safety Canada (2017), The Regional Resilience Assessment Program website, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

When respondents were asked how they foster effective partnerships with operators of critical infrastructure, 22 pointed to an established CIP programme. These programmes generally provide for scheduling regular meetings between government bodies and operators to ensure adequate information flows. In addition to or in some cases in lieu of regular meetings, 20 respondents reported that voluntary information sharing takes place, and 16 reported mandatory information sharing is in place.

Voluntary information sharing about vulnerabilities of critical risks can play an important role as a form of partnership where mandatory requirements are either considered not appropriate or not legislated. Examples of good practice in information sharing across public and private sectors can be found in Australia, Canada, Sweden, Switzerland, the United Kingdom and the United States where governments have been pro-active in providing platforms for regular co-operation. The trend of increasing threats of cyber-attacks has led the European Union to legislate for an incident reporting requirement and mandatory information sharing under the Directive on Security of Network and Information Systems (the NIS Directive), adopted by the European Parliament on 6 July 2016.

Figure 3.4. Partnerships with critical infrastructure operators



Notes: Answers were received from 29 out of 34 responding countries. Five countries also reported counterterrorism strategies.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Box 3.4. Good practice in developing national critical infrastructure strategies: Canada and Sweden

Canada: Strategy and action plan for critical infrastructure protection

The National Strategy for Critical Infrastructure sets the direction for enhancing the resilience of Canada's critical infrastructure against current and emerging hazards. It provides the framework for a collaborative approach whereby federal, provincial and territorial critical infrastructure activities are complementary and respect the laws of each jurisdiction.

The strategy outlines mechanisms for enhanced information sharing and information protection. These are key capacities to achieve the goals of a risk management-based approach to strengthening the resilience of critical infrastructure. These goals are pursued through a combination of security measures, business continuity planning and emergency management planning. Security measures address intentional and accidental incidents. Business continuity practices plan for disruptions by identifying and prioritising essential services in advance. And emergency management ensures adequate response procedures are in place to deal with unforeseen disruptions and natural disasters. At the national level, the strategy classifies critical infrastructure within the following sectors: energy and utilities, finance, food, transportation, government, information and communication technology, health, safety, water, and manufacturing.

Sweden: The National CIP Strategy

The goal of the National Critical Infrastructure Protection (CIP) Strategy is to strengthen the resilience of Sweden's critical infrastructure in a comprehensive way. Resilience refers to the ability to withstand disruptions and to maintain functionality as

far as possible or, failing that, to re-attain it. Resilience has the following four components:

- robustness of the systems themselves (critical infrastructure, society, economy and state)
- availability of redundancies
- ability to mobilise effective relief efforts
- speed and efficiency of relief efforts.

Based on these components, the goal of the National CIP Strategy is subdivided into two areas. The first relates to the initial component above: strengthening the robustness and flexibility of critical infrastructure and improving co-operation across and beyond critical infrastructure subsectors to in turn strengthen the robustness and flexibility of society, the economy and the state (national, regional and municipal agencies). The second area covers the remaining three components: ensuring that effective and rapid relief and redundancies are available in case of an adverse event. This two-fold goal can be attained by improving integrated protection through a concerted and co-ordinated approach among all actors. The measures of the National CIP Strategy of 2012 are currently being implemented and will be reviewed.

Sources: Public Safety Canada (2014), Action Plan for Critical Infrastructure (2014-2017), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-en.aspx; MSB (2014), Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, https://www.msb.se/RibData/Filer/pdf/27412.pdf; OECD (2017), Toolkit for Risk Governance website, https://www.oecd.org/governance/toolkit-on-risk-governance/.

Equip all of government to anticipate and manage human induced threats

This capacity is a key element to ensure a comprehensive all-of-government approach to managing critical risks. While countries demonstrate steady technological progress in the development of monitoring and early warning systems for natural hazards, the tools for anticipating human induced threats have not kept pace. Human induced threats include terrorist attacks, illicit trade and organised crime.

When asked how they anticipate human induced threats, for example terrorist attacks, respondents noted that they look to factors such as motive, opportunity and capability to anticipate attacks. These factors and criteria help untangle the many possibilities open to malevolent human choices. Several respondents cited national security considerations or a lack of available information as a reason not to provide information on this topic, yet the benefits of sharing information include enhanced tactical intelligence and public vigilance. A few respondents reported using analytical frameworks that also incorporate knowledge about the perceived vulnerability of potential targets at a specific time or place.

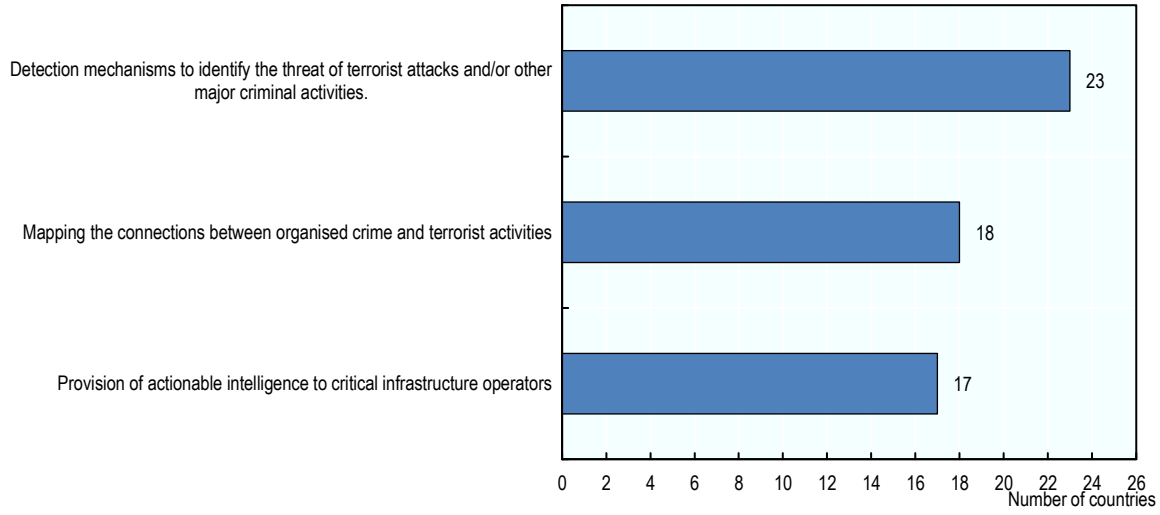
Twenty-three respondents reported having developed intelligence networks and other detection mechanisms to identify and assess the threat of terrorist attacks and other major criminal activities. But they provided no further information to describe them. Several respondents did report that they could not respond to questions about intelligence networks, either due to the classification of this information or because this information was not available to them. Eighteen respondents reported that they have adopted mechanisms to map the activities of actors in the illegal economy, which is intricately linked to terrorist financing.

The survey results revealed that countries look for patterns across previous malicious attacks to help glean insights about future threats, and thereby support better designed prevention policies and the targeting of resources to carry out protection plans. Analysis of patterns, however, is limited due to the low number of terrorist attacks. It could be enhanced if international partners increased access to their underlying data on a reciprocal basis.

Ten respondents did not provide any more detail about mechanisms to detect terrorist threats due to concerns about reducing the effectiveness of their methods. The survey responses often noted that confidentiality is an important barrier to information sharing, and that responding agencies would benefit from policy solutions that address this challenge. This is the case, for example, where inter-agency assistance is needed to respond to and recover from the increased threat of a terrorist attack or to diffuse organised criminal feuding that can injure or kill citizens.

Respondents showed that they do share specific information with the media that can raise public awareness, as this supports vigilance that can prevent or mitigate the deadly consequences of attacks. The media has played an important role in raising public awareness about common *modus operandi* in terrorist attacks, for example concerning the use of vehicles as weapons against crowds. This helps prepare the public to take precautionary measures under similar circumstances.

Figure 3.5. Measures to anticipate human induced threats



Notes: Answers were received from 23 out of 34 responding countries. Eleven countries did not respond but said either that this was confidential information or that the information was not available in their organisation.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Map the connections between criminal and terrorist networks

Organised crime has such adverse economic, social, environmental and even political impacts that many respondents consider it a critical risk. However, few countries map the linkages between organised networks, which can be gleaned through the supply, demand and laundering of proceeds from illicit markets. Mapping such activity does not

necessarily provide sufficiently detailed information to prevent or prepare for a specific criminal or terrorist act.

The countries that do conduct mapping have a clearer picture of convergence areas where international co-operation could focus its efforts. Creating choke points in these areas can deprive criminal networks of the capital required to continue and fortify their operational capabilities.

Investigate and assess damages and losses due to disasters

Several countries have a clear framework, set forth in disaster risk management plans and policies, on how to assess actual losses after disasters. Such assessments are useful to evaluate the cost effectiveness of disaster risk prevention and mitigation investments, as well as to estimate and better manage contingent liabilities in public finance strategies.

Several respondents provided specific examples of the value in systematically collecting loss statistics to inform policy making. For example, in Japan these statistics have enabled risk managers to show that over the course of the past decade public investments in disaster risk reduction have substantively reduced total damages and losses. Japan in fact presents a good practice in investigating and assessing damages and losses due to disasters. The Ministry of Land, Infrastructure and Tourism has a comprehensive accounting framework for floods in place that allows separate assessments of direct damages to private and public assets and losses caused by disruptions of public services and business operations based on a standard methodology. In the United Kingdom, a regularly updated flood damage assessment handbook has been published since 1977. Additional good practices can be found in Denmark, where flood damage assessments are based on approximate unit cost estimates, and in Australia, which adopted a Disaster Loss Assessment guideline that features a step-by-step loss assessment process using a unit-cost approach.

Twelve respondents reported that responsibilities for disaster loss data collection are centralised by one dedicated national body,[2] but only nine countries have developed a national repository for disaster loss and damage data. The most common practice is for different institutions to collect hazard-specific data. As a result, the quality of disaster loss and damage information varies significantly across countries.

Different institutions, from national to municipal level, are active in collecting data for economic losses from disasters. Canada, Colombia and Mexico have official nation-wide databases and provide good examples for the centralised collection of economic loss data from national ministries and provincial and territorial governments.

Only four countries answered that they collect disaster loss data for both natural and man-made hazards. Canada is a good example of centralised collection of disaster loss data for both types of hazards, and the data are made publicly accessible.

A clear area for improvement is the collection of economic losses and losses due to man-made hazards. Disaster loss information is collected for man-made disasters in Canada, Finland, Mexico and Turkey, but the databases in about half of the countries cover natural hazards only. The more common practice across countries is for different institutions to collect hazard-specific data. In Finland, for example, each ministry is responsible for collecting economic losses, depending on the type of hazard they are in charge of managing.

Minimise the impact of risks on public finances

Countries should plan for contingent liabilities within clear public finance frameworks by enhancing efforts to minimise the impact that critical risks may have on the fiscal position. Respondents pointed to a mix of practices when asked whether they established clear rules in advance of a disaster that clarify government plans on compensating disaster losses (Table 3.1). In Japan, explicit commitments are made for a wider range of losses compared to other countries. The response sample for this issue, however, is relatively small; the OECD Secretariat succeeded in collecting information from only 20% of countries.

Table 3.1. Examples of explicit commitments for post-disaster financial assistance

Country	Legal responsibility of the central government to finance disaster response and recovery	Cost-sharing arrangements between central and sub-national governments to finance disaster response and recovery	Legal responsibility of the central government for central government-owned public asset reconstruction and maintenance	Explicit liability of the central government to finance rehabilitation and reconstruction of private assets	Legal liability of the central government for other expenses incurred by sub-national governments (e.g. payments to businesses or individuals)	Government guarantees for disaster losses incurred by public corporations and PPP's
Australia	✓	✓	✓	✓	-	✓
Canada	✓	✓	-	-	-	-
Costa Rica	✓	-	✓	-	✓	-
Colombia	✓	-	-	-	-	-
Japan	✓	✓	✓	✓	✓	✓
Mexico	✓	✓	✓	✓	✓	-
New Zealand	✓	✓	✓	**Partially**	**Partially**	✓

Source: OECD/World Bank (*forthcoming*), Boosting financial resilience to disasters: understanding and strengthening the role of government

Respondents reported that implicit commitments arise especially after exceptional disaster events. So-called implicit contingent liabilities are expenditures the government makes in response to a disaster due to a perceived moral obligation for social welfare, rather than clearly established rules. In Japan, the scope of existing, explicit commitments have been expanded even further during "exceptional circumstances", such as after the Great East Japan Earthquake, which made the government shoulder a much greater share of the fiscal burden than it was legally obliged to. In New Zealand, the Canterbury earthquakes led the government to bailout a private insurance company and to provide several welfare benefits to the affected population, though neither action was based on a prior explicit commitment.

Respondents reported a range of different policy approaches to encourage households, businesses and insurers to take responsibility for disaster losses within the context of their resources. All countries plan for immediate relief assistance to households, such as providing temporary shelter and food, though the plan may be implemented by a mix of actions led by civil society and the private sector.

Government financial support for rehabilitating and reconstructing private assets, however, differs significantly across countries. In Australia, for example, support for private households affected by a disaster includes emergency response needs and also

compensation for demolition costs and rebuilding houses, without consideration of previous risk reduction arrangements.

The financial support made available to private businesses varies widely. A number of countries (such as Australia, Canada and Japan) provide low interest loans or interest rate subsidies to small and medium-sized businesses whose assets have been significantly damaged or that have foregone a significant amount of income.

Respondents pointed to post-disaster tax deferment programmes as another form of financial relief granted to households and businesses on a discretionary, event-by-event basis. While all respondents acknowledge the importance of providing support to businesses in the aftermath of disasters in an attempt to reduce more widespread or longer lasting negative economic impacts of disasters, none provided information about actually rewarding business continuity measures.

Estimate, account for and disclose contingent liabilities

The Recommendation calls on countries to establish mechanisms for estimating, accounting for and disclosing contingent liabilities associated with losses to critical sectors in the context of national budgets. Only a few respondents showed that they compile information to quantify and account for government contingent liabilities. Several respondents noted, however, that this type of information is collected at sub-national levels of government by different agencies and departments. New Zealand, for example, records information both on the central and sub-national governments' past response and recovery spending. This includes spending on the repair or replacement of damaged public infrastructure, on increased welfare benefits, on additional public resources allocated to recovery through special policies and on expenditures emanating from guarantees issued to the Earthquake Commission. However, this information is not compiled in a systematic manner to quantify New Zealand's overall fiscal exposure to disaster related contingent liabilities.

Transparency of disaster related contingent liabilities remains limited. Several countries have reported contingent liabilities and prepared a dedicated fiscal risk report, but few systematically disclose them. Where the liabilities are disclosed, this may be limited to a qualitative mention or to ongoing recovery payments rather than future expected government outlays. For instance, in Mexico the disclosure of the most relevant fiscal risks is required in the annual General Economic Policy Guidelines, which informs the central budget planning process. This includes a brief reference to natural disasters. In addition, past allocations from Mexico's major disaster recovery fund are publicly disclosed online.

Assess risk-related expenditures

Countries should adopt broad frameworks for recording and assessing disaster risk-related expenditures at national and sub-national levels. Few respondents provided information on recording such expenditures in public accounts or budgets as a separate item. This practice, however, is crucial to determine whether expenditures on disaster risk reduction projects and programmes are more cost effective than investing in emergency response. In addition, certain investments and expenditures on disaster risk reduction may be embedded in other projects, i.e. expenditure for a project may only partly pertain to disaster risk reduction.

Several countries have conducted national level studies of disaster risk-related expenditures,[3] but these are not a regular and continuous effort to retrieve expenditure information from sectoral budgets and different levels of government. For example, the Swiss National Platform for Natural Hazards conducted a onetime spending survey for disaster risk management, while in France the General Commission for Sustainable Development developed a onetime overview on *ex ante* disaster risk management expenditures.

Expenditures made at sub-national levels are often not reflected in these studies at national level. In Japan, for example, central government budget data for both *ex ante* and *ex post* disaster management expenditures is annually published in the "Disaster Management in Japan White Paper" (with the exception of data for civil protection activities), while data on sub-national post-disaster relief and recovery expenditures is collected in a separate process and not featured in the annual White Paper.

Key trends and self-assessment

All countries have identified the critical hazards and threats facing their territory and population, and they have implemented multiple measures to develop their capacity to anticipate risks. Countries have shown progress in preparing for critical risks through developing anticipation capacity. All countries reported that they have established some measures aimed at this, with emergency response exercises identified as the most common means to anticipate risks.

Respondents noted that exercises strengthen readiness and response and are a useful tool to conduct quality assurance of the response to emergencies and evaluation of the existing risk profile. Exercises provide an efficient means to test, evaluate, and improve planning. They allow for practice in a low risk environment for responders, emergency managers and senior officials at all levels of government.

The majority of countries have adopted a functional national risk assessment, or at least possess the expertise within line ministries to assess most forms of critical risks. Strong progress is observed across most countries in building preparedness through forward-looking risk assessments and early warning mechanisms that assist timely decision-making. Respondents reported that risk anticipation helps to set a clear context for risk assessment and to clarify where the focus of government should be in respect to changes in the risk environment in the future. An especially impressive finding is that 25 countries conduct research on emerging risks, which indicates an evolution and maturity in the disaster risk assessment processes. Local level risk assessments are carried out in 27 countries, which is also a positive development and supports effective response before, during and following a major disaster. The majority of countries indicated that they carry out horizon scanning and that this ensures that the portfolio of short-term risks is linked to decision-making and strategic early warning of events.

Relatively few countries have shown that their all-hazards, transboundary national strategy led to an improved understanding and identification of inter-dependencies between critical systems. Investments in research on hazard exposures and risk identification have enabled many countries to establish priorities for preparedness and planning, and to elevate the importance of investing more in risk prevention among the phases of the risk management cycle.

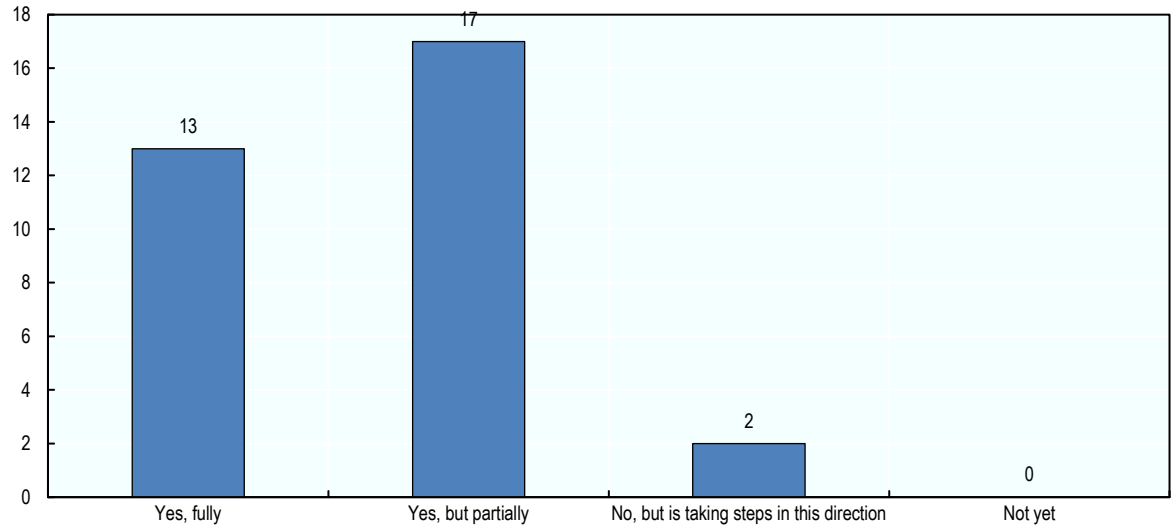
Countries use several means of partnering with the operators of critical infrastructure to achieve shared responsibilities aligned with their overall national

strategy for the governance of critical risks. Most such partnerships are structured within dedicated government strategies for the protection of critical infrastructure, which foster regular briefing meetings and strengthen trusted relationships between government agencies and private sector companies. Only about half the countries have established both voluntary as well as mandatory information sharing with critical infrastructure operators (Figure 3.5).

Respondents did not report widely on implanting capacities to anticipate and manage human induced threats, such as terrorist attacks, illicit trade or organised crime. This, however, is a key element to ensure a comprehensive all-of-government approach to managing critical risks.

Countries rated themselves relatively successful in fulfilling the second key recommendation: building preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impacts (Figure 3.6). Thirteen of the 34 responding countries believe they have fully met its provisions, while 17 believe they have fulfilled it partially. Only two countries answered that they have not fulfilled its provisions but are taking steps in that direction.

Figure 3.6. Self-assessment on implementing the second key recommendation



Note: Answers were received from 32 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Conclusions

Countries that have already established a national risk assessment should revise it in light of recent events, shifting priorities and new information, as called for by the Recommendation. **Countries that have not already performed an all-hazards national risk assessment should strengthen efforts to do so within the next five-year reporting period.** Multiple good practices are available to learn from fellow countries, including identifying risks and creating inter-ministerial working groups or a committee to conduct a government-wide portfolio of critical risks. Ensuring the right experts are involved helps to establish a common understanding of the assessment and to obtain consensus on the outcome of the exercise across government, and hence buy-in to the resulting action plan.

Countries could focus more on developing tools that identify and assess potential disruptions to hubs of critical infrastructure networks. Arrangements between government bodies and operators of critical infrastructure could be further developed to share information about vulnerabilities of critical risks. Such voluntary approaches play an important role as a form of partnership where mandatory requirements are considered inappropriate.

Due to the lack of detail received in the survey responses, it is unclear where countries stand overall in terms of cross-border co-operation to anticipate and manage human induced threats, such as terrorist threats, illicit trade or organised crime. Increasing levels of human induced risks in many countries, however, underscore the need to enhance these capacities through international co-operation. This could be furthered concretely by integrating multiple information sources to map the web of people, companies, trading routes and transactions that define the networks involved in such nefarious activities.

Note

[1] See SONAR: www.swissre.com/library/expertise-publication/swiss_re_sonar_new_emerging_risks_insights_2017.html.

[2] The following 17 countries responded to the 2016 OECD Survey of Disaster Loss and Damage: Australia, Austria, Canada, Colombia, Costa Rica, Denmark, Estonia, Finland, France, Japan, Israel, Mexico, Norway, Poland, Slovak Republic, Sweden and Turkey.

[3] Ibid.

References

Commission for Consultation of Sector Councils (2008), Horizon Scan Report 2007: Towards a Future Oriented Policy and Knowledge Agenda, The Hague.

European Commission (2010), "Risk assessment and mapping guidelines for disaster management", Commission Staff Working Paper, SEC(2010) 1626 final, http://ec.europa.eu/echo/files/civil_protection/civil/pdfdocs/prevention/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf.

Irish Department of the Taoiseach (2017), "National Risk Assessment 2017: Overview of Strategic Risks", Dublin, https://www.taoiseach.gov.ie/eng/Publications/Publications_2017/National%20Risk%20Assessment%202017%20-%20Overview%20of%20Strategic%20Risks.pdf.

MSB (2014), Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, Swedish Civil Contingencies Agency, https://www.msb.se/RibData/Filer/pdf/27412.pdf.

OECD (2017), Toolkit for Risk Governance website, https://www.oecd.org/governance/toolkit-on-risk-governance/.

OECD (2016a), OECD Survey on the Governance of Critical Risks, OECD, Paris.

OECD (2016b), Toolkit for Risk Governance: National Risk Assessment in the Netherlands, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/nationalriskassessmentinthenetherlands.htm.

OECD (2016c), Toolkit for Risk Governance: Ireland National Risk Assessment 2015 − Overview of Strategic Risks, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/irelandnationalriskassessment2015-overviewofstrategicrisks.htm.

OECD (2016d), "Preparing governments for long-term threats and complex challenges", discussion note for the High Level Risk Forum Policy Seminar, 23 September 2016, www.oecd.org/gov/Preparing-governments-for-long-threats-and-complex-challenges.pdf.

OECD/World Bank (forthcoming), Boosting financial resilience to disasters: understanding and strengthening the role of government, jointly developed by the OECD and the World Bank Group for the APEC Finance Ministerial Meeting, October 2017.

Public Safety Canada (2017), The Regional Resilience Assessment Program website, Government of Canada, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

Public Safety Canada (2014), Action Plan for Critical Infrastructure (2014-2017), Government of Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-en.aspx.

Chapter 4. Critical risk reduction, prevention and communication

This chapter reports on the implementation of the third key OECD Recommendation of the Council on the Governance of Critical Risks. This Recommendation calls on countries to raise awareness of critical risks to mobilise households, businesses and international stakeholders and foster investment in risk prevention and mitigation. The chapter begins by examining risk communication policies that countries have carried out in accordance with the Recommendation. It then reviews their actions to develop a mix of structural and non-structural protection measures. The chapter concludes with suggestions for further engaging the private sector, reducing disaster risks reduction and increasing partnerships for national resilience.

Good practices and policy tools

Risk communication is a fundamental element of a sound risk management framework that seeks to reduce future losses and damages from disasters. Without strong risk communication, the public may underestimate some risks, and thus take insufficient precautions, and overestimate others, leading to sub-optimal allocation of resources. The third key recommendation emphasises the responsibility of governments to (i) engage the whole of society to increase the awareness of households, businesses and communities about their exposure to risk and their vulnerabilities, and (ii) inform them of specific prevention, mitigation and preparation measures they could take. Such knowledge can also spur an informed debate on the need for public investment in prevention, mitigation and preparedness and is thus a key element of good governance in risk management policy.

Encourage a whole-of-society approach to risk communication

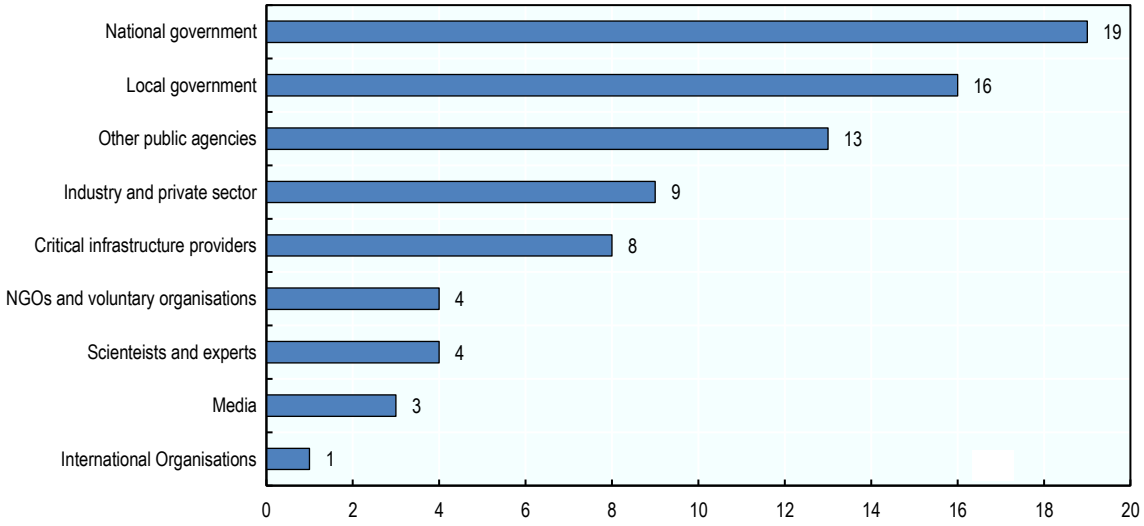
The Recommendation promotes communication that facilitates transboundary co-operation using risk registries, media and other public communications on critical risks. Respondents to the OECD Survey on the Governance of Critical Risks were asked about the range of actors that have been assigned formal responsibilities for risk communication.[1] All 34 responding countries assign central government a lead in communicating risks (Figure 4.1), and 16 indicated that this responsibility is shared with sub-national governments. Sharing responsibility for communicating about risks with sub-national levels of governments is essential to tailor messages to local conditions.

Only about half of respondents indicated that the private sector has a formal role in risk communication. The most obvious formal roles belong to media companies that conduct planned public service announcements or broadcast information to inform the public when an incident poses a safety threat to the wider public. Operators of critical infrastructure are another type of private sector actor that often has a formal role in risk communication, for example chemical plants and nuclear power stations in the case of an accident.

A good practice example of private sector risk communication can be seen in countries of the European Union having implemented the Seveso Directives. These directives spell out responsibilities for risk communication stemming from hazardous private sector activity that should be channelled through public authorities to inform potentially affected populations.

Respondents also pointed to various forms of private sector engagement that provide raw data and information in support of risk communication. For example, countries have partnered with private research institutes and monitoring services as suppliers of raw data and information for public services to broadcast. In France, the *Mission Risques Naturels* has established partnerships and platforms for exchanges between public authorities and private sector actors to discuss risk communication strategies and to jointly train actors responsible for risk communication.

Figure 4.1. Actors with formal responsibilities for risk communication



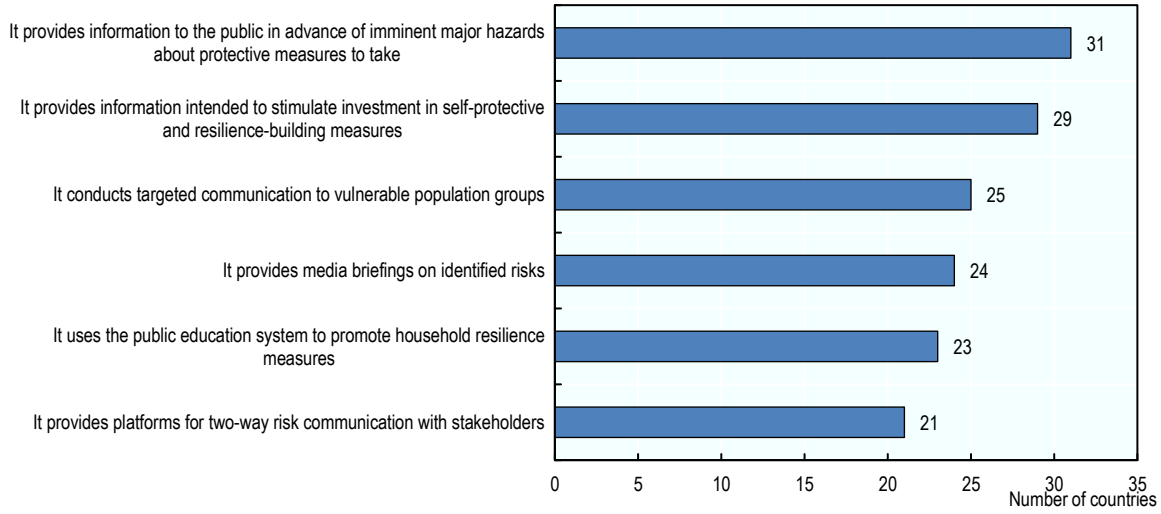
Note: Answers were received from 19 out of 34 responding countries.
Source: OECD (2015), OECD Survey on Risk Communication Policies and Practices.

Surprisingly, only one respondent pointed to international organisations as a source of risk communication, despite the fact that the World Health Organisation, the World Meteorological Organisation, UNESCO and many other organisations have well-developed programmes for communicating to governments about pandemics, hydro-metrological risks and tsunamis. Inside the OECD, the Working Group on Chemical Accidents (WGCA) provides a platform for the chemical industry and regulators to discuss industrial safety issues. The group issued guidelines for all stakeholders that are potentially affected by chemical accident prevention, preparedness and response (OECD, 2003). The objective is to engage private industry leaders to accept some responsibility for the consequences industrial accidents may have on societies and economies. The WGCA has organised training seminars for top industry leaders in Canada, Sweden and the United Kingdom to engage industries to better prepare for major industrial accidents.

When respondents were asked how they encourage a whole-of-society approach to risk communication, almost all replied that they provide information to the public about imminent disasters and emergency preparedness measures that need to be taken (Figure 4.2). Even though traditional communication channels are important to reach a broad audience, social media is increasingly used to foster awareness and empower people to react to disasters. In New Zealand, for example, the Ministry of Civil Defence and Emergency Management communicates about tsunami preparedness measures through Twitter. The country's "Long or Strong" campaign instructed recipients on preparedness measures based on the first signs of a tsunami occurrence.[2]

Twenty-nine respondents reported that they engage in risk communication to stimulate investment in risk prevention and mitigation measures. Distribution of pamphlets and outreach material is a common tool. For example, in Italy the "Civil Protection in the Family" pamphlet is distributed at national level, and the city of Naples' distributes a multi-risk pamphlet called the "Emergency Exit" to inform the local population about preparing for disasters and where to evacuate in case of particular events.

Figure 4.2. Communicating about risks, risk prevention and emergency preparedness



Note: Answers were received from 33 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Table 4.1. Aims of strategies that encourage a whole-of-society approach to risk communication

	Foster inclusiveness		Encourage self-protective measures		Promote two-way communication	
	Target communication to vulnerable population groups	Promote household resilience measures through the public education system	Provide information to stimulate investment in self-protective and resilience-building measures	Inform the public in advance of imminent major hazards about protective measures to take	Brief the media on identified risks	Create platforms for two-way risk communication with stakeholders
Australia	○	○	●	●	●	●
Austria	○	●	●	●	○	●
Canada	●	○	●	●	●	●
Chile	●	●	●	●	●	○
Denmark	○	○	●	○	○	●
Estonia	○	○	○	●	●	○
Finland	●	●	●	●	●	●
France	●	●	●	●	●	●
Germany	●	●	●	○	●	○
Greece	○	○	●	●	○	●
Iceland	●	○	●	●	●	●
Ireland	●	●	●	●	●	○
Italy	●	●	●	●	●	●
Japan	●	●	●	●	○	●
Korea	●	●	●	●	●	●
Latvia	●	●	○	●	○	●
Luxembourg	●	○	○	●	●	○
Mexico	●	●	●	●	●	●
Netherlands	●	●	●	●	●	●
New Zealand	●	●	●	●	●	●
Norway	●	○	●	●	●	○
Poland	x	x	x	x	X	x
Portugal	○	●	○	●	○	○
Slovak Republic	○	●	●	●	○	●
Slovenia	●	●	●	●	●	○
Spain	●	●	●	●	●	○
Sweden	●	●	●	●	●	●
Switzerland	●	●	●	●	●	●
Turkey	●	●	●	●	●	○
United Kingdom	●	○	●	●	○	●
United States	●	●	●	●	●	●

Source: OECD (2016a), OECD Survey on the Governance of Critical Risks

Use two-way communication between government and stakeholders

Governments should use two-way communication with stakeholders, ensuring that information sources are accurate and trusted. Two-way communication between message providers and message receivers builds trust and credibility that one-way transfers of

information cannot. Two-way communication allows unique local characteristics and diverse communities, sectors, industries and international actors to be taken into account. Twenty-two countries reported that they provide platforms to facilitate two-way risk communication with stakeholders.

The challenge facing risk communication about extreme events is that the messages are often forgotten by the time a disaster event takes place. Social media is increasingly used as a channel for effectively fostering a dialogue about risks, for example by creating an interactive electronic platform. Many countries, including France, Korea, Norway and Switzerland, use social media to allow stakeholders to provide feedback to risk management authorities and to facilitate interactions. Similarly, Turkey has established a web-based portal for citizens to communicate with civil protection authorities.

Conduct targeted risk communication

Different population groups have different needs that have to be taken into account for risk communication to be effective. For example, elderly people may have physical constraints to hearing broadcasts or seeing posters, billboards and other signs meant to raise awareness about risk exposures or actions to take during an imminent emergency. Countries have developed communication strategies tailored to vulnerable groups. For example in Norway, fire hazard exposure is communicated with specific attention to the elderly and disabled. In Turkey, the Disaster and Emergency Management Authority developed a mobile phone application to inform all citizens about past and imminent earthquake events, with special applications for visually impaired people.[3]

Having learned from the heatwave in 2003 that caused an estimated 15 000 deaths in France alone (INSERM, 2004), public authorities now pay special attention to targeting communications about heatwaves to vulnerable groups such as children and the elderly. The Ministry of Health in France provides materials online that can be used by any group engaged in risk communication efforts to communicate to specific target groups.

Some countries have tailored their strategies to tourists. In Greece, the civil protection authorities design communication strategies to inform tourists and translate risk information into different languages. Similarly, in Italy the civil protection authorities publish pamphlets in English and distribute them widely to tourists visiting vacation areas exposed to natural hazards. These pamphlets provide information about the types and likely locations of extreme weather conditions that can endanger their activities. They also provide information on prevention and self-protection measures to take.

Inform and educate the public

The Recommendation calls on countries to inform and educate the public in advance of a specific emergency about what measures to take when it occurs. Countries should mobilise public education systems to promote a culture of resilience by integrating community resilience skills and concepts into curriculums and thereby pass information on to households through students. Twenty-three countries pointed to their use of the public education system to promote household resilience measures (Figure 4.2).

In Latvia, for example, all university students are required to participate in emergency training courses. As of 2020, the courses will be expanded into secondary education. In support of these courses, the Latvian Fire and Rescue Service developed comprehensive information material and posters that can also be accessed online.[4] To engage with citizens beyond the mandatory training, the Latvian Fire and Rescue Service also uses

social media channels, such as Facebook and Twitter, to share information on self-protection measures.

Austria's Civil Protection Association (*Zivilschutzverband*) organises events at schools to raise children's risk awareness and enhance their preparedness. For example, it has held the Children's Safety Olympics every year since 2000 to teach children how to behave in emergency situations and how to avoid dangers in daily life.[5]

Whereas adults can more readily process straightforward factual information, communicating about risks to school children may require metaphors and stories to convey meaning with nuance and empathy. Since 2009, Mexican primary school programmes have integrated risk management into their curriculums in history, ethics, Spanish, natural sciences, mathematics and geography. Furthermore, free books that include prevention information are distributed to each level of the primary education cycle.

In France, a network of 500 trainers spread across the 30 school districts informs and trains education professionals on how to manage critical risks. There is a particular focus on risks faced by schools.

The Recommendation suggests making risk information accessible in a manner appropriate to diverse communities. Respondents revealed several good practice examples of how sub-national authorities have effectively engaged in tailoring messages for their communities. The United Kingdom's Met Office conducts specific campaigns for particular areas to take into account local prevailing conditions, such as the "Ready for Winter?" campaign developed to help people living in areas vulnerable to cold weather conditions. In France, the Local Community Information Document described in Box 4.1 is an effort to raise awareness of prevailing conditions at the municipal level. In Japan, municipalities are obliged to disseminate hazard maps to the public that indicate evacuation routes to be taken and anticipated safe meeting points. In many municipalities, citizens participate in establishing these maps.

The Canadian "Get Prepared" public awareness campaign encourages Canadians to prepare themselves to overcome the first 72 hours of an emergency without assistance. This enables first responders to focus on those in immediate need first and increases the effectiveness of relief activities. To reach a wide audience, the campaign works closely with the provinces and territories, as well as with non-government organisations. Since 2016, an annual Emergency Preparedness Week held in all provinces has complemented the campaign.

In Italy, particularly exposed municipalities have published and distributed risk awareness pamphlets. Pamphlets provided by the city of Portici explain the risk of an eruption of Vesuvius, including likely lava flows and evacuation routes.

Box 4.1. Local community document about major risks: France

France introduced the *Document d'information communal sur les risques majeurs (*DICRIM) in 1990. Every community subject to a Risk Prevention Plan must draw up an information document about the safety measures to take in the event of a potential threat. The mayor and the municipal council are responsible for the DICRIM. The document is tailored to the locally prevailing hazards and includes information on the following:

- natural and technological risks
- measures taken by the municipality to reduce risk exposure
- safety measures to be follow in the event of an emergency or an alarm (for example, taking behavioural measures, securing assets from areas at risk, and mounting electricity and gas counters above a potential flooding level)
- critical public infrastructure (including retirement homes and schools)
- landowners' and renters' obligations to communicate about the safety measures stipulated in the DICRIM.

The objective of the DICRIM is to raise awareness among citizens about local major risks which they could be exposed to. The DICRIM informs citizens about the nature of the threats, their potential consequences, and the measures they can take to protect themselves or reduce their exposure and potential damages. The DICRIM encourages inter-municipal hazard analysis, on which local land use restrictions can be informed.

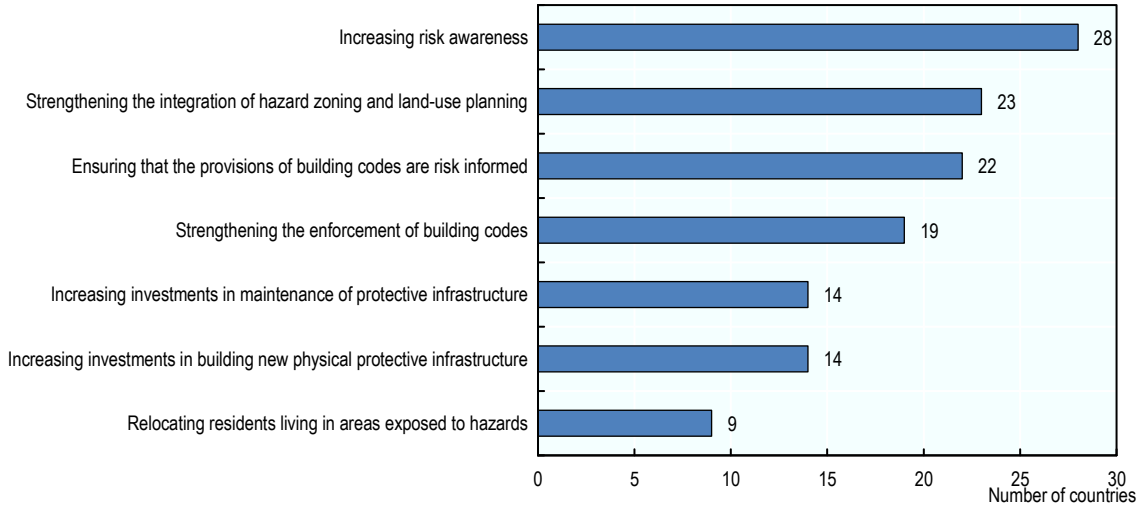
Source: French Ministry of Ecology (2009), "Le document d'information communal sur les risques majeurs (DICRIM)", www.prim.net.

Strengthen the mix of structural protection and non-structural measures

Generally, both structural and non-structural measures aim at limiting the exposure of people and core services to known hazards and at reducing their vulnerability. Structural measures seek to reduce disaster impacts through engineering or civil work prevention measures, such as retention walls, dykes and dams for floods or storm surges. Non-structural or organisational measures encompass hazard zoning, spatial planning, building codes and their enforcement, risk communication measures, and business continuity planning. Other physical measures are used on an emergency needs basis, such as mobile protection measures used in the event of floods, or automatic weather stations to provide early warning information.

Respondents reported that non-structural or organisational measures are more often a priority than structural ones (Figure 4.3). They ranked increasing risk awareness, strengthening risk-informed land-use planning and enforcing building codes as relatively more important than investing in or maintaining structural measures. This result reflects a healthy policy mix that acknowledges the limits of structural risk prevention measures and that embraces the value of organisational measures. Immediate comparisons of priorities across countries are difficult to make as exposures to risks vary and may require different measures to address them. Historical legacies in risk reduction may also contribute to priorities shifting from one country to another. The marginal value of additional investment may be low in some areas which benefited from high past investment, while others may yield greater returns.

Figure 4.3. Countries' priorities in strengthening risk prevention and mitigation



Note: Answers were received from 29 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

When asked, only 14 countries reported that "increasing investments in physical protective infrastructure" is a priority for their risk reduction policy mix (Figure 4.3). The same number ranked "maintaining protective infrastructure" as a risk reduction priority. These stated priorities reflect the views of respondents who represent central governments, and not necessarily those of sub-national governments in charge of maintaining physical protection measures.

The cases of Austria and France illustrate these points. In Austria, where the central government co-finances about half of structural protection investments, demand from municipalities for protective measures has exceeded the supply that can be co-financed by the central government by about 40% in recent years. In France, the current demand and supply for structural investments are more or less equal. However, French authorities expect future demands for protective infrastructure investments from the sub-national levels to increase. This is due partly to increasing exposure to risks and partly to a backlog because of the time it has taken sub-national authorities to put their requests and planning documents together to have access to central co-financing.

Several respondents commented that they have to compete for available resources to invest in structural protection measures. For any public investments, but especially those made in environments of competing resources, funding should be allocated equitably and efficiently based on priorities. Respondents identified tools that help to evaluate costs and benefits of such measures. Exhaustive evaluations of direct and indirect costs and benefits are often undertaken for large investments. This is the case, for example, for investments exceeding EUR 1 million in Austria and EUR 2 million in Switzerland. Standard costs and benefits include costs for items such as construction and maintenance and benefits for items like avoided damages to buildings or to critical infrastructure.

Respondents find it particularly challenging to address criteria that are as important as protecting lives but are also so difficult to value monetarily. Austria has addressed this issue by including intangible benefits on a point scale as an add-on to the results of the standard cost-benefit analysis. This makes comparison complex but at least ensures that

such criteria are taken into consideration. In France, alternative methods are proposed, such as multi-criteria analysis for investments in flood management measures. The analysis enables project owners to not only assess the economic cost and benefits of a project but to also evaluate the intangible impacts that are difficult to monetise, e.g. on human health, the environment or cultural heritage. In Switzerland, the online tool "EconoMe 4.0"[6] allows standardised cost-benefit analysis of complex projects. Social standards and environmental requirements are equally taken into account, and in many cases the project proposal also undergoes public consultation processes.

Countries noted that where there is high exposure to intense natural hazards they have already built a large stock of protective infrastructure. The challenge has been to ensure adequate maintenance through rehabilitation and strengthening projects to preserve the level of protection for which the infrastructure was initially conceived. While allocations for structural measures may be a fixed part of sectoral budgets, they do not, or only to a limited extent, include a budget for the maintenance expenses.

In some countries, such as Austria, maintenance costs are budgeted into the initial project allocation that is co-funded by the central government, but after some years these costs have to be covered by sub-national government or the immediate beneficiaries of a protective infrastructure. Devolving this responsibility is common practice, even in relatively more centralised administrative systems like France. The costs of such significant investments exceed the fiscal capacity of sub-national governments and groups most at risk. Without maintenance of the protective infrastructure, the choices remaining include to accept the risk, reduce vulnerability or move.

With an increasing stock of protective infrastructure and growing budget constraints, including at the local level, the sub-national responsibilities for maintaining protective infrastructure have become a challenge. At sub-national level, financial resources and technical capacities can differ across jurisdictions. This can produce different levels of quality in maintenance and hence affect protection levels in the future.

Recognising these risks, countries have tried to examine the problem more systematically and set up a central monitoring mechanism. In Austria, the Ministry of Environment developed a central database that contains some 270 000 protective infrastructure. It holds information on their physical dimensions, an assessment of their condition, and documentation on monitoring, inspections, corrective maintenance, rebuilding and other modifications. In 2011, the United States Army Corps of Engineers created the National Levee Database, which contains up-to-date and publicly available information on the location, condition and maintenance of the majority of dikes and dams built across the country. An online mapping tool illustrates the information. In Mexico, the General Directorate of the Fund for Natural Disaster (FONDEN) manages a database of federal infrastructure, including those designed to protect against major hazards and any that have received funds for rehabilitation following damages from disasters.

Respondents pointed to privately-owned assets that provide safety and protection to the public against damages from natural and man-made disasters as a grey area of government responsibility. Some countries have begun to require populations that are direct beneficiaries of protection to share in the cost of maintenance for investments in disaster risk prevention. Bottom-up initiatives, like the water boards in Austria (Box 4.2), have shown to be effective in unlocking additional investments and enabling long-term ownership.

Respondents noted the downside of tying maintenance funding to cost-sharing agreements. Only wealthy communities increase their level of protection. Also a significant amount of available funding goes unused every year, because lower income communities generally do not apply for support.

Box 4.2. Bottom-up risk prevention initiative: Water boards in Austria

Water boards are statutory corporations under Austrian law (Water Act of 1959) and can be composed of any number and combination of individuals, municipalities or companies. Each member contributes financially to a common fund, which is used for developing and maintaining mitigation or prevention measures. The readiness to financially contribute to infrastructure investment can be considerable. For example, in the case of the Saalbach (province of Salzburg) water board, which is relatively big with 600 members, individual contributions can reach EUR 50 000 annually. The level of contribution is determined by a point system derived from the exposure of a member's property or dwelling.

Water boards may decide to take responsibility for co-financing sometimes costly protective infrastructure, instead of leaving this to local authorities. There are several advantages for taking such an initiative. For example, water boards can expedite the request for a protective infrastructure, which serves the interests of those directly impacted by hazardous events. Water boards, like municipalities, can initiate and request the construction of protective infrastructure, and thereby oblige its members to finance the measures. In the case of the torrent and avalanche control, water board investment proposals are treated faster and at a higher central co-financing rate than requests submitted by local government. The difference can be as high as 15%, thus rewarding individual willingness to contribute to financing protective infrastructure.

As water boards become the formal owners of the protective infrastructure they build, they are responsible for maintaining it. This has led to significantly better upkeep of protective infrastructure over time, compared to infrastructure for which maintenance is the responsibility of other interest groups, such as municipalities, that may face resource challenges. Considering the longer-term maintenance requirements of protective infrastructure investment, municipalities may encourage investment by water boards.

Source: OECD (2017a), "Boosting resilience through innovative risk governance: The case of Alpine areas in Austria", http://dx.doi.org/10.1787/9789264281370-5-en.

Invest in prevention and mitigation

The Recommendation calls on countries to reinforce investment in prevention and mitigation efforts that limit the exposure of people and core services to known hazards and reduce their vulnerability. In comparative terms, respondents ranked organisational risk prevention measures, such as the integration of hazard zones and of land-use planning and the enforcement of building code provisions, as a higher policy priority than structural prevention measures (Figure 4.3). This survey finding reflects the recognition among countries that they have achieved a level of diminishing returns in structural risk reduction measures. To form an optimal policy mix for disaster risk reduction, countries are giving more priority now to non-structural measures, such as risk communication, hazard zone mapping, risk mapping, spatial planning or building code enforcement.

Countries have made significant and rapid progress in covering their territories with updated maps to identify and assess hazards, heavily emphasising natural hazards. Countries such as Austria and Switzerland have made hazard information publicly accessible via online platforms that provide exposure information for individual postal address locations. In Germany, the German Insurance Association provides a similar address-based service for natural hazards that complements online platforms and applications created by sub-national authorities. Similarly, information on technological hazards can be accessed on a platform run by the Central Reporting and Evaluation Office for Major Accidents and Incidents in Process Engineering Facilities.

In France, hazard information is proactively provided to buyers of real estate as part of the legally required disclosures during the purchasing process. The persisting challenges have been to keep hazard information regularly and sufficiently updated.

Box 4.3. Informing about hazards: The United Kingdom's Natural Hazard Partnership

The United Kingdom's Natural Hazard Partnership (NHP) is a collaboration between 12 technical and scientific agencies and 5 government partners. It provides a forum for exchanging data, information and outcomes of risk analysis. The partnership also contributes to the national risk assessment, which identifies new hazards and advises on worst-case scenarios.

Through a comprehensive website, the public can access easily understandable information on all relevant hazards, ranging from flooding and extreme weather to earthquakes and wild fires. In addition to the general hazard information available on the website, the NHP provides Daily Hazard Assessments, which describe all potential natural hazards and health implications that could affect the United Kingdom over the following five days. A general outlook that covers the following 30 days complements the DHA.

Since its creation in 2011, the NHP has significantly improved the co-ordination among different stakeholders, avoiding duplication and overlaps, which had previously been a challenge. During the 2007 floods, for example, the overlapping mandates of the multiple agencies involved hindered efficient data and information sharing.

Source: OECD (2017b), Toolkit for Risk Governance: UK Natural Hazard Partnership, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/uknaturalhazardpartnership.htm#tab_description; NHP (2016), The Natural Hazards Partnership website, www.naturalhazardspartnership.org.uk/.

Hazard maps can be improved in the future to reflect the continuous changes and arising complexities in disasters. They can be strengthened in two ways:

- By harmonising and integrating maps across different hazards: Hazard maps across countries have often been developed by different authorities in charge of managing different types of hazards. This is true for natural as well as man-made hazards. In the United Kingdom, the Natural Hazard Partnership (Box 4.3) has addressed the challenge of hazard mapping by integrating hazard information provided by the participating public bodies and research institutes.
- By including cascading impacts across different types of hazards: There is significant scope to integrate potential cascading effects in the traditional mapping

process. Switzerland has made concerted efforts to better identify and assess scenarios of extreme disasters. The EXAR project described in Box 4.4 illustrates this.

Box 4.4. Evaluating extreme flood risks: Switzerland

In 2013 the Swiss Federal Offices for the Environment, Energy and Civil Protection as well as the Federal Nuclear Safety Inspectorate launched the 'Hazard information for extreme flood events on the rivers Aare and Rhine' project. It aims at establishing a common baseline to evaluate the risks of extreme flood events for infrastructure built close to the rivers Aare and Rhine. In the beginning phase of the project, data were collected and methodologies developed that enable a standard evaluation of extreme flood events along the two rivers. The data includes gauge height, flow velocity, morphological changes of the rivers and flood recurrence probabilities. Projections are based on estimated return periods of 10 000 years.

The initial ground work established the evidence base for modelling extreme flood events of the Aare. In 2016 the Federal Office for the Environment commissioned a study to evaluate interaction scenarios or cascading impacts of extreme flood risk events. These include erosion, landslides, blockages through floating refuse and dyke breaches. The objective of this study is to understand vulnerabilities of infrastructure.

Source: FOEN (2016), Beurteilung der Gefährdung durch Extremhochwasser der Aare: Hauptstudie lanciert. [Evaluation of extreme flood hazards along the Aare: Main study launched], Federal Office for the Environment, Switzerland www.bafu.admin.ch/dokumentation/medieninformation/00962/index.html?lang=de&msg-id=60609.

Integrating hazard maps into land-use planning is a core step in reducing the exposure of people and assets to hazards. Preventing people from settling in hazard-prone areas is the most efficient way to avoid exposure to risks. However, scarcity of land for settlements and a desire to increase densification to achieve higher economies of scale create tensions between land-use and hazard zone planning.

In many countries, hazard-prone areas were settled long before detailed hazard information became available. Nevertheless, hazard mapping can guide retrofitting measures and any repair or expansion work that may be undertaken. To effectively inform land-use decisions, hazard information needs to be available at the local level by parcel of land and must be frequently updated to reflect changes in prevalent risks and risk levels.

Build safer communities

The Recommendation promotes building safer and more sustainable communities by co-ordinating risk management and urban planning to reduce the concentration of people and assets in areas of known exposures. Respondents pointed to challenges they face in applying knowledge of risks in land-use planning and decisions. Information on hazard exposures is not always legally binding for land-use decisions, and several respondents noted that government officials at a sub-national level choose whether to take it into account. This is the case, for example, in Austria, Costa Rica, France and Switzerland. One respondent reported that local authorities failing to consider hazard exposures in issuing construction permits have been the subject of lawsuits in the aftermath of recent

disasters. In one case, people died, and negligent homicide charges were brought against the authorities.

Integrating hazard information into land-use planning decisions has been most successful in high-risk areas where construction bans have been issued and enforced (Box 4.6). Recent disasters have confirmed that damages have been reduced in those areas.

However, in some countries where integrating hazard information into land-use decisions is considered good practice, a relatively higher accumulation of damages occurs in areas deemed as lower risk areas. Analyses have shown that more than 50% of insured damage claims[7] have been filed in minor hazard zones, where no specific land-use requirement was previously issued. This implies that protection or stricter regulations might have been overlooked in those zones.

Box 4.5. Integrating land-use planning in hazard assessments: France

In France, hazard mapping is used in developing Prevention Plans against Natural Risks (PPRNs). The plans outline hazard zones for possible earthquakes, floods, avalanches, wildfires and landslides. To evaluate flood risks, PPRNs take into account obstacles that could prevent the river flow, including in retention zones. Local offices of the Ministry of Ecological Transition and Solidarity (*Directions départementales des territoires*) and public engineering bureaus are responsible for hazard mapping. The hazard maps are publicly accessible, and the public as well as sub-national authorities and other stakeholders participate in the hazard mapping process.

Hazard maps are regularly included in land-use planning. The spatial development code requires local authorities to take hazard maps into consideration when preparing spatial planning documents and to include a Risk Prevention Plan as an annex. Flood Risk Prevention Plans go even further; they establish clearly designated areas where construction is not allowed.

Mayors are responsible for enforcing hazard zones in land-use decisions, and they are in charge of granting construction permits. At the department level, the prefect monitors the integration of hazard zones in urban planning decisions. In case of doubts about whether a major respected a hazard zone in granting a construction permit, the prefect can launch a legal procedure against the municipality. Mayors can be held liable for ignoring hazard zones. Regions monitor the integration of hazard zones in sub-national land-use decisions.

Source: OECD (2017c), "Boosting resilience through innovative risk governance: The case of the Rhône river in France", http://dx.doi.org/10.1787/9789264281370-6-en.

In areas that are subject to recurrent and large disaster impacts and areas that could usefully serve to mitigate disaster impacts (such as flood retention areas), some countries have used resettlement as a risk prevention instrument. Most countries have relocated exposed populations, although rarely, as a measure of last resort. Only nine countries list relocating residents as a priority policy area in their risk prevention strategies (see Figure 4.3). Box 4.6 describes an example of good practice in resettlement: the Austrian Machland Dam project's flood canal.

Box 4.6. Integrative flood risk management: The Machland Dam in Austria

The Machland Dam is the biggest flood protective infrastructure work that has been undertaken in Austria and possibly in Europe. The dam, constructed from 2008 to 2012, spans over 36.4 km to protect 22 400 inhabitants spread over 7 municipalities in the Machland region.

The dam was complemented by an 8.7 km flood canal spreading from Naarn to Wallsee/Mitterkirchen. The canal constituted an element of the project's integrative flood risk management design. It was created to prevent small-scale floods, thus protecting lives and preserving the environment.

The design of the flood canal expanded into settlement areas, which required citizens to relocate. A total of 254 voluntary resettlement agreements for houses located in areas at risk of flooding were concluded, costing EUR 92 million in compensation payments. The process began in 1993, and only 5 resettlement agreements were made in the first 5 years. Successive floods convinced the remaining citizens to move, with the 2002 floods leading to the rapid resettlement of 221 properties.

Compensation for house owners was based on the replacement value of their houses as well as their demolition costs. The authorities provided 80% of the overall costs in compensation: the federal province paid 30% of total costs and the central level 50%. Property owners kept their initial land titles; however, the land had to be dedicated as pasture, since the right to build on it was revoked. New lots for rebuilding houses were made available in adjacent communities to protect relocating citizens from hikes in land prices and to ensure that communities were rebuilt.

Sources: Machland-Damm (2017), Machland-Damm website, www.machlanddamm.at*;* Oberösterreich Landesrechnungshof (2014), *LRH-Bericht, Initiativprüfung, Hochwasserschutz Machland Nord, LRH-100000-12/9-2014-LI.*

Encourage business continuity

Countries should encourage businesses, particularly critical infrastructure operators, to take steps to ensure business continuity. The Recommendation specifically suggests the following:

- developing standards and toolkits designed to manage risks to operations or the delivery of core services
- ensuring that critical infrastructure, information systems and networks still function in the aftermath of a shock
- requiring first responders stationed in critical infrastructure facilities to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable
- encouraging small community-based businesses to take proportionate business resilience measures.

Business continuity planning constitutes a key element to reduce the potential disruption of the supply of goods and services, especially in vital systems such as hospitals, water and energy, public security, transport, and communications. After a disaster, the economic recovery of a country or region depends heavily on the continued productive capacities of such essential services and needs to be accompanied by specific recovery

programmes. For public and private sector organisations alike, the first step in business continuity planning is to model the potential impacts and consequences of a hazard on the organisation's entire range of activities. It must distinguish the organisation's essential parts and functions from what can be abandoned temporarily.

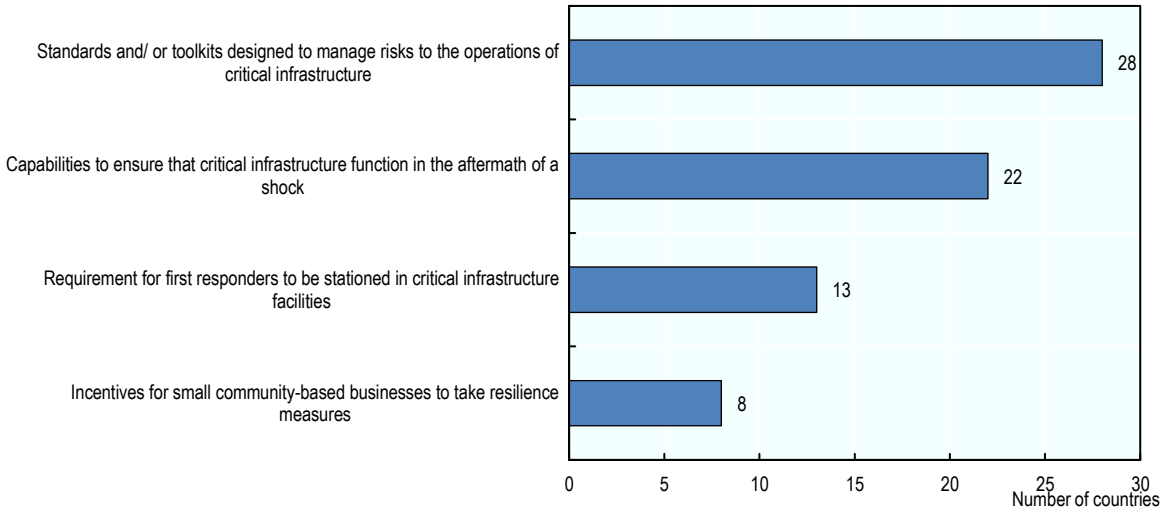
When asked about measures to encourage the private sector in business continuity planning, 28 respondents stated they use standards or toolkits (Figure 4.4). Countries have made efforts to improve and develop business continuity plans, and in a few cases governments have even provided advisory services or guidelines. However, there is little evidence available on putting these in practice.

In Switzerland, the implementation of national guidelines is gaining momentum. Although the Swiss "Guideline for the Protection of Critical Infrastructure" is not binding, economic associations and critical infrastructure providers increasingly apply it.

In Poland, the first National Critical Infrastructure Protection Programme was adopted in 2013 and updated in 2016. A textbook series and training courses on critical infrastructure resilience, attended by over 800 individuals, accompanied the programme.

Other countries are developing integrated approaches for critical infrastructure protection. The Netherlands' approach offers guidance on maintaining and increasing the resilience of vital infrastructure. In Finland, the National Rescue Act details duties of business and industrial operators and of building owners and occupants to ensure self-preparedness and resilience in the case of disaster.

Figure 4.4. Measures to encourage business continuity planning in the private sector



Note: Answers were received from 31 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Despite the high cost that disasters can inflict on businesses, few incentives are provided to community-based businesses to take resilience measures. Where they are available, businesses may be unaware of the support for prevention and mitigation measures. To address this challenge and to reduce overall economic losses caused by disasters, some governments include businesses in their disaster risk reduction strategies (see Box 4.7). In Australia, for example, the government created the Organisational Resilience programme

to boost risk awareness among businesses and increase the number that invests in resilience measures.

In France, programmes specifically tailored for businesses have shown success in increasing their resilience. A programme to reduce vulnerability to floods in the Loire river basin has increased risk awareness and preventive measures. In the Rhône river basin, where the agricultural sector is of great economic importance, measures to make agricultural activity flood resilient were introduced.

New Zealand and the United Kingdom offer other examples. To provide science-based solutions for business continuity planning, in New Zealand a government-supported group conducts research on resilience for organisations of different sizes, sectors and ownership structures. The United Kingdom published a guidebook for business continuity that follows the format of the well-known "for Dummies" series. Business continuity planning has since increased sharply throughout the country.

Box 4.7. Boosting business resilience: Australia, France, New Zealand and United Kingdom

In **Australia**, the Organisational Resilience programme offers businesses the opportunity to test their own resilience online. The Organisational Resilience HealthCheck is carried out according to 13 indicators. This allows businesses to quickly evaluate their resilience attributes and to identify opportunities to improve resilience capability. Once the confidential HealthCheck has been completed, businesses are provided with a comprehensive overview of their individual resilience capability. This helps them locate possible bottlenecks and to identify appropriate resilience measures from a list of good practices. Businesses can also refer to a range of guides on organisational resilience, as well as to information from the Australian Emergency Management Knowledge Hub. In addition, the programme organises courses and workshops.

Given the exposure to flood risk along **France**'s river basins and the number of nearby businesses, vulnerability awareness programmes have been put in place. In the Loire river basin, for example, the business vulnerability reduction programme is a basin-wide initiative that helps businesses situated in flood zones to take measures to reduce a flood's impacts on business activity. The programme includes a risk communication campaign and awareness survey. In addition, an on-site flood vulnerability diagnosis is offered to businesses located in flood risk areas. Local authorities then provide financial support, through co-funding, to apply risk reduction measures. Through this programme, more than 20 000 businesses have gained valuable knowledge about their flood risk exposure, around half of which were originally unaware of their exposure.

The government of **New Zealand** provides funding for business continuity research and the development of application tools. Resilient Organisations is a research and consulting group benefitting from this funding. The group conducts research to help businesses prepare for, respond to and recover from disruptions of all kinds. While much of the research is made available online, businesses can also request individually tailored consulting services.

In the **United Kingdom**, in 2011 only 5% of small and medium-sized enterprises (SMEs) had business continuity management plans in place. To increase this number, the government published **"**Business Continuity for Dummies". It is a straight-forward and user-friendly book proposing detailed guidelines for companies and most particularly SMEs. The book was written by experts sponsored by the Cabinet Office, the Business

Continuity Institute and the Emergency Service Planning. It helps identify key products and services, as well as the critical activities that underpin them, and delivers accessible, affordable and achievable tips for business continuity and resilience.

Sources: Australian Government (2017), Organisational Resilience, www.organisationalresilience.gov.au/Pages/default.aspx; OECD (2016b), "Business vulnerability reduction to flood programme in the Loire basin", https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/businessvulnerabilityreductiontofloodprogrammeintheloirebasin.htm#tab_description; OECD (2017c), "Boosting resilience through innovative risk governance: The case of the Rhône river in France", http://dx.doi.org/10.1787/9789264281370-6-en; OECD (2016c), Toolkit for Risk Governance − For Dummies: Business Continuity Guide Book in the UK, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/fordummiesbusinesscontinuityguidebookintheuk.htm#tab_description; Resilient Organisations (2017), About Organisational Resilience, www.resorgs.org.nz/.

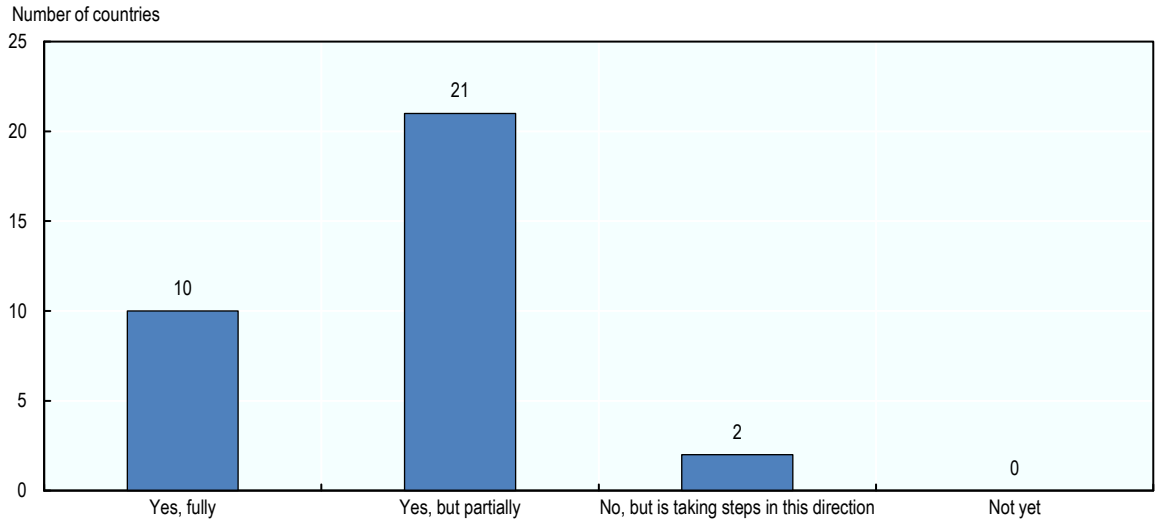
Key trends and self-assessment

Countries have exercised strong leadership in driving a whole-of-society approach to risk communication aimed at raising public awareness of exposures to hazards and threats. This is key to increasing public acceptance of disaster risk reduction. The use of interactive platforms that support two-way communication between citizens and risk management authorities is on the rise. This has been valuable for designing risk reduction actions that are publicly acceptable. Another common good practice is risk communication tailored to different local communities and vulnerable population groups, such as the elderly, disabled, youth and tourists. Additionally, countries have taken advantage of the education system at primary, secondary and in some cases tertiary levels to sensitise the population to exposures to natural hazards. Common areas for improvement include undertaking efforts to communicate about transboundary risks.

Countries have largely embraced the need to implement a mix of policies to achieve disaster risk reduction that includes both investments in structural measures and organisational risk reduction measures. Disaster risk reduction is now a high priority area for policy that complements emergency preparedness and crisis management functions. In terms of implementing disaster risk reduction, countries have carried out a range of different actions: from hazard mapping and prescriptions on building in exposed areas, to investments in protective physical infrastructure and providing guidance to strengthen business continuity capacities. The responsibility for policies to sustain the benefits of these investments is often put in the hands of sub-national governments. However, some lack sufficient financial and technical capacity to monitor and inspect all new construction works and to maintain the expensive infrastructure that provides structural protection.

The self-assessment picture of the third key recommendation is mixed (Figure 4.5). When asked, 10 countries stated that they had fulfilled it, 21 countries responded that they had partially fulfilled it, and two replied that they are taking steps to do so in the future. Therefore, respondents' self-assessment is comparatively lower for the third key recommendation than for the first, second and fourth key recommendations. This self-assessment echoes the efforts of the international risk management community. Agreements such as the Sendai Framework for Disaster Risk Reduction and the Sustainable Development Goals focus on investing in prevention and mitigation.

Figure 4.5. Self-assessment on implementing the third key recommendation



Note: Answers were received from 32 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Conclusions

Countries should strengthen efforts to engage the private sector in disaster risk communication in order to stimulate household and business investment in risk reduction measures. The private sector has displayed many good practices in risk communication, however its role in an overall country risk management strategy is often based on goodwill rather than formal arrangements. Countries that have not done so should establish two-way communication channels to solicit stakeholder feedback through online platforms. Finally, there is a gap in empirical research concerning the effectiveness of risk communication. Conducting targeted research on how it changes behaviour, such as leaving hazard exposed areas or taking self-protection measures, could help countries reform their risk communication strategies.

Countries should continue to strengthen disaster risk reduction in light of their on-going risk assessments. They should build the results of long-term risk analyses into the design of sustainable communities. A governance challenge in this respect is for policy makers to look beyond results that can be obtained during their own mandate. Another challenge is financing structural reinforcement, especially for rural communities with low capacity to pay for infrastructure needs. Countries need to act urgently to address potentially rising vulnerabilities by filling gaps in their capacity to enforce organisational measures, such as building codes and hazard-informed land-use decisions.

Countries should increase partnerships with operators of critical infrastructure to share responsibilities for national resilience. They should continue progress in developing business continuity standards, especially for critical infrastructure sectors. This is crucial to prevent disasters from causing business interruptions that would significantly damage the economy. Finally, a significant number of SMEs still need business continuity planning and risk reduction measures.

Notes

[1] This report benefits here from the additional results of the OECD Survey on Risk Communication Policies and Practices conducted in 2015 that was designed on the basis of the Recommendation. The following countries responded: Australia, Austria, Colombia, France, Germany, Greece, Japan, Korea, Luxembourg, Mexico, Norway, Poland, Slovak Republic, Slovenia, Sweden, Switzerland, Turkey and the United Kingdom.

[2] https://twitter.com/NZcivildefence?ref_src=twsrc%5Etfw.

[3] See Deprem Bilgi Sistemleri (Earthquake Information Systems): www.afad.gov.tr/tr/HbIcerikDetay.aspx?ID=96.

[4] See *Vai tu zini, kā rīkoties ārkārtas gadījumos?* [Do you know how to handle emergencies?]: http://vugd.gov.lv/lat/drosibas_padomi/vai_tu_zini__ka_rikoties_arkartas_gadijumos_.

[5] See SAFETY-Tour Bundesfinale 2015: www.zivilschutzverband.at/de_at/home/194.

[6] More information about the EconoMe 4.0 Platform, see: https://econome.ch/eco_work/index.php.

[7] The obligatory natural hazard insurance system in Switzerland provides useful and representative information in that regard.

References

Australian Government (2017), Organisational Resilience, www.organisationalresilience.gov.au/Pages/default.aspx.

FOEN (2016), "Beurteilung der Gefährdung durch Extremhochwasser der Aare: Hauptstudie lanciert" [Evaluation of extreme flood hazards along the Aare: Main study launched], Federal Office for the Environment, Switzerland, www.bafu.admin.ch/dokumentation/medieninformation/00962/index.html?lang=de&msg-id=60609.

French Ministry of Ecology (2009), "Le document d'information communal sur les risques majeurs (DICRIM)", Paris, www.prim.net (accessed November 2016).

INSERM (2004), "Surmortalité liée à la canicule d'août 2003", Institut national de la santé et de la recherche médicale, France.

Machland-Damm (2017), Machland-Damm website, www.machlanddamm.at.

NHP (2016), The Natural Hazards Partnership website, www.naturalhazardspartnership.org.uk/.

Oberösterreich Landesrechnungshof (2014), *LRH-Bericht, Initiativprüfung, Hochwasserschutz Machland Nord, LRH-100000-12/9-2014-LI.*

OECD (2017a), "Boosting resilience through innovative risk governance: The case of Alpine areas in Austria", *in Boosting Disaster Prevention through Innovative Risk Governance: Insights from Austria, France and Switzerland*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264281370-5-en.

OECD (2017b), Toolkit for Risk Governance: UK Natural Hazard Partnership, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/uknaturalhazardpartnership.htm#tab_description.

OECD (2017c), "Boosting resilience through innovative risk governance: The case of the Rhône river in France, in *Boosting Disaster Prevention through Innovative Risk Governance: Insights from Austria, France and Switzerland*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264281370-6-en.

OECD (2016a), OECD Survey on the Governance of Critical Risks, OECD, Paris.

OECD (2016b), "Business vulnerability reduction to flood programme in the Loire basin", https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/businessvulnerabilityreductiontofloodprogrammeintheloirebasin.htm#tab_description.

OECD (2016c), Toolkit for Risk Governance − For Dummies: Business Continuity Guide Book in the UK, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/fordummiesbusinesscontinuityguidebookintheuk.htm#tab_description

OECD (2015), OECD Survey on Risk Communication Policies and Practices, OECD, Paris.

OECD (2003), *OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264101821-en.

Resilient Organisations (2017), About Organisational Resilience, www.resorgs.org.nz/.

Chapter 5. Strategic crisis management

This chapter assesses progress across countries in implementing the fourth key OECD Recommendation of the Council on the Governance of Critical Risks. The chapter focuses on three core areas highlighted in the Recommendation: to establish strategic crisis management capacities to prepare for the unknown or so-called "black swan" events, to strengthen crisis leadership capacities to warn and make sense of crisis and exercises, and to establish scaling-up mechanisms for emergency response. The chapter describes good practices and policy tools and presents key trends. The conclusions suggest future actions to engage the private sector, benefit from risk analyses and partner with operators of critical infrastructure.

Good practices and policy tools

Establish strategic crisis management capacities to prepare for unknown and unexpected risks

Most countries have experienced a major crisis in recent years, one with which their government and risk management system were not able to cope. Table 5.1 provides a selection of events of national significance for which countries were not properly prepared and which led to major reforms of policies or systems. Such events challenge crisis managers by their unexpectedly large scale, their novelty or unprecedented nature, and their complexity, all of which bring uncertainty regarding their consequences and how to handle them effectively. Ultimately, such crises may threaten core social values, increase tensions among different stakeholders and even lead to political backlash against decision makers.

Governments need to adapt their crisis management approaches to an institutional context which has evolved significantly. Waves of decentralisation and privatisations have left central governments with fewer levers to activate when a crisis occurs. New actors have emerged with whom governments need to engage in crisis situations, from local governments to the private sector and civil society. Gaps in crisis management have often resulted from a lack of co-ordination or communication either between levels of governments as in the case of Hurricane Katrina in New Orleans in 2005, or between government and the private sector as shown in Japan during the 2011 Fukushima crisis which involved the power operator TEPCO.

Civil society also expects more and more information during a crisis – including through social media – and to play a bigger role in the response, through volunteerism and action at the community level. Greater media scrutiny is another aspect of increased societal demands for governments to act swiftly and efficiently during crises. Finally, international co-operation is an essential pillar for crisis management, given the often transboundary nature of today's crises and the opportunities it can offer for a more effective response.

In today's landscape marked by more complex crises, governments coexist with a larger network of stakeholders and face increased pressure from society and media. As a result, traditional emergency management based on standard operating procedures no longer suffices. New complementary approaches are required to face the unexpected and respond to shocks of an unprecedented nature. While pre-prepared emergency plans triggered by early-warning systems can be valuable for familiar contingencies, these should be complemented by more agile partnerships across a multi-stakeholder emergency network and by capacities to make sense of complexity and to provide meaning to citizens with renewed crisis communication approaches.

The ultimate responsibility lies at the highest levels of government, which have a key role to play to fulfil these crisis management functions effectively, from inter-agency co-ordination to decision-making and communication. This is fundamental for maintaining public trust, which is particular tested during emergencies: citizen's trust in government is directly affected by how quickly, efficiently and transparently government decisions are taken in crisis situations. Political leadership is considered accountable for good or poor crisis management.

Table 5.1. Selected major crises

Country	Crisis	Year	Novelty – Complexity – National significance
Australia	Queensland floods	2011	Unprecedented scale and duration of the floods caused by an exceptional La Niña event
Canada	Fort McMurray fires	2016	Massive forest fires surrounding an entire city forcing its full evacuation and stopping oil production
France	Paris terrorist attacks	2015	Simultaneous jihadi attacks with massive shootings in large gatherings and public spaces
Germany	Migration crisis	2015	Large migrant flow crossing European borders to Germany
Iceland	Eyjafjallajökull volcanic eruption	2010	Ash cloud dispersing particles across Europe affecting global air transportation for a week
Italy	Costa Concordia accident	2012	Accident of a large-size cruise boat with multinational victims and technical complexities
Japan	Great East Japan Earthquake	2011	Very high magnitude earthquake and devastating tsunami affecting the Fukushima nuclear reactors
Korea	Sinking of ferry Sewol	2014	304 people – mostly students – killed in the sinking of a ferry caused by disrespect of safety and security procedures
Mexico	Hurricanes Odile and Edward	2014	Hurricanes simultaneously affecting both the Pacific and Atlantic coasts
Netherlands	MH17 plane explosion	2014	Plane departing from Amsterdam exploding over Ukraine killing numerous Dutch citizens
Norway	July 2011 terrorist attacks	2011	Simultaneous bombing of centre of government and youth mass-killing by a lone-wolf extremist
New Zealand	Christchurch earthquake	2011	Unprecedented damages to the country's third largest city
Sweden	Indian Ocean tsunami	2004	Unprecedented number of casualties of Swedish tourists
United States	Hurricane Katrina	2005	Levees breaking causing large-scale socio-economic damages to the city of New-Orleans

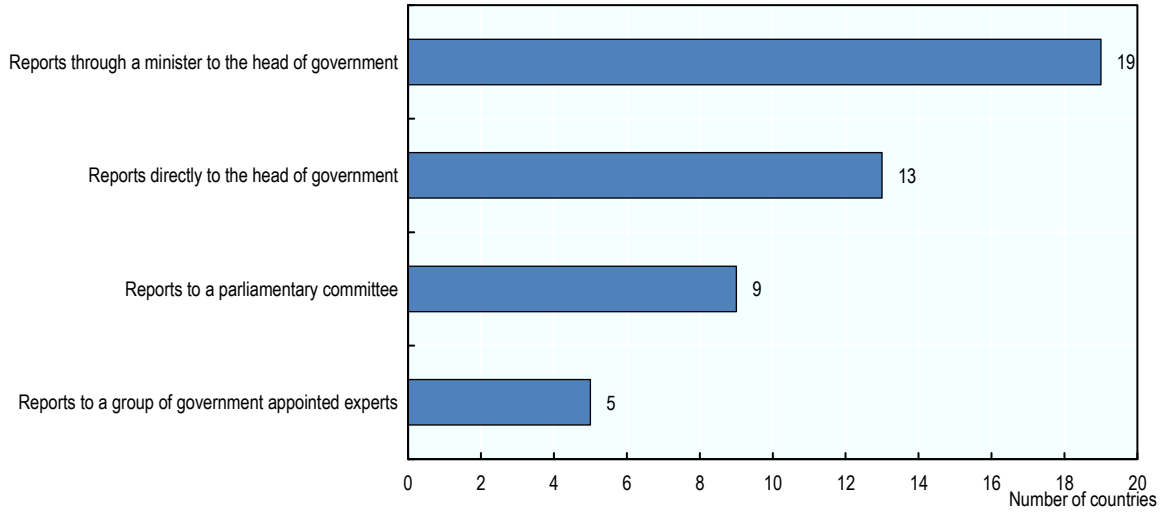
Note: This selection of crisis events is proposed by the Secretariat based on recent materials shared at the OECD for events of national significance that led to policy reform. The intention is to illustrate the diversity of novel and complex crises governments need to prepare for.

Engage the whole-of-government across levels and sectors in strategic crisis management

National crisis governance frameworks should ensure that the appropriate structures and institutional arrangements are put in place to deal with the complexity, novelty, ambiguity and uncertainty that characterise many modern crises. They engage both the strategic leadership, to address policy trade-offs and communicate with the public, and the inter-agency network of emergency responders.

While a high number of countries have established a national framework for crisis management, these frameworks differ in the way they report to the centre of government (Figure 5.1). When asked, 13 of the 34 respondents to the OECD Survey on the Governance of Critical Risks answered that their lead institution reports directly to the head of government, and 19 replied that they report through a minister. Thus the highest level of political leadership does not directly control crisis management in the majority of the countries. Several respondents said that a group of appointed experts serve as the first level of reporting before accessing political leaders. Eight respondents report to a parliamentary committee, however mostly in the post-crisis phase for accountability purposes or for policy improvement (see Chapter 6).

Figure 5.1. Reporting to the centre of government



Note: Answers were received from 28 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Beyond strong leadership, managing crises demands broad governance arrangements that involve a large number of government and non-government actors. All respondents apart from one pointed to the existence of an inter-agency co-operation mechanism for strategic crisis management. Twenty-nine respondents have mechanisms in place to draw together civil protection resources from sub-national levels of government to manage large-scale disasters. While this shows that almost all countries have means to engage the whole-of-government across sectors and levels in crisis management, different models exist depending on the institutional frameworks in which these systems operate.

Overall, countries have implemented one of two models. In one model, centralised administrations rely on vertical co-operation, with scaling-up mechanisms that automatically activate from the top when local capacities are not capable of managing the crisis on their own (e.g. in Denmark or France). In the other model, sectoral authorities operate primarily on the basis of subsidiarity; local governments are the first in charge of the emergency response, requesting support from higher levels of government when necessary. This is the case in countries where states or other forms of sub-national governments often have the primary responsibility to manage crises affecting their territory and are the first responders to disaster and security incidents. Examples are Australia, Canada, Germany, Italy, Mexico, Switzerland and the United States.

National crisis management frameworks should engage the different line ministries or sectoral agencies beyond those usually in charge of crisis management. While in the health, police, civil protection or transport sectors, line ministries or agencies have established crisis management capabilities for many years, few countries demonstrate a whole-of-government engagement in crisis management beyond these sectors.

Several approaches have proven successful to ensure such large inter-agency engagement. For instance, in France each ministry has a high-level civil servant in charge of security and defence, and they together form an inter-agency network which can directly be activated when a crisis occurs. In Finland, the Security Strategy for Society has created a large multi-sector engagement. It identifies seven vital functions necessary in all

situations and 49 strategic tasks of the government which contribute to securing these functions. The strategy has assigned responsibilities to ministries for each of these tasks.

The main tool countries use to facilitate multi-sector engagement in risk as well as crisis management is the national risk assessment (NRA) (see Chapter 3). Fifteen respondents apply the NRA to gain consensus or a common understanding of risks across sectors and to create a collaborative risk management culture. In addition, the NRA is often referred to when planning for crisis management capabilities. Half of the responding countries have made progress in engaging multiple sectors in crisis management.

Leverage the private sector and civil society in the response to strategic crises

Governments cannot manage crises alone. Developing trusted partnerships with the private sector, civil society organisations and volunteers, as well as international partners, is fundamental. As explained in Chapter 3, many countries have started partnering with operators of critical infrastructure to better assess vulnerabilities and define resilience measures. But engaging them in the crisis management processes also requires specific partnerships. Operators from water, energy, telecommunications or other sectors − public or private − often have their own internal crisis management structures and processes that they activate to restore disrupted services. Appropriate governance arrangements must be established prior to a crisis. Mutual aid agreements between utility operators are a good example (e.g. in the United Kingdom and the United States; see Box 5.1).

The private sector can provide key capabilities which are required by governments to manage specific crises situations. In the cases of the Deepwater Horizon Oil Spill in the Gulf of Mexico in 2010, the Fukushima nuclear accident in 2011 and the Costa Concordia accident in Italy in 2012, governments had to contract rapidly with the private sector to find appropriate technical solutions. The ability to evaluate which capabilities are required and contract with the providers is key to ensure an effective response.

Box 5.1. Partnering with electricity companies: United States

Hurricane Sandy caused a massive power outage in New York and New Jersey leaving 8.5 million customers without power. In response, the United States president requested that the Federal Emergency Management Agency establish an Energy Restoration Task Force. The Task Force supported a huge private power restoration effort in which electric companies carried out mutual aid agreements. They deployed over 70 000 workers and flew 229 power-restoration vehicles to the affected areas to help restore power.

Source: FEMA (2013), Hurricane Sandy FEMA After-Action, https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

Civil society is a growing part of the new environment of crisis management. Citizens, volunteer organisations, and national and international non-governmental organisations (NGOs) all have a role to play in the response system. Properly articulating their roles and functions with other emergency response actors is fundamental. Such civil society capacities should be supported, including through incentive mechanisms. In several countries, including Austria, Finland, Germany, Italy (Box. 5.2) and Sweden, volunteer organisations are well integrated into the emergency response phase. A few countries rely on citizens to act as first responders, and public authorities have developed dedicated

policies to support societal resilience in this respect. This is particularly the case where small settlements are spread across large territories, such as in Canada – with the Get Prepared Programme – and in Finland – with the Internal Security Programme.

Countries significantly exposed to natural and technological hazards, such as Mexico, have established policies concerning industrial operators. Operators that use large buildings must develop and train internal units for civil protection. The personal safety and security of the personnel and citizens involved in these actions is a major consideration.

Box 5.2. Good practice in mobilising volunteer organisations: Italy

In Italy, volunteer organisations are now one of the most vital components of the civil protection system. More than 4 000 organisations are registered on the list of the National Civil Protection Department. With over 1 million members across the country, 100 000 to 150 000 volunteers can be mobilised in two hours. Volunteerism also contributes to a more cost-efficient response to major events. Following the Aquila earthquake, 730 000 volunteer working days were counted in the response phase, corresponding to EUR 100 million if professionals had been hired.

The participation of volunteer organisations in civil protection activities is regulated by the Presidential Declaration 194/2001. It stipulates that voluntary associations can be formed by any freely constituted body, including municipal groups, and need to be non-profit, democratically structured and set up for solidarity purposes. Associations have to be recognised in regional and national registries in order to guarantee benefits and protection to their members. The state contributes to upgrading their equipment and technical training courses. Moreover, volunteers have guarantees such as the preservation of their job and pension during their volunteer time, as well as the benefit of a specific insurance coverage. These legal provisions have improved volunteerism in Italy and associated volunteer organisation more closely within the national network for emergency response. The volunteer force engaged in forecasting, prevention and relief is growing and is now about 1 million people in Italy as a whole.

Source: OECD (2016b), Toolkit for Risk Governance: Italian system for the mobilisation of volunteers in civil protection, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/italiansystemforthemobilisationofvolunteersincivilprotection.htm.

Crisis management requires that centres of government invest in their ability to manage large multi-stakeholders and multi-form public/private/NGO response networks. Co-operation mechanisms are in place in most countries and are often based on standard operating procedures (SOPs). These govern the operations of most of the entities involved, from scaling-up to engaging with partners. In Mexico, for instance, the Civil Protection Manual describes precisely the roles and functions of the 34 federal institutions that can take part in the response to an emergency.

SOPs present limitations for managing a novel crisis with unforeseen consequences across sectors. They restrict the ability of a response network to adopt the more flexible and agile approaches that might be necessary to face the unexpected. The crisis management doctrine is therefore evolving in several countries in line with the provisions of the Recommendation. Having experienced co-ordination failures during major crises, these countries have adopted more flexible co-operation arrangements based on common

principles and interoperable tools. Common and harmonised protocols for emergency response processes are essential to foster inter-agency crisis co-operation across the emergency response network (Box 5.3).

Box 5.3. Incident Command System: United States

The United States revised its crisis management approach after Hurricane Katrina and adopted the Common Response Framework. This framework favours interoperability of the different units engaged in the response of a crisis. In addition, the National Incident Management System was renewed to establish common competencies and behaviours for emergency management.

The Incident Command System (ICS) consists of a standardised emergency management structure that allows federal, state, tribal and local governments, NGOs, and the private sector to respond to the demands of a crisis situation, regardless of jurisdictional and political boundaries. Aimed at fostering interoperability and inter-agency co-operation, the ICS provides schemes for 14 management characteristics related to incident command, operations, communication, planning, logistics, finance and administration, and intelligence and investigation. Management objectives and action planning are centralised in a single unit of command to prevent diverging orders and promote accountability to a unified command and reporting institution. This allows agencies to respond to emergencies in a cost-effective and co-ordinated way that supports mutual objectives and strategies. At the same time, the ICS is flexible enough to be implemented for all kinds of incidents, small or large.

To facilitate communication, the system offers a common inter-agency terminology. Information exchange is co-ordinated by public information officers who are in permanent contact with the incident command organisation and the safety officer. In order to promote an inter-disciplinary approach, training and specific guidelines on ICS are provided to agencies such as the Food and Drug Administration, healthcare providers and hospitals, and institutions of higher education.

Source: OECD (2016c), Toolkit for Risk Governance: US National Incident Management System (NIMS), https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/usnationalincidentmanagementsystemnims.htm.

Strengthen crisis leadership, early detection and sense-making capacities

Leaders in charge of crisis decision-making have to recognise the issues at stake in a crisis, its potential development, and the associated uncertainties. Sense-making, decision-making and meaning-making are fundamental for effective crisis leadership. Countries have developed sense-making functions, to complement early-warning systems, within dedicated methods and structures – such as crisis cells – often located within centres of government.

Countries have made great strides in administrative practices and technological advances that together have vastly improved early-warning systems at both national and international levels. Hydro-meteorological phenomena, infectious disease outbreaks, volcanoes, tsunamis and many other types of natural hazards are now continuously monitored in all countries. The capacities of countries to forecast, detect and anticipate the evolution of hazardous events have improved notably though innovations such as the

increased use of satellite data, investments in super computers, data treatment and modelling capacities, as well as international data exchanges.

Capacities to track social phenomena and man-made threats have also dramatically improved in recent years. Some countries (e.g. Korea) have set up technical platforms to analyse information exchanged through social networks (Box 5.4) and deep web applications. Furthermore, these diverse systems to forecast, detect and anticipate the evolution of hazardous events are now better linked with emergency services, which trigger warnings and activate emergency plans that alert citizens. Many survey respondents provided examples of comprehensive early warning systems (e.g. Chile, Colombia, Japan, Mexico and Slovenia) and of the increasing use of telecommunications to tailor messages to individuals based on their location. The OECD Toolkit for Risk Governance identifies good practices in early warning systems from France and Switzerland.

Box 5.4. Monitoring social media to enhance risk management: in Korea

The popular social media and microblogging service Twitter is a useful tool for sharing information in a quick and easy manner. During disasters and emergencies, the service often sees a surge of users generating and retweeting information related to the event. The tweets and retweets often contain first-hand, local information that is not available via other news streams, but turning the stream of tweets on a disaster or emergency into actionable information can be challenging. Recognising the value that Twitter may bring to disaster management, researchers have developed analytical tools.

In Korea, researchers have created a real-time monitoring system for disaster situation management called the Smart Big Board. With this tool, real-time weather information, satellite images and closed-circuit television cameras are displayed on the map to support decision-making. Tweets containing geo-location data and disaster-related keywords such as “rain”, “typhoon” and “flooding” are also displayed to analyse the information on those areas. The National Disaster Management Research Institute has test-operated the system.

Source: Korea National Disaster Management Institute, “GIS-based information integration framework for disaster risk management”, presentation from the Korea National Disaster Management Institute.

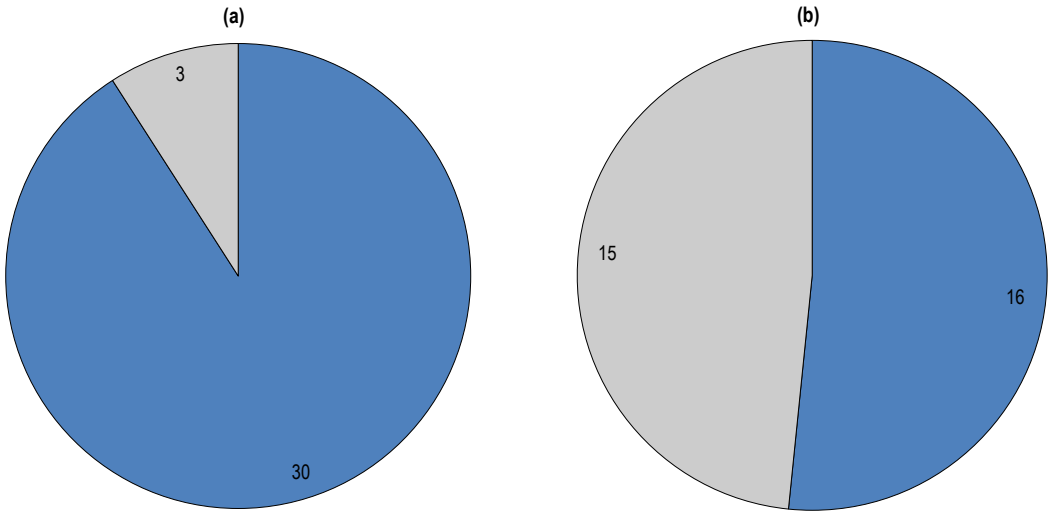
Countries need to ensure that reliable, trusted and co-ordinated expert advice translates into informed decisions by national leaders. Crises most often take governments by surprise and lead to difficulties in sense-making, i.e. the identification of core values at stake in a crisis and its potential development. When an unexpected crisis occurs, it is necessary to quickly obtain, digest and channel accurate information and trustworthy expertise to help leaders make sense of it. Often leaders are not adequately informed before taking crucial decisions at times of high uncertainty, conflict over values and high expectations.

Most countries reported to have already established mechanisms and systems to monitor crisis situations and to build situation awareness. However, only just over half of them stated that they have established specific approaches to anticipate the “unknown” or more “chaotic” crises that do not correspond to past events (Figure 5.2b). This shows that countries have made mixed progress in developing the tools required to prepare for and be able to respond to “black swan” events. A few highly advanced countries have set up

such knowledge management systems and expert networks across multiple sectoral, professional and disciplinary boundaries. These networks aim to take account of the context-dependant characteristics of each crisis, such as the organisational and political contexts that enable and constrain the decision-making ability of leaders and advisors.

Box 5.5 describes good practices in Denmark, Switzerland and the United Kingdom in setting up such tools which can inspire other countries. These include the Pandora Cell of the Danish Emergency Management Agency which focuses on anticipating future development of a crisis. Another is the Federal Crisis Management Support provided by the Swiss Federal Chancellery that combines several sense-making tools. A third example is the Scientific Advisory Group in Emergencies of the United Kingdom, which mobilises multi-disciplinary expertise when the Cabinet Office Briefing Room is confronted with complex crises.

Figure 5.2. Mechanisms for situation awareness (a) and complex crisis anticipation (b)



Note: Answers were received for (a) from 33 out of 34 respondents and for (b) from 31 out of 34 respondents.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Box 5.5. Good practices to anticipate and make sense of complex crises: Denmark, Switzerland and United Kingdom

The **Danish Emergency Management Agency** (DEMA) designed its **Pandora Cell** to support the emergency response process by providing crisis anticipation analysis to crisis managers. In case of a crisis, the Pandora Cell is deployed as an arm of the crisis management structure. It works independently to provide crisis management leaders with an extended analysis of the ongoing crisis and its potential evolution. The Pandora Cell aims at identifying elements that could lead to a deterioration of the crisis, and therefore prevent the crisis situation from getting worse. These elements could be linked to the crisis response effort itself but could also be related to the crisis' general dynamics. The Pandora Cell is made up of three to seven experts, from different backgrounds, with analytical skills and experience in crisis management. Scientific experts support them on an ad hoc basis. The Pandora Cell first gives an overview of the current disaster and the response provided, and informs crisis managers of previous cases of similar events at home or abroad. It delivers a horizon-scanning analysis, by developing both standard and alternative scenarios for the future and challenging the assumption that the crisis will follow a standard trajectory. Finally, it outlines issues that could cause the crisis to deteriorate.

The Swiss Federal Chancellery has been tasked through the 2012 Government and Administration Organisation Act to set up a new presidential service aimed at advising and supporting the Federal Council regarding the timely detection and the management of crises. The Federal Crisis Management Support is available to provide services in a crisis situation to the Swiss president or to any Federal Crisis Cell mandated by the Cabinet. This support is composed of three complementary functions: (i) a crisis counsellor, who serves as a critical observer, challenging assumptions, providing out-of-the-box thinking and sharing lessons from past crises, (ii) scientific and technical networks similar to the United Kingdom Scientific Advisory Group for Emergencies, and (iii) a Rapid Reflexion Force that presents and validates, from an external perspective, a series of strategic questions, developments, sense-making and possible measures. The combination of these three entities provides the necessary expertise and capacity to anticipate risks and challenges and contributes to improving operational co-ordination among key actors.

The **United Kingdom Scientific Advisory Group for Emergencies (SAGE)** is an independent support group that provides science-based expertise for the management of complex and unprecedented crises for the Cabinet. SAGE convenes in situations that require cross-government co-ordination, notably when the Cabinet Office, in consultation with the prime minister, decides to activate the Cabinet Office Briefing Room (COBR). SAGE provides scientific and technical advice on the development of the crisis, potential scenarios and their impacts. Under the authority of the government Chief Scientific Advisor, SAGE includes experts from all sectors and disciplines to analyse data, to assess existing research or to commission new research. To inform cross-government decision-making during the emergency response and the recovery phases, SAGE submits policy option papers which outline scientific and technical solutions and their pros and cons and response scenario papers. SAGE representatives are invited to attend the COBR to explain scientific issues. Since its establishment in 2009 during the H1N1 influenza pandemic, SAGE has become a key mechanism to support COBR in complex crises situation such as the 2010 volcanic ash cloud and the

2011 Great East Japan Earthquake and Fukushima nuclear accident.

Source: OECD (2016d), Toolkit for Risk Governance: Denmark's Pandora Cell for crisis anticipation; https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/denmarkspandoracellforcrisisanticipation.htm; OECD (2016e), Toolkit for Risk Governance: Switzerland's Federal Rapid Reflection Force, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/switzerlandsfederalrapidreflectionforce.htm; OECD (2016f), Toolkit for Risk Governance: UK Scientific Advisory Group in Emergencies, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/ukscientificadvisorygroupinemergencies.htm.

Develop strategic crisis management exercises and drills

Countries conduct exercises and drills to test their procedures and emergency plans. When asked, all countries but one indicated that they conduct emergency management exercises to anticipate crises, and exercises are often mentioned as a key element of national risk management strategies (Chapter 3). However, the crises of today often require crisis managers to go beyond pre-existing plans, rules and procedures and to be able to improvise, adapt to rapidly changing contexts and establish partnerships with diverse organisations, including internationally.

Respondents provided examples of developing such skills and capabilities. These include revising training and crises exercises to strategically engage leaders and establishing inter-agency networks of crisis managers, the private sector and civil society. Respondents identified the challenges of conducting meaningful exercises that are operational enough to test processes, while also pushing participants to think strategically and preparing decision makers to anticipate the unexpected. Countries conduct regular training courses and exercises to establish and maintain inter-agency networks that involve the private sector and civil society, as well as to improve policies and practices (Chapter 6).

Countries noted their progress in designing large-scale exercises to test and train the inter-agency network of emergency responders and involve the private sector and civil society. Good examples include the following:

- Germany has conducted the LÜKEX series of strategic crisis management exercises since 2004 (Box 5.6).
- In May 2016, France organised the Sequana exercise on the risk of a major flood from the Seine river in Paris. It involved many agencies, the private sector, international partners as well as the population, during a two-week period. This exercise proved to be useful when the Seine floods materialised just two weeks later and every participant had the lessons of the Sequana exercise fresh in their memory.
- In the United States, the recent ShakeOut exercise tested a “known unknown” scenario of a magnitude 7.8 earthquake on the San Andreas Fault in Southern California: 10 million Californians participated by subscribing to the exercise website and followed the drill.

Conduct exercises to strengthen capacities of government leaders

Crisis management exercises that involve leaders or that are used to stress-test international co-operation during crises are conducted to a lesser extent by countries.

Crises force strategic-level decision makers to act under very difficult circumstances. Leaders along with their teams, organisations and key partners must be prepared to cope with the rigours of contemporary crisis management. Developing the skills and capacities to manage and prepare for complex crises is therefore key to effectively fulfilling leadership functions.

This is the case particularly for tasks such as sense-making, strategic decision-making and crisis communication or meaning-making, where leadership plays a major role. When citizens' expectations are at their highest, leaders need to find the right words to provide meaning to what is happening, especially when a crisis reaches a level of severity that challenges trust in the government. This meaning-making function of leadership refers to the capacity to provide not only information, but also a narrative that responds to public expectations.

Training leaders is thus a pre-requisite for efficient crisis management. However, strategic level leaders are a particularly challenging target group to engage in crisis management. Their time and attention are scarce resources, and they may be over-confident in their ability to cope with complex crises or may fear exposing themselves in crisis simulation exercises.

A few countries have nevertheless demonstrated the usefulness of organising such training or exercises and have found ways to overcome these challenges. Finland, for example, conducted a cyber-threat exercise in 2014 at cabinet level during which leaders were left without functioning smartphones. In Germany, the LÜKEX exercise involves presidents of the *Länder* and the chancellor (Box 5.6). In Sweden, cabinet members have regular training, simulations or table-top exercises since 2006 after the prime minister at that time insisted on this recurrent investment of time and awareness building. The United States Federal Emergency Management Agency initiated the Thunderbolts exercises as surprise drills for its leadership; they are another exemplary way to stress-test emergency services' ability to react effectively to crises.

Organise exercises to strengthen international co-operation

Respondents and their leaders have participated in international crisis management exercises, but this practice remains infrequent. Developing further international crisis management exercises is necessary for improving capacities to cope with the cross-border effects of complex and large-scale crises. Conducting exercises is essential for developing, testing and improving the ability of countries to co-operate effectively under adverse conditions.

International exercises, although challenging to arrange, design, develop and implement, can play a key role in improving preparedness. Some international organisations, such as the North Atlantic Treaty Organisation and the International Atomic Energy Agency, World Bank and G20, conduct international crisis exercises at the level of political leaders. The European Union, through its Directorate General for Humanitarian Aid and Civil Protection and its Integrated Political Crisis Response arrangements, conducts regular exercises as well. In 2017, European Disaster Response Exercise 17 (EDRC) tested for the first time the combined crisis management capacities at the political and operational levels.

A high number of countries also organise cross-border or regional exercises, including France and Switzerland, Mexico and the United States, and the Council of the Baltic States. The work conducted by the OECD through its workshops on Strategic Crisis

Management identified one example where G20 leaders conducted such exercises together; the exercises took place in the context of the Hague Nuclear Security Summit in 2014 (Box 5.6). Since then, the G20 conducted a crisis management exercise on pandemics for health ministers under the 2017 German presidency.

Respondents underlined many preparedness benefits of planning and staging exercises in addition to testing emergency response capability. The use of scenario planning in exercises helps countries to map out the sequence and evolution of consequences that future disasters might follow, and thus to anticipate any gaps in co-ordination and response capabilities. Exercises also present an opportunity to validate emergency plans, systems and procedures, raise the awareness of businesses and citizens about exposures, and educate them about their roles in an emergency.

Respondents were asked whether their countries perform multi-agency exercises to anticipate potential challenges in emergency response co-ordination and develop solutions in a simulated emergency environment. Among the good examples identified were several exercises performed shortly before a major incident, which therefore helped in handling the real incident.

Box 5.6. Strategic crisis management exercises: Germany and Netherlands

LÜKEX is a national strategic crisis management exercise conducted in **Germany** every two years by the Ministry of Interior and the Federal Office of Civil Protection and Disaster Assistance. LÜKEX involves political leadership across government levels from presidents of the *Länder* to the chancellor, as well as cross-ministerial crisis staff, operators of critical infrastructure and volunteer organisations. It aims to raise the awareness regarding top issues in crisis management and to test abilities to react to extreme threats. The exercise helps in creating horizontal and vertical co-operation within the government and with the critical infrastructure providers. This nationwide exercise was one of the key features of the new strategy for population protection in Germany adopted by the Ministry of the Interior and the *Länder* in the aftermath of the 9/11 terrorist attacks in the United States and the 2002 large-scale Elbe floods. Since 2009, LÜKEX is also enshrined in the civil protection and disaster relief legislation which fixes the common responsibility for dealing with extraordinary danger and damage situations.

LÜKEX has allowed testing different threat scenarios. These include a large-scale blackout, terrorist and cyber-attacks, chemical, biological, radiological and nuclear situations, and a large-scale storm surge affecting several countries. Each crisis simulation entails a 24-month-long exercise cycle including several phases from planning (6-8 months), preparation (9-11 months), and execution (2-3 months) to the final evaluation (4-5 months). These phases create a network among decision makers long before conducting the exercise. LÜKEX has had several positive results, such as identifying areas to improve crisis management structures and strategies, increasing co-operation between the different civil protection actors and critical infrastructure providers, strengthening risk and crisis communication though the high media attention, and more importantly improving decision-making among inter-ministerial crisis management staff in various federal as well as regional agencies.

The Netherlands conducted an international strategic crisis management exercise **with G20 leaders** at the occasion of the Hague National Security Summit in 2014. The aim was to raise awareness, to share internal co-ordination approaches and to

foster international co-operation as well as shared communication. In order to overcome the challenge of convincing leaders and their staff to expose themselves in such an exercise and accept not to read the scenario in advance, the summit organisers developed a dedicated "scenario based policy discussion". A video with a crisis scenario was followed by a series of multiple choice questions, and the answers were used to start a discussion among leaders. This successful exercise showed that political leaders require specific approaches: the discussion must focus on broad political concepts and avoid procedural points and factual questions.

Source: OECD (2016g), Toolkit for Risk Governance: Germany National Strategic Crisis Management Exercise – LÜKEX, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/germanynationalstrategiccrisismanagementexercise-lukex.htm; OECD (2014), 3rd OECD Workshop on Strategic Crisis Management, www.oecd.org/gov/risk/3rd-workshop-strategic-crisis-management.htm.

Key trends and self-assessment

Most countries have experienced at least one major crisis linked to a critical risk within the past 20 years for which they were not adequately prepared. In several cases this entailed an unidentified risk (e.g. the volcanic ash cloud over Europe), or a risk of unexpected magnitude or complexity (e.g. the Tohoku earthquake in 2011). Generally, countries have been highly responsive and active in revising their crisis management governance frameworks to foster inter-agency co-operation, to establish mechanisms for joint and co-ordinated use of scientific advisors and civil protection resources, and to strengthen government leadership as a core competence of good governance.

Countries have increased their technical capacities to forecast, detect and anticipate imminent hazards, threats and other circumstances that can introduce instability. Crisis managers continue to see challenges for further improving their capabilities to face the unexpected. Just over half the countries have established specific approaches to anticipate the unknown or more chaotic crises which are prevalent today. Few countries have established reflection groups of experts, however, that can be called on when a crisis is imminent. Such groups can augment sense-making capacities with the aim to untangle the complexities of unexpected crises.

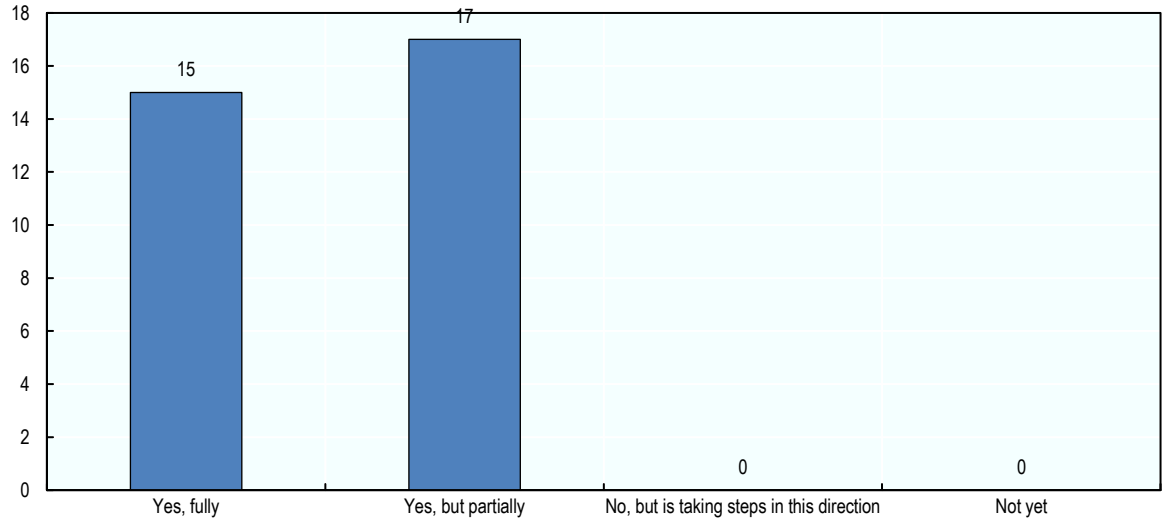
Countries have demonstrated a whole-of-society approach to crisis management, including leveraging private sector and civil society in the response system. Still, it is a challenge to articulate and co-ordinate their roles and functions with other emergency response actors. Many such groups become involved because they believe government services cannot be relied on; thus collaborating under the command and control of government could be counterproductive to their aims.

Countries have shown a high level of policy implementation in organising large-scale exercises and regular training courses. These include international response units and in a few instances have involved even the highest level of political leadership. Regular strategic crisis management drills and exercises have begun to include scenarios of cascading impacts due to critical infrastructure failures with cross-border impacts. Countries often find it a challenge, however, to involve political leaders in crisis preparedness.

Concerning the fourth key recommendation, the perspectives of respondents were mixed (Figure 5.3). In total, almost half (15) of the countries consider themselves as having fully

achieved the provisions of this recommendation, while 17 countries consider they have done so only partially.

Figure 5.3. Self-assessment on implementing the fourth key recommendation



Note: Answers received from 32 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Conclusions

Countries that have not done so already should establish specific approaches to anticipate unknown or more chaotic crises. This could be improved by co-ordinating response efforts and investing in crisis sense-making. If the crisis managers themselves do not have tools to help make sense of high levels of uncertainty, the challenge for leaders will be even more difficult.

To ensure that response capacities remain up to date with the evolving nature of disasters and crisis situations, countries should organise regular training and exercises for their emergency units. These include conducting large-scale exercises and exercises that include international response units, as well as cross-border crisis management exercises.

Countries should continue to develop their strategic crisis management capacities by training political leaders through dedicated exercises and by developing and "stress-testing" their capacity to cope with novel and large-scale emergencies. Major events test the highest levels of political leadership. Hence it is important to step up efforts to involve political leaders in crisis preparedness and to train them to develop their crisis management skill-set, including sense-making, decision-making and meaning-making.

References

FEMA (2013), Hurricane Sandy FEMA After-Action, Federal Emergency Management Agency, United States, https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

Korea National Disaster Management Institute, "GIS-based information integration framework for disaster risk management", presentation at the 2015 OECD workshop on Strategic Crisis Management .

OECD (2016a), OECD Survey on the Governance of Critical Risks, OECD, Paris.

OECD (2016b), Toolkit for Risk Governance: Italian system for the mobilisation of volunteers in civil protection, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/italiansystemforthemobilisationofvolunteersincivilprotection.htm.

OECD (2016c), Toolkit for Risk Governance: US National Incident Management System (NIMS), https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/usnationalincidentmanagementsystemnims.htm.

OECD (2016d), Toolkit for Risk Governance: Denmark's Pandora Cell for crisis anticipation, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/denmarkspandoracellforcrisisanticipation.htm.

OECD (2016e), Toolkit for Risk Governance: Switzerland's Federal Rapid Reflection Force, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/switzerlandsfederalrapidreflectionforce.htm.

OECD (2016f), Toolkit for Risk Governance: UK Scientific Advisory Group in Emergencies, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/ukscientificadvisorygroupinemergencies.htm.

OECD (2016g), Toolkit for Risk Governance: Germany National Strategic Crisis Management Exercise – LÜKEX, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/germanynationalstrategiccrisismanagementexercise-lukex.htm.

OECD (2014), 3rd OECD Workshop on Strategic Crisis Management, www.oecd.org/gov/risk/3rd-workshop-strategic-crisis-management.htm.

Chapter 6. Transparency, accountability and lessons learned

This chapter addresses implementation of the fifth key OECD Recommendation of the Council on the Governance of Critical Risks. This Recommendation calls on countries to demonstrate transparency and accountability in risk-related decision-making. The chapter first focuses on how countries are incorporating good governance practices and continuously learning from experience and science. It then presents countries' key trends and self-assessments. The conclusions present ways countries can further benefit from lessons learned.

Good practices and policy tools

Share information used in risk management decisions

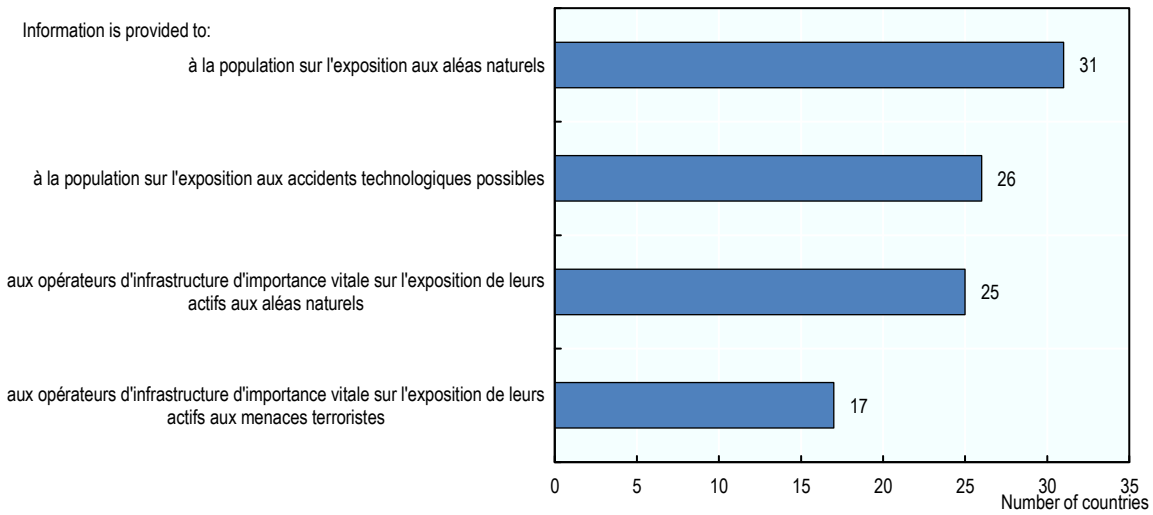
Countries should be transparent with information used in making risk management decisions to ensure they are better accepted by stakeholders, to facilitate policy implementation and to limit reputational damage. Providing public access to the information used in policy design can help neutral third parties to evaluate and validate risk management decisions objectively. It is important for stakeholders to be able to hold risk management decisions to account by testing the assumptions behind risk analyses and potentially improving on risk assessment models.

Empowering the public with risk information provides reassurance that risk management policies and decisions are grounded in evidence and designed to serve the public interest. Public access to the underlying information and data used for risk analysis also increases stakeholder engagement.

Thirty-one of the 34 countries that responded to the OECD Survey on the Governance of Critical Risks make information available about the public's exposure to natural hazards (Figure 6.1). In some cases this information also includes self-protection measures to reduce and prepare for risks (Box 6.1). Only 26 countries share information on the public's exposure to technological accidents (Box 6.2). This lower availability of access to information might be explained by the responsibility resting primarily with the private sector operators of facilities where accidents could occur rather than with the government department that responded to the survey. Factories where hazardous substances are produced, processed or stored are often required to inform the public about potential exposure to toxic materials, radiation, explosions, etc. Among member states of the European Union, industries dealing with hazardous substances are required to make information available to the public in furtherance of the Seveso Directive. The directive is widely considered a benchmark for chemical safety in industrial plants and has been a reference for legislation in many countries (see Chapter 4).

Survey respondents indicated that making risk exposure information available to critical infrastructure operators is less common. Their countries are uneasy with providing information to the public on exposure of critical infrastructure to terrorist threats (Figure 6.1). Twenty-five respondents reported that infrastructure operators receive information about exposure to natural risks, but only 17 reported that information about impending terrorist threats is provided. In a context of increased threat levels, this is becoming more a concern for critical infrastructure operators that want to take an intelligence-led risk informed approach. Box 6.3 offers a good example from Australia that highlights how the intelligence community and the private sector can communicate information effectively.

Figure 6.1. Providing information on risk exposure



Note: Answers were received from 33 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Foster an honest and realistic dialogue with the public

Countries should dialogue with the public about the nature of hazards and threats as well as the potential impacts and the cost-effectiveness of various mitigation, response and recovery options. Some governments also inform stakeholders about the basis of the assessment and the government's judgement of the most likely and most serious types of emergency. In the United Kingdom, for example, the national risk register for civil emergencies provides information not only on the exposure of citizens and infrastructure to all hazards facing the national territory, but also on how the likelihoods and impacts of civil emergencies are assessed, and on what types of risk management options are envisaged (United Kingdom Cabinet Office, 2017).

Similarly, in Mexico, the National Centre for Disaster Prevention (CENAPRED) makes information available on the data used to develop risk assessment through the National Risk Atlases, an innovative web tool that integrates data on exposure and vulnerability. The Risk Atlases are accessible via Internet for most federal states, informing the public and businesses about natural and technological (mostly related to toxic and flammable substances) risks to which they are exposed as well as about the risk reduction measures undertaken.

Austria provides information on the results of hazard assessment processes and risk management options. The government engages in an open dialogue with citizens in the process. After draft hazard assessments are carried out by government experts, they are subject to a public consultation where a commission collects and assesses comments. Experience shows that this process is not necessarily used by private interests to decrease the size of hazard zones, but rather for citizens to bring in local knowledge on experiences with past disasters. Involving citizens in this process has often led to an expansion of the proposed hazard zones and hence an increased acceptance of the risk assessment process.

A high number of countries show signs of progress concerning the transparency of risk information, for example by communicating about risks associated with exposure to natural hazards. However, in a context of increased terrorist threats, some countries have begun to reduce the amount of information shared with the public, in particular information indicating potential target areas for malicious acts. In France for example, following the June 2015 bombing of a chemical plant near Lyon and attacks on two oil tanks at a petrochemical site near Aix-en-Provence, the government launched an action plan aimed at strengthening the protection against malicious acts of Seveso classified establishments. The plan includes balancing the requirement of transparency with the confidentiality of data relating to the characteristics and functioning of Seveso sites.[1] This example shows that the benefits of transparency in risk information need to be weighed against jeopardising national security.

Box 6.1. Providing public access to risk information and self-protection measures for natural hazards: Austria and Switzerland

In Austria, publicly accessible Internet portals, such as www.hora.gv.at, provide easily accessible hazard information. Exposure to multiple hazards (such as floods, avalanches and torrents) can be explored based on individual addresses. In addition, information on natural hazards is transmitted through brochures, booklets and leaflets, as well as via age-tailored initiatives, such as the *Biber Berti* programme. The Austrian Civil Protection Association adds to this by informing the public about self-protection measures, using local safety and security information centres to directly communicate to the public.

In Switzerland, the government has partnered with insurance providers, which now inform customers about both the hazards they face and appropriate self-protection measures. To support risk-adapted behaviours, some insurance providers have developed automated text messages that warn about bad weather or imminent disasters. The Swiss risk management agencies themselves have also taken steps to make information on natural hazards easily accessible. Examples include the www.natural-hazards.ch platform, where information on current hazard warnings, previous events and measures to deal with natural hazards are described in the country's four languages, as well as in English. Another good practice is the "Risk Dialogue" initiative (www.planat.ch/en/risikodialog/), which aims to raise risk awareness among all stakeholders and to inform about available risk reduction and preparedness measures. Beyond that, it outlines the responsibilities of public authorities, including sub-national governments, with regard to risk communication. This enables the public to hold their authorities accountable, if natural hazard information is not adequately communicated.

Source: OECD (2017), "Boosting resilience through innovative risk governance: The case of Switzerland", http://dx.doi.org/10.1787/9789264281370-7-en; OECD (2016b), "Boosting Resilience through Innovative Risk Governance: The Case of Alpine Areas in Austria"; Swiss Confederation (2017), www.natural-hazards.ch/home/current-natural-hazards.html; National Platform for Natural Hazards (2017), www.planat.ch/en/risikodialog/; Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management (2017a), Natural Hazard Overview & Risk Assessment Austria, http://hora.gv.at/; Austrian Civil Protection Association (2017), www.zivilschutzverband.at; Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management (2017b), Biber Berti, www.biberberti.com/de/index.php.

Box 6.2. Providing public access to technological hazards information: European Union, Germany and United Kingdom

In the **European Union**, the online Major Accident Reporting System (eMARS) regularly publishes information on lessons learned. In particular, it facilitates the exchange of information on accidents and near misses that have occurred in major hazard establishments in Europe and globally, as well as technical reports on chemical accident prevention. This platform went online in 2008, following the European Commission Decision of 2 December 2008 (European Commission, 2008). The original database, MARS, was launched as a voluntary mechanism under the first Seveso Directive in 1984 (82/2015/EC). It became the official reporting mechanism (using a desktop application) when recording major chemical accidents became an obligation of the Seveso II Directive (96/82/EC) for member states and European Economic Area countries. The regulatory obligation to report major accidents to eMARS was maintained in the current Seveso III Directive (2012/18/EU).

In 2000, member countries of the OECD agreed to exchange accident information voluntarily through the eMARS database. The database therefore also contains reports from Canada, Japan, Korea, Switzerland and the United States. At the same time, parties to the United Nations Economic Commission for Europe's Convention on the Transboundary Effects of Industrial Accidents also agreed to report transboundary chemical accidents to the database. Additional third parties are encouraged to use the database, and currently China has provided nine accident reports to eMARS.

In **Germany**, the Central Reporting and Evaluation Centre for Major Accidents and Incidents in Process Engineering Facilities (ZEMA), at the Federal Environmental Agency, is the key actor making information about technological accidents and incidents public. It documents, assesses and publicises all technological accidents and incidents that are subject to statutory reporting requirements in annual reports, sub-dividing the events according to their hazard potential (major accidents and disturbance of normal operation). In addition, ZEMA runs a publicly accessible database, where citizens can access information on past events. The database includes a search function by zip code, as well as by date, intensity, type of industry affected and cause of the accident.

In the **United Kingdom**, the Health and Safety Executive regularly publishes bulletins on its website (www.hse.gov.uk/safetybulletins/). The health and safety bulletins aim to share information with those that might be affected by failures in equipment, process, procedures and substances. The bulletins can be accessed online, via an email newsletter or through RSS feeds (including on mobile phones). Depending on the incident, the bulletin takes the form of a safety alert or of a safety notice. Safety alerts are for major accidents that would result in a serious or fatal injury and where immediate remedial action is required, while safety notices are issued to facilitate a change in procedure or if the level of protection needs to be improved. They may also include instructions for a potentially dangerous situation.

Sources: UBA (2017), "Zentrale Melde- und Auswertestelle für Störfälle und Störungen, German Environment Agency, www.umweltbundesamt.de/themen/wirtschaft-konsum/anlagensicherheit/zentrale-melde-auswertestelle-fuer-stoerfaelle; HSE (2017), What are health and safety bulletins?, www.hse.gov.uk/safetybulletins/whatarebulletins.htm; European Commission (2017), eMARS (database), https://minerva.jrc.ec.europa.eu/en/emars/content/.

Box 6.3. Providing intelligence information to the private sector: Australia

The Business Liaison Unit (BLU), within the Australia Security Intelligence Organisation (ASIO), provides a public interface between the Australian Intelligence Community and the country's private sector. The BLU's role is to provide reliable information to Australian business security managers about national security issues, enabling them to do the following:

- recognise and respond to national security threats
- develop risk mitigation strategies appropriate to their business
- provide informed briefings to executives and staff.

The BLU website contains intelligence-backed unclassified reporting on the domestic and international security environment. This reporting is drawn from the full range of ASIO's information holdings and expertise, including the multi-agency National Threat Assessment Centre. The BLU has a large range of reports and products available on the website covering the international and domestic security environment, security threats to specific critical infrastructure sectors, terrorist incidents, issue motivated groups, espionage, physical and personnel security, and tactics and methodology. The website also includes reports and products from other Australian government departments and some foreign intelligence agency reports.

In support of its website, the BLU engages directly with businesses on a one-to-one basis, working to build strong relationships between ASIO and the private sector. Additionally, the BLU manages an executive programme on behalf of the Director-General of Security to raise national security matters at the levels of chief executive officer and board of directors in major Australian companies. Subscribers to this secure website cover a diverse range of industry sectors, and subscription is free.

Source: Australian Government (2017), Australian Security Intelligence Organisation website, https://www.blu.asio.gov.au/about-us.

Make the most of resources dedicated to public safety, national security, preparedness and resilience

Decision-making should be well grounded in evidence that clarifies trade-offs. Objectives should be continuously monitored to evaluate how effectively they serve the public interest and to ensure they are not arbitrary or politically expedient. Countries have implemented a mix of policy tools and practices to inform decisions, optimise resources, and ensure oversight such as quality assurance audits and open government platforms, as well as analytical frameworks governing resource allocation and personal accountability.

Respondents pointed to technical decision-support tools that help identify the marginal cost of achieving additional levels of safety and security through preparedness, prevention or resilience investments. These tools can align the level of such investments to the level of security and resilience that is both desirable and affordable. Decision-support tools, such as multi-criteria and cost-benefit analysis, enable countries to compare options and evaluate the advantages and disadvantages of different courses of action.

Respondents identified, for example, the loss exceedance curve. It plots the annual probability of aggregate disaster losses exceeding the annual average amount of disaster losses based on past events. This tool provides decision makers with a marker to guide investment decisions aimed to avoid or reduce disaster losses.

A high number of countries have established a common framework for allocating resources in risk management. In the United Kingdom, for example, the British Health and Safety Executive advises on how to determine acceptable levels of risk with regard to industrial hazards (Davies and Etheridge, 2004).

In Switzerland, the direct democratic tradition has shaped how risk management investments are decided on. Significant protective infrastructure investments are publicly scrutinised through often lengthy consultation processes. Although blockages can occur by only a minority of citizens opposing investment plans, this process has by and large ensured an efficient and effective provision of protective infrastructure that enjoys the strong support of the country's population.

Respondents pointed to audits and review mechanisms as means to improve risk management capacities. These measures provide independent opinions and recommendations on the use of public resources for emergency preparedness and risk reduction measures. A good practice example comes from Norway. There the Ministry of Justice and Public Security has audited each ministry that shares responsibility for emergency preparedness to ensure a comparable level of quality through efficient use of public resources (Box 6.4). In Turkey, the Court of Account has developed a specific way to ensure post-disaster assistance, and funding contributes to developing higher safety standards and to strengthening resilience in general.

Box 6.4. Audits for enhanced emergency preparedness: Norway

In Norway, each ministry is responsible for civil protection and emergency preparedness planning in its own sectoral area. This covers both direct management of underwritten agencies and businesses, and broader responsibility for public security vis-à-vis actors such as municipalities, private sector and non-governmental organisations within the ministry's policy area. Furthermore, each ministry must define its roles and the areas of importance to public security. The ministries are also responsible for obtaining an updated assessment of risk and vulnerability for their sectors (including the ministries themselves). Based on the risk analysis and an assessment of available measures, each ministry must assess, decide on and implement measures to reduce vulnerabilities and weaknesses within its entire area of responsibility. The ministries must also establish contacts with other ministries to ensure that their work is well co-ordinated. These requirements are laid down in the Instruction for the ministries' work with civil protection and social security (revised 1 September 2017).

The Ministry of Justice and Public Security oversees audits as a quality assurance measure to ensure each ministry meets the requirements. The Directorate for Civil Protection and Emergency conducts the audits on behalf of the Ministry of Justice and Public Security. The purpose of the audits is to contribute to high quality civil protection and emergency preparedness planning within each ministry's area of responsibility, as well as targeted and efficient use of resources for civil protection and emergency preparedness. If the audit reveals violations, the responsible ministry must take the necessary measures to meet the requirements. The audit ends when the government concludes that all requirements are met.

Source: OECD (2016c), Toolkit for Risk Governance: Norway Quality Assurance for National Preparedness, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/norwayqualityassurancefornationalpreparedness.htm.

Respondents identified the efficient use of public resources as a particular challenge during the recovery and reconstruction phases of disaster risk management. Unlike pre-crisis preparedness and prevention investments, which can be planned for as part of a normal budget process, the recovery and reconstruction phases are marked by especially time sensitive needs for financial assistance. Adequate evaluation and oversight of disbursements are balanced against the pressure for meeting basic needs, especially housing. Respondents highlighted the risks of waste and undue influence in procurement contracts as reasons behind the need for tools to ensure transparency in how emergency funds are spent. Chile, Italy and Mexico offer good practice examples of open government platforms that provide information on specific transfers of post-disaster assistance to individual households and firms (Box 6.5).

Box 6.5. Ensuring efficient use of public resources in the early recovery and reconstruction process: Chile, Italy and Mexico

After a major earthquake struck off the coast of central **Chile** in 2010, the national government decided on a sizeable four-year reconstruction programme to be implemented by the Ministry of Housing and Urban Development with an envelope of USD 2.75 billion. The government wanted to ensure that the funding, mostly allocated to reconstructing housing and public infrastructure, was effectively used and its disbursement monitored. The government therefore set up an online platform that provided information on the use of resources. In addition, it published regular implementation reports and established a direct dialogue with citizens, the private sector and civil society. The focus on resource efficiency and open dialogue ensured trust in Chile's government during this critical period.

Launched in **Italy** after the 2009 L'Aquila earthquake that struck the Italian region of Abbruzzo, the *Open Data Ricostruzione* portal was established to increase transparency and efficiency in the use of public resources in the reconstruction phase. The portal collects, systematises and makes available all information relating to the investments made during the reconstruction processes. It is in an easily accessible tool for various stakeholders, including citizens and researchers. The portal provides information on the allocation and use of funds as well as the progress in implementing public works programmes, including technical and administrative details on the procedures.

In **Mexico,** a centralised Natural Disaster Fund (Fonden) finances response and recovery needs in the aftermath of natural disasters. *ReconstrucciónMX* was been created to increase transparency and efficiency in the use of the Fund's resources. It collects information from various sources and levels of government involved in the response and recovery process of communities affected by natural disasters. It provides easy access to information on recovery needs and measures being implemented in the affected areas, both to the general public and to the decision-making and operating agencies. To further increase transparency and accountability in the use of funds, *ReconstrucciónMX* allows citizens to directly report on any observed misuses of the Fund's resources.

Source: OECD (2016d), Toolkit for Risk Governance: Chile Reconstruction Process Transparency, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/chilereconstructionprocesstransparency.htm; GSSI (2017), OpenData Ricostruzione, http://opendataricostruzione.gssi.it/; OECD (2016e), Observatory of Public Sector Innovation website, https://www.oecd.org/governance/observatory-public-sector-innovation/home/.

Share knowledge through post-event reviews

The Recommendation calls on countries to continuously share knowledge, including lessons learned from previous events, research and science through post-event reviews. The purpose is to evaluate the effectiveness of prevention and preparedness activities, as well as response and recovery operations, in order to identify the lessons learned for policy makers. In the aftermath of a major disaster, policy makers often declare, "It will never happen again". Vested interests can stand in the way of meaningful reforms. Post-disaster reviews should consider objectively the effectiveness of prevention and preparedness measures, as well as response and recovery operations.

When asked, 27 respondents stated that they had conducted a post-disaster evaluation of risk management policies within the previous three years. This high number provides evidence that post-disaster evaluation processes are becoming a common feature across countries. Such reports not only help identify gaps in the implementation of existing policies during crises, but are used to evaluate the need to reform existing policies.

In the United Kingdom, for example, following the devastating floods of 2007, the *Pitt Review* was launched to evaluate the lessons to be learned from this catastrophic event, with a view to make high-level recommendations for improving policy. The report collected evidence about the houses impacted by floods to show that they had been built in areas known to be at risk. The report subsequently made proposals to strengthen land-use prescriptions and their enforcement (Pitt, 2008).

Another example of a large-scale lessons learned process concerned the response to Hurricane Katrina (The White House, 2005). This report identified deficiencies in the United States federal government's response to the hurricane. It also suggested measures to improve policies for all levels of government as well as for non-governmental stakeholders to strengthen emergency preparedness and response.

Organise briefings for stakeholders

When asked, only 21 respondents stated that they had communicated the results of post-disaster evaluations to the public within the previous three years. However, a high number of countries provide links to lessons learned in post-disaster technical reports. This effort is an important step, but the relevant technical findings could be summarised and formulated for a wider audience, including the media, the third sector, academics and business associations. Countries should meaningfully dialogue with stakeholders with a view to change future behaviour.

Good practice examples of detailed, yet engaging reports written for the public include the above-mentioned *Pitt Review* and the 9/11 Commission report. These reports led to comprehensive sets of policy recommendations that their respective governments implemented. The reports also provided a factual evidence base for debate in the policy reform process. The subsequent policies have helped increase the overall capacity to prevent and respond to disasters.

Incorporate lessons learned into preparedness and resilience planning

Continuously improving risk management policies requires learning from experience and incorporating findings into revised policies. Results of post-disaster evaluations can inform marginal changes in the implementation of existing policies. But, where more substantial gaps are revealed, they need to support more significant institutional changes and reform processes. These must be built on a continuous effort of collecting evidence and forming public awareness.

When asked, 21 respondents stated that their governments have used the results of lessons learned evaluations to revise risk management policies. Box 6.6 provides good examples of how recent post-disaster evaluations across countries have led to revised policies. Despite the fact that most of the countries have suffered a major disaster within the past 15 years, this survey result shows evidence that many countries are stalling on revising risk management policies.

Across countries, examples can be found of lessons learned in the aftermath of a major disaster that have sparked significant policy reforms. For example, the 9/11 terrorist

attacks in the United States led to the enactment of the United States Patriot Act. This is a central provision for removing obstacles to information sharing between the intelligence and law enforcement communities with the aim of intercepting and obstructing terrorism. The Great East Japan Earthquake in 2011 triggered a major re-thinking in energy policies in Japan and abroad. It led to a decision in Germany to phase out its nuclear energy and close all plants by 2022.

The National Civil Protection System of Mexico (SINAPROC) was established to improve the country's civil protection capacities following the devastating earthquakes of 1985. Mexico realised that ad hoc co-ordination efforts for response and recovery were no longer sufficient to address challenges from large-scale disasters, and that a comprehensive and systematic approach to co-ordination was needed.

In Sweden, after a severe winter storm in Gudrun in January 2005, the government reformed the electricity market. This measure has led power companies to invest in putting power lines underground.

Box 6.6. Evaluations used to revise risk management policies: Ireland, Japan, Netherlands, New Zealand and Norway

In **Ireland**, the "Guidelines for coordinating a national level emergency response" include a systematic post crisis review process with a generic template to document all lessons learned. While a National Framework for Emergency Management was under discussion with a generic review of the system, the repetitive severe weather events of the winter of 2013-14 and large-scale flooding in the country provided key lessons to be integrated into this process. These included issues related to (i) harmonising early-warnings and integrating them into the emergency preparedness process, (ii) better linking local and regional mechanisms with national emergency planning and response, and (iii) measuring economic losses from disasters to facilitate recovery financing and prioritise prevention investment.

In **Japan**, the International Research Institute of Disaster Science (IRIDeS) of the Tohoku University identified lessons from the Great East Japan Earthquake. Its report proposes 37 recommendations ranging from such topic as evacuation processes, tsunami early warning systems, building back better after a disaster, structural mitigation measures and territorial planning in tsunami-prone areas. This post-crisis research is the first major outcome of IRIDeS which was established after the earthquake in the tsunami affected areas. IRIDeS has become a world reference for disaster management research, with a secure ten-year budget from the national government.

In the **Netherlands**, since 2012 the National Coordinator for Security and Counterterrorism of the Ministry of Security and Justice manages all hazards and threats with its National Crisis Centre (NCC). The NCC is a flexible structure of crisis management professionals which can support all sectoral ministries in a crisis situation with specific tools for sense-making, decision-making and meaning-making. This recent set-up aims to respond to deficiencies identified through different evaluation processes. These include the lack of leadership and professional crisis management capacity, overly sectoral approaches, complicated structures and slow reactiveness, inappropriate crisis communication, and inefficient exercises. Given the low frequency of crises in the Netherlands, the opportunities of mass gathering events were utilised to

test and run this new structure, including the coronation of the new king in 2013 and a Nuclear Security Summit in 2014. When the MH17 flight crashed in Ukraine in July 2014 with many Dutch citizens aboard, this crisis structure was up and running in 30 minutes. It efficiently established a picture of the situation and supported decision-making and communication, with full trust and confidence between all partners involved.

In **New Zealand**, each crisis that takes place is subsequently reviewed by a formal process to draw lessons and revise procedures. Following the Christchurch earthquakes in 2010-11, and other previous crises, a new risk and crisis management paradigm has emerged that distinguishes exceptional events from more routine crises. A traditional approach for the latter is based on risk mitigation measures and standard rules in the response phase. However, the former requires a revised approach that accounts for more uncertainty and complexity. This approach is grounded in principles and guidelines that are based on pre-agreed governance arrangements. They aim to strike a balance between proactive and reactive investment and allow for both risk management and resilience.

In **Norway,** a commission was established after the July 2011 attacks. It identified a series of failures which taken together explained how this tragic event happened despite the fact that security measures and emergency preparedness had been high on the government's agenda for years. The commission's report pointed to the need to learn from exercises, to co-ordinate and interact across agencies, and to exploit information and communications technology. A number of initiatives, measures and changes have been implemented at the political, strategic and tactical levels in the aftermath of the attacks. These include strengthening the co-ordinating role of the Ministry of Security and Justice, the Action Plan against radicalisation and violent extremism, and policies aimed to promote government business continuity. Three years after the attacks, the recently established Commission on Digital Vulnerability became involved in the issues of surveillance of Internet activities and the challenge to find the acceptable balance between individual freedom and national security measures.

Source: OECD (2014), Workshop on "Learning from crises and fostering the continuous improvement of risk governance and management", Oslo, Norway, 17-18 September 2014, www.oecd.org/gov/risk/high-level-risk-forum-oslo-workshop-2014.htm.

Support scientific research

The Recommendation calls for incorporating findings from research and science, while guarding against unintended adverse impacts, such as the creation of additional risks or the failure to recognise potential changes in risk characteristics. The adoption of new public policy tends to occur more slowly than the processes that drive many critical risks. Investment in scientific research and technological development can provide knowledge and data to inform and continuously improve risk management policies. Research on potential drivers of risks, such as increased urbanisation, critical infrastructure dependencies or climate change, improves risk assessments and in turn leads to improved risk management policies. Research and science can also benefit from open approaches, allowing scientists to use compiled basic data and pull out trends and effects of hazards and threats. Updated knowledge about hazard exposures and drivers of vulnerability can

ensure that the evolution of risk management policies keeps pace with the processes that can drive new risks.

When asked, 28 respondents reported that their government invests in scientific research and technological development related to managing critical risks. A popular research theme across a high number of countries is climate change related risks. For example, Austria has engaged in developing a forward-looking approach to its risk prevention and mitigation management by regularly updating dynamic hazard zone maps and adapting protective infrastructure to the potential impacts of climate change. France has developed a national observatory on the effects of climate change. It is designed to collect and disseminate information on the risks linked to global warming and make recommendations on the adaptation measures to be considered to limit the impacts of climate change.

Similarly, in Japan, the Program for Risk Information on Climate Change has been put in place to advance the available technology for climate change projection, predict the probability of the occurrence of extreme concentrated heavy rainfall and conduct risk evaluation research of the associated damages. However, how much of this research has been applied to improve management policies remains an open question.

Good practice examples also come from Canada, Germany and the United States. They have applied programmes to unlock the potential of science and technology in order to improve risk management policies (Box 6.7).

Box 6.7. Science and technology for disaster risk management: Canada, Germany and United States

Integrating science and technology into both policy making and implementation for disaster management is critical to help improve disaster risk management. Through science and technology, new and more efficient ways to prevent, prepare for and respond to disasters become possible. Here are examples of countries that have recognised the value of science and technology and promote its use.

In **Canada**, the Canadian Safety and Security Program (CSSP) was created to unite the knowledge and expertise of the science and technology community with the policy, operations and intelligence expertise of the government. Under the project, funding is available to support joint projects that include both a project partner from any level of government, as well as a non-governmental partner.

In **Germany**, the Federal Office of Civil Protection and Disaster Assistance (BBK) maintains a research programme that focuses on research into chemical, biological, radiation and nuclear hazards. In addition, the BBK regularly supports research projects that improve the knowledge base for civil protection action. Recent examples include projects on improving early warning systems and risk communication, and establishing standards to protect critical infrastructure.

In the **United States**, the Department of Homeland Security's Science and Technology Directorate (S&T) Office of University Programs taps the expertise of the nation's colleges and universities to tackle homeland security problems. Through the programmes, the Department can access academic expertise to answer research questions, deliver technical solutions and build a highly specialised workforce. The Minority Serving Institutions Program provides grants and awards to build a diverse, highly capable,

technical workforce for the homeland security enterprise. Linked with the Department's Centers of Excellence, these programmes provide the homeland security community with a broad pool of high achieving students who bring valuable insight and understanding to complex security challenges.

Source: Government of Canada (2016), "Canadian Safety and Security Program", news.gc.ca/web/article-en.do?nid=1060469; BBK (2017), Federal Office of Civil Protection and Disaster Assistance, www.bbk.bund.de/DE/AufgabenundAusstattung/Forschung/Forschungsfoerderung/forschungsfoerderung_node.html; DHS (2017), Science & Technology Strategic Plan 2015-2019, https://www.dhs.gov/science-and-technology/centers-excellence.

Key trends and self-assessment

Countries have shown progress in making information about natural hazards publicly available. But they should interact more with the public, as this information can be the foundation for policy dialogue. Information on hazard exposures can be accessed if requested or researched. However, few countries provide opportunities for the general public to discuss the cost-effectiveness of various mitigation, response and recovery options before putting them in place. Typically such consultations are held with specialised commissions and experts. Publishing post-disaster evaluations is fairly common, but discussing the findings in public fora to consider revising risk management policies is not.

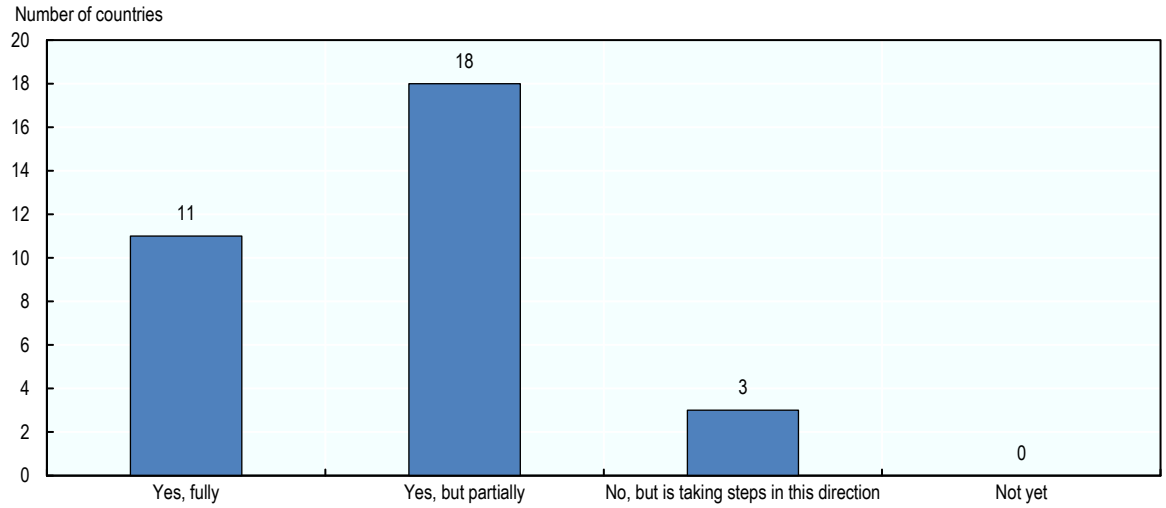
Transparency in risk-related decision-making is now well understood, although countries rarely share information for debating a specific disaster risk reduction measure that could affect property interests. Not all countries that conduct post-disaster evaluations make them available to the public for dialogue on how to reconstruct after a disaster, and fewer still have shown that they use the evaluations to revise risk management policies. Many governments have realised that revised approaches to post-disasters reviews are needed, but they remain uneasy about communicating risk information beyond communities of experts.

Since the 2008 financial crisis, many countries have undergone reforms that emphasise fiscal discipline and accountability. Disaster risk management policies are often scrutinised for not making the best use of resources. However, this may be justified given a lack of priority setting tools, of clearly defined trade-offs and of monitoring progress. A few countries are transparent with regard to information concerning where public funds are spent on disaster risk management programmes, especially in the context of recovery assistance and reconstruction funding for public infrastructure and housing.

Countries have shown wide support for scientific research which focuses on better understanding the implications of climate change on risk management policies. Investing in social and natural sciences research has helped countries to revise priorities for shoring up preparedness capacities, and in some cases to build evidence-based evaluations of risk management policies. Research and technology development efforts across disciplines have been useful for reviewing both what has and has not worked well in the past.

The self-assessment responses highlight that many countries are still struggling to fulfil the provisions of the fifth key recommendation (Figure 6.2). In this area, countries rated themselves relatively low. Less than one-third of the countries believe they have fully met it, while the majority believes they have fulfilled it partially.

Figure 6.2. Self-assessment on implementing the fifth key recommendation



Note: Answers received from 32 out of 34 responding countries.
Source: OECD (2016a), OECD Survey on the Governance of Critical Risks.

Conclusions

In line with the Recommendation, countries should ensure transparency in risk management decisions not only by making information available, but by creating conditions for stakeholders to use the information during the policy formulation phase. This can foster stakeholder buy-in, facilitate policy implementation by reducing compliance costs and limit reputational damage. Where they have not yet done so, countries should make the factual basis for risk management related decisions transparent in order to ensure that policies gain public acceptance and are continually improved. Many countries have implemented good governance principles into risk management policies for natural hazards, but these efforts remain incomplete. In particular, the underlying data and information of risk analyses for disaster risk reduction policies are often not made publicly available to avoid scrutiny by third party experts. This cloaks important policy decisions in opaqueness and can provoke resistance, especially to land-use prescriptions, on grounds that they are arbitrary or serve a private interest.

Countries should consider undertaking voluntarily a risk governance review to identify good practices that could potentially transfer to other countries, as well as improve areas for themselves. Many countries make strong efforts to support scientific research. However, these efforts need to continue and be reinforced if the evolution of risk management policies is to keep pace with the processes that drive emerging risks. Several countries have already worked closely with the OECD to monitor and evaluate specific risk management policies relevant to the Recommendation. These efforts increase capacity to make the most of existing resources, set priorities and align agendas with a wide range of stakeholders.

Where they have not yet done so, countries should put in place systematic processes to learn from past events, near miss-events and similar risks encountered by different organisations. They should also develop knowledge-sharing platforms with international partners. It is important to periodically take a step back from the status

quo and consider how research and post-event reviews can help improve risk management policies. Performing regular quality assurance audits is a good practice that more countries could apply. But for most countries, empowering one ministry to audit all other ministries' implementation of risk management policies remains a challenge. An alternative approach is to require an audit process in each ministry. While post-disaster policy evaluations are conducted regularly, the results often are not communicated to the public and seldom lead to systematic risk management policy reforms.

References

Austrian Civil Protection Association (2017), Austrian Civil Protection Association website, www.zivilschutzverband.at/.

Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management (2017a), Natural Hazard Overview & Risk Assessment Austria website, http://hora.gv.at/.

Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management (2017b), Biber Berti website, www.biberberti.com/de/index.php.

Australian Government (2017), Australian Security Intelligence Organisation website, https://www.blu.asio.gov.au/about-us.

BBK (2017), Federal Office of Civil Protection and Disaster Assistance, Germany.

Davies, P. and B. Etheridge (2004), *Horizontal Scanning*, UK Health and Safety Executive Board Paper HSE/04/027, 27 September 2004.

DHS (2017), Science & Technology Strategic Plan 2015-2019, United States Department of Homeland Security, https://www.dhs.gov/science-and-technology/centers-excellence.

European Commission (2017), eMARS (database), https://minerva.jrc.ec.europa.eu/en/emars/content/.

Government of Canada (2016), "Canadian Safety and Security Program", http://news.gc.ca/web/article-en.do?nid=1060469.

GSSI (2017), OpenData Ricostruzione, Gran Sasso Science Institute in collaboration with the University of L'Aquila, the Aquila Municipality Special Reconstruction Offices and ActionAid, http://opendataricostruzione.gssi.it/.

HSE (2017), What are health and safety bulletins?, Health and Safety Executive, United Kingdom, www.hse.gov.uk/safetybulletins/whatarebulletins.htm.

National Platform for Natural Hazards (2017), "Praxiskoffer Risikodialog Naturgefahren" [Praxis box risk dialogue natural hazards], www.planat.ch/en/risikodialog/.

OECD (2017), "Boosting resilience through innovative risk governance: The case of Switzerland", in Boosting Disaster Prevention through Innovative Risk Governance: Insights from Austria, France and Switzerland, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264281370-7-en.

OECD (2016a), OECD Survey on the Governance of Critical Risks, OECD, Paris.

OECD (2016b), "Boosting Resilience through Innovative Risk Governance: The Case of Alpine Areas in Austria", Preliminary Version, OECD, Paris.

OECD (2016c), Toolkit for Risk Governance: Norway Quality Assurance for National Preparedness, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/norwayqualityassurancefornationalpreparedness.htm.

OECD (2016d), Toolkit for Risk Governance: Chile Reconstruction Process Transparency, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/chilereconstructionprocesstransparency.htm.

OECD (2016e), Observatory of Public Sector Innovation website, https://www.oecd.org/governance/observatory-public-sector-innovation/home/

OECD (2014), Workshop on "Learning from crises and fostering the continuous improvement of risk governance and management", Oslo, Norway, 17-18 September 2014, www.oecd.org/gov/risk/high-level-risk-forum-oslo-workshop-2014.htm.

Pitt, M. (2008), *The Pitt Review: Learning Lessons from the 2007 Floods*, http://webarchive.nationalarchives.gov.uk/20100702215619/http://archive.cabinetoffice.gov.uk/pittreview/thepittreview/final_report.html.

Swiss Confederation (2017), Natural Hazards Portal, www.natural-hazards.ch/home/current-natural-hazards.html.

The White House (2005), *The Federal Response to Hurricane Katrina Lessons Learned*, Washington, DC, https://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/References.

UBA (2017), "Zentrale Melde- und Auswertestelle für Störfälle und Störungen" [Central Reporting and Evaluation Center for Malfunctions and Disorders], German Environment Agency, www.umweltbundesamt.de/themen/wirtschaft-konsum/anlagensicherheit/zentrale-melde-auswertestelle-fuer-stoerfaelle.

United Kingdom Cabinet Office (2017), *National Risk Register of Civil Emergencies*, London, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf.

[1] See *Instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance* (NOR: DEVP1518240J): http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&r=39951.

Annex A. Technical notes

Average annual deaths per million inhabitants, 1995-2015

The average annual deaths per million inhabitants is calculated using the sum of the total number of deaths *n* caused by a disaster *d* during a year *j* multiplied by 1 million, which is then divided by the country's population *POP* for the year *j* for each country *i*. If for one year there are no disasters or no deaths, the value for that year will be 0. The final average rate for the country over the period 1995-2015 will be as follows:

$$Number\ of\ deaths\ per\ 1\ million\ inhabitants\ for\ country_i = average\left(\frac{\sum_d X_{dij} \times 1\,000\,000}{POP_{ij}}\right)$$

$$Where:$$

$X_d = estimated\ deaths\ per\ disaster\ d$

$POP = population\ estimates\ according\ to\ OECD\ population\ database$[1]

We assume that "missing" for the variable "total deaths" corresponds to 0 deaths. This implies that we will slightly underestimate the average value. However, deaths are well reported in *The Emergency Events Database* (EM-DAT) with few missing values.

The OECD average is the non-weighted arithmetic mean of the 35 OECD member countries. It does not include data for non-members.

Due to methodological differences in the attribution of deaths due to heatwaves, the figure comparing average deaths per million inhabitants against the OECD average excludes these deaths.

The period of time 1995-2015 was chosen because gross domestic product (GDP) data for several OECD countries is not calculated before 1995, and not all of them have data for 2016.

Average annual damage as percentage of GDP, 1995 to 2015

To calculate the amount of average annual damage as a percentage of annual GDP, the sum of damage that occurred throughout all disasters *d* in a given year *j* is multiplied by 100 and divided by the annual GDP for the year *j* for each country *i*. If for one year there are no disasters or no recorded damage, the value for that year will be 0. The final rate for the country over the period 1995-2015 will be the average of this calculated percentage:

$$Economic\ losses\ as\ \%\ of\ GDP\ for\ country_i = average\left(\frac{\sum_d X_{dij} \times 100}{GDP_{ij}}\right)$$

$$Where:$$

$$X_d = estimated\ economic\ damages[3]\ per\ disaster\ d$$

We assume that "missing" for the variable "total damage" corresponds to USD 0 damage. It is important to keep in mind that this methodology will largely underestimate the average losses due to the high percentage of missing values. The higher the percentage of missing values for one country the more the country average will be underestimated.

Table A.1 shows the number of missing values, the total number of observations and the percentage of missing values by country for the period 1995-2015.

Table A.2. Missing values for the variable "total damage" by country, 1995-2015

OECD countries	Missing values	Total observations	Percent missing
Australia	81	211	38.39
Austria	29	52	55.77
Belgium	44	64	68.75
Canada	92	136	67.65
Chile	70	104	67.31
Czech Republic	15	27	55.56
Denmark	12	20	60
Estonia	5	6	83.33
Finland	3	5	60
France	174	235	74.04
Germany	66	125	52.8
Greece	91	110	82.73
Hungary	26	40	65
Iceland	5	10	50
Ireland	16	26	61.54
Israel[4]	17	25	68
Italy	118	178	66.29
Japan	167	260	64.23
Korea	81	141	57.45
Latvia	7	9	77.78
Luxemburg	3	12	25
Mexico	268	345	77.68
Netherlands	23	47	48.94
New Zealand	35	62	56.45
Norway	18	23	78.26
Poland	54	69	78.26
Portugal	41	56	73.21
Slovak Republic	16	24	66.67
Slovenia	5	11	45.45
Spain	104	145	71.72
Sweden	9	15	60
Switzerland	31	61	50.82
Turkey	225	248	90.73
United Kingdom	78	134	58.21
United States	545	1 008	54.07
Non-members			
Colombia	197	219	89.95
Costa Rica	40	61	65.57

$GDP = GDP\ million\ at\ current\ prices\ and\ purchasing\ power\ parities\ (PPPs)$

The OECD average is the non-weighted arithmetic mean of the 35 OECD countries. It does not include data for non-member countries.

Notes

[1] Population data from OECD statistics for most countries are until year 2013. We complete them with World Bank population data for years 2014 and 2015.

[2] Gross domestic product estimates according to the *OECD National Accounts* database: www.oecd.org/std/na/.

[3] The amount of damage to property, crops and livestock. The value of estimated damage is given in USD ('000). For each disaster, the registered figure corresponds to the damage value at the moment of the event, i.e. the figures are shown true to the year of the event.

[4] The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Annex B. Recommendation of the Council on the Governance of Critical Risks

The Council

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35], the Recommendation of the Council concerning Guidelines on Earthquake Safety in Schools [C(2005)24], the Recommendation of the Council concerning Chemical Accident Prevention, Preparedness and Response [C(88)85(Final)], the Recommendation of the Council on Good Practices for Mitigating and Financing Catastrophic Risks [C(2010)143/REV1], the Recommendation of the Council on Regulatory Policy and Governance [C(2012)37], and the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security [C(2002)131/FINAL];

RECOGNISING that effective risk governance is a means of maintaining or achieving national competitive advantage against a backdrop of numerous geopolitical, environmental, societal and economic uncertainties as it represents an opportunity to invest in safer and better lives for the future;

RECOGNISING that critical risks may develop quickly and through unforeseen pathways to spread across borders, resulting in adverse impacts of national significance, disrupting vital infrastructure sectors, degrading key environmental assets, negatively impacting public finances and eroding public trust in government;

RECOGNISING that citizens and businesses expect governments to be prepared for a wide range of possible crises and global shocks and to handle them effectively should they arise;

RECOGNISING that broad-based partnerships that leverage skills, knowledge energy and flexible capabilities are needed to meet the challenges posed by critical risks, and that international cooperation fosters enhanced anticipation and preparedness capacities;

NOTING that the OECD plays a leading role in helping countries to share good practices in governance across the risk management policy cycle, and that this work has been welcomed by international forums, such as the G20 Finance Ministers and Central Bank Governors;

NOTING that the OECD identified an Agenda for Action for emerging risks in the 21st century in the early 2000s, that the report ‘Future Global Shocks’ took this Agenda for Action a step further by focusing on the policy challenges to contend with unlikely or unforeseeable disruptive events of high magnitude, and that since 2011 the High Level Risk Forum of the Public Governance Committee has provided a platform for government officials, private sector risk managers, think tanks and civil society to exchange policy practices and raise awareness;

NOTING that during the meeting of the Council at Ministerial level on 29-30 May 2013, Ministers considered the importance for governments to improve their ability to anticipate and manage complex policy challenges that pose a potential threat to the well-being of citizens and businesses, which includes identifying and managing risks, planning for long-term change and dealing with multi-sectoral issues [C/MIN(2013)4/FINAL];

On the proposal of the Public Governance Committee:

I. AGREES that, for the purpose of the present Recommendation, the following definitions are used:

- "Critical risks": threats and hazards that pose the most strategically significant risk, as a result of (i) their probability or likelihood and of (ii) the national significance of their disruptive consequences, including sudden onset events (e.g. earthquakes, industrial accidents, terrorist attacks), gradual onset events (e.g. pandemics), and steady-state risks (notably those related to illicit trade or organised crime);
- "Core capability": human and technical means to accomplish a mission, function or objective that is necessary to achieve national preparedness and resilience goals;
- "Hazard": a natural or man-made source or cause of harm or difficulty;
- "National risk assessment": a product or process that collects information and assigns a value to risks at a strategic, national level for the purpose of informing priorities, developing or comparing courses of action, and informing decision making;
- "Risk assessment": a methodology to determine the nature and extent of risk by analysing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and their environment;
- "Resilience": ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions;
- "Sense making": a crisis management capacity that aims to understand the nature of an emerging crisis situation, its magnitude and impacts, its potential to evolve, the core societal values under threat and to clarify any associated uncertainties;
- "Structural measures": engineering or civil work prevention measures aimed at reducing exposure to hazards by protecting assets or communities, or controlling the variability of natural phenomena (e.g. dams or dykes for floods or storm surges, grids for rock falls, barriers for avalanches, anti-bomb walls or concrete blocks for terrorist attacks);
- "Non-structural measures": measures focused on the reduction of exposure and vulnerability through longer term planning and adaptation to hazard patterns and threats (e.g. raising public awareness, emergency preparedness and early warning systems, land use prescriptions, urban planning, building codes or the restoration of natural functions of ecosystems to buffer extreme hazards);
- "Transboundary (impacts)": spill-over risk consequences that cross national borders, or migrate from one economic sector, administration or community to another, often with differentiated effects;
- "Third sector": entities for whom preparation response and/or recovery are core parts of their business, and non-governmental voluntary and other non-profit entities that have public well-being as part of their purpose;

- "Whole-of-society approach": the involvement of all stakeholders, from individuals to government entities, businesses, non-governmental organisations and the third sector.

II. RECOMMENDS that Members establish and promote a comprehensive, all-hazards and transboundary approach to country risk governance to serve as the foundation for enhancing national resilience and responsiveness.

To this effect, Members should:

1. Develop a national strategy for the governance of critical risks which would:
    i. identify and designate core capabilities required to preserve public safety, sustainable economic growth, market integrity and the environment against the harmful impacts of critical risks;
    ii. clarify roles for the management of the full country portfolio of critical risks, and identify who is responsible for taking actions to protect citizens and assets;
    iii. adopt an all-hazards approach that identifies inter-dependencies between critical systems;
    iv. set goals for each phase of the risk management cycle, defining priorities for prevention, mitigation, response, recovery and rehabilitation, and ensure that these priorities are integrated into the policies and programmes of departments and agencies.
2. Assign leadership at the national level to drive policy implementation, connect policy agendas and align competing priorities across ministries and between central and local government through the establishment of:
    i. multidisciplinary, interagency-approaches (e.g. national coordination platforms) that foster the integration of public safety across ministries and levels of government and ensure cooperation between governmental and non-governmental entities;
    ii. platforms to identify inter-linkages that underlie critical risks (e.g. expert discussions, mutual trust building, information sharing, risk assessment workshops);
    iii. desired levels of preparedness consistent with the national strategy, ensuring the availability of and continuously investing in the strengthening of the capabilities needed to ensure resilience nationwide.
3. Engage all government actors at national and sub-national levels, to coordinate a range of stakeholders in inclusive policy making processes which would:
    i. support citizen engagement and invite communities, businesses, individuals and households to take greater responsibility for their own safety;
    ii. develop a shared vision of critical risks and the division of responsibilities for shouldering the management burden;
    iii. foster a whole-of-society approach to clarify accountability and achieve better outcomes with more resilient communities.
4. Establish partnerships with the private sector to achieve responsiveness and shared responsibilities aligned with the national strategy by:
    i. identifying shared interests and common goals across public and private sectors in the governance and management of critical risks;
    ii. creating models for public-private partnerships (PPPs) to develop trusted information sharing networks that help identify where disruptions to

critical infrastructure and supply chains could lead to knock-on effects across borders, and cascading effects;

iii. taking advantage of private sector capability and expertise to develop new technologies, build resilient infrastructure and deliver financial mechanisms.

III. RECOMMENDS that Members build preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impacts.

To this effect, Members should:

1. Develop risk anticipation capacity linked directly to decision making through:
    i. the development of capacity for horizon scanning, risk assessment and early warning with a view to ensuring that the results feed directly into timely decision making;
    ii. the identification of critical hazards and threats so as to assess them using the best available evidence, investing in new research and tools where required, setting aside the necessary resources. Risks should be understood in terms of their potential likelihood, plausibility and impacts;
    iii. the adoption of all-hazards approaches to national risk assessment to help prioritise disaster risk reduction, emergency management capabilities and the design of financial protection strategies;
    iv. the revision of their national risk assessment periodically in the light of recent events, shifting priorities, and new information. This process should include the investigation and the assessment of damages and losses derived from disasters as soon as possible after they occur. The national risk assessment should help analyse the drivers behind exposures and the vulnerability of populations, assets and activities that can give rise to critical risks;
    v. the development of location-based inventories of exposed populations and assets, as well as infrastructures that reduce exposure and vulnerability. The assessment process should also consider identifying inter-linkages between different types of critical risks and the possible sequencing of hazardous events and cascading effects, which require cross-sectoral and even international cooperation.
2. Equip departments and agencies with the capacity to anticipate and manage human induced threats through:
    i. the development of capabilities needed to provide citizens and businesses with a safe environment for the normal functioning of society, and to safeguard economic and social life.
    ii. the acquisition of tools to assess and manage such threats, to map the activities of actors in the illegal economy and enable a fuller understanding of the connections between different forms of illicit activities, in order to increase economic and societal resilience to transnational criminal and terrorist networks.
    iii. the mapping of illicit activities and other analyses to help compare the level of national risk posed by these types of threats with that posed by naturally-occurring hazards and gradual onset conditions.
    iv. the development and operation of reliable intelligence networks and other detection mechanisms to identify and assess the threat of terrorist attacks and other major criminal activities.
3. Monitor and strengthen core risk management capacities through:

i. the allocation of resources to develop and maintain the capabilities at all levels of government that are needed throughout the risk management cycle;
ii. assistance for the development and continued training of specialised services (e.g. to conduct risk assessments, hazard mapping and real-time monitoring, but also law enforcement, security and rescue services) and the provision of modern and interoperable equipment;
iii. the implementation of efficient inspection systems, supplemented by the power to impose and implement sanctions, to ensure that minimum standards are adhered to for civil protection services in local levels of government.

4. Plan for contingent liabilities within clear public finance frameworks by enhancing efforts to minimise the impact that critical risks may have on public finances and the fiscal position of a country in order to support greater resilience. This could be done by:
    i. developing rules for compensating losses that are clearly spelled out at all levels in advance of emergencies to the extent that this is feasible to achieve cost effective compensation mechanisms;
    ii. taking into account the distribution of potential losses among households, businesses and insurers, and encourage policies whereby all actors take responsibility within the context of their resources. In countries or areas that are known to be highly exposed or vulnerable to extreme events, cost-effective compensation should consider a mix of pre-funding mechanisms and clear and agreed public finance rules before a crisis occurs. The mix of mechanisms should include market-based mechanisms that enable households and businesses to transfer financial risks to insurance and capital markets;
    iii. establishing mechanisms for estimating, accounting and disclosing contingent liabilities associated with losses to critical sectors in the context of national budgets;
    iv. adopting broad frameworks for assessing risk-related expenditures. These frameworks should record, to the extent that this is feasible, the expenses at national and local level.

IV. RECOMMENDS that Members raise awareness of critical risks to mobilise households, businesses and international stakeholders and foster investment in risk prevention and mitigation.

To this effect, Members should:

1. Encourage a whole-of-society approach to risk communication and facilitate transboundary co-operation using risk registries, media and other public communications on critical risks through:
    i. a two-way communication between government and stakeholders, ensuring that information sources are accurate and trusted, and the information is made accessible in a manner appropriate to diverse communities, sectors, industries and with international actors;
    ii. the combination of targeted communication with the provision of incentives and tools for individuals, businesses and non-governmental organisations to work together and take responsibility for investment in self-protective and resilience-building measures;
    iii. providing notice to households about different scales of hazards and human induced threats, and supporting informed debate on the need for prevention, mitigation and preparation measures;

iv. informing and educating the public in advance of a specific emergency about what measures to take when it occurs, and mobilising public education systems to promote a culture of resilience by integrating community resilience skills and concepts into curriculums and thereby pass information on to households through students.

2. Strengthen the mix of structural protection and non-structural measures to reduce critical risks through:
    i. the reinforcement of investment in prevention and mitigation efforts that limit the exposure of persons and core services to known hazards and reduce their vulnerability;
    ii. strategic planning to build safer and more sustainable communities, paying attention to the design of critical infrastructure networks (e.g. energy, transportation, telecommunications and information systems). This strategic planning should be coordinated with urban planning and territorial management policies to reduce the concentration of people and assets in areas where known exposures have increased over time;
    iii. robust surveillance, monitoring and alert networks should be used to reduce critical risks associated with malicious attacks and threats to public health;
    iv. the development of fiscal and regulatory options to promote reserve capacity, diversification or back-up systems to reduce the risk of breakdowns and prolonged periods of disruption in critical infrastructure systems;
    v. the incorporation of risk management decisions, safety and security standards in national and local regulations for land use, building codes and the design, development and operations of critical infrastructure;
    vi. the use of cost/benefit analyses conducted to maximise the cost-effectiveness of public and private investments that reduce the exposure of housing and commercial facilities.
3. Encourage businesses to take steps to ensure business continuity, with a specific focus on critical infrastructure operators by:
    i. developing standards and toolkits designed to manage risks to operations or the delivery of core services;
    ii. ensuring that critical infrastructure, information systems and networks still function in the aftermath of a shock;
    iii. requiring first responders stationed in critical infrastructure facilities to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable; encouraging small community-based businesses to take proportionate business resilience measures.

V. RECOMMENDS that Members develop adaptive capacity in crisis management by coordinating resources across government, its agencies and broader networks to support timely decision-making, communication and emergency responses.

To this effect, Members should:

1. Establish strategic crisis management capacities to prepare for unknown and unexpected risks that provoke crises by:
    i. establishing and building upon a solid foundation of standard operating procedures, pre-defined emergency plans, conventional training and drills on a regular basis to contend with known hazards and threats;
    ii. complementing these core capacities with flexible resources that bolster resilience, enabling reaction to novel, unforeseen and complex events;

iii. facilitating the sharing of multi-disciplinary expertise to make sense of incomplete information before and during a crisis, as well as to prepare and respond to crises of an unexpected nature.

2. Strengthen crisis leadership, early detection and sense making capacity, and conduct exercises to support inter-agency and international co-operation by:
    i. strengthening government leadership before and during a crisis to drive transboundary cooperation and maintain public trust;
    ii. developing strategies, mechanisms and instruments for "sense making" to ensure reliable, trusted and coordinated expert advice translates into informed decisions by national leaders;
    iii. preparing crisis cells that can be rapidly mobilised to identify options for action and minimise uncertainties;
    iv. iv) developing and funding early warning systems to monitor hazards and threats;
    v. nurturing international cooperation opportunities and joint training with international stakeholders/actors to develop a range of crisis preparedness capacities (e.g. global risk monitoring systems and early warning systems) and crisis response capacities (e.g. shared "sense making", the coordination of strategic crisis management structures, the interoperability of emergency forces, the mobilisation of specialised teams, tools and supplies at transnational levels, and harmonised crisis communication processes).
3. Establish the competence and capacities to scale up emergency response capabilities to contend with crises that result from critical risks, in particular through:
    i. the designation of an authority in charge of drawing on and coordinating sufficient resources to manage civil contingencies, whether from departments and agencies, the private sector, academia, the voluntary sector or non-governmental organisations;
    ii. the interoperability of equipment, clear quality standards, regular training and multi-stakeholder drills to support efficient civil protection capabilities;
    iii. the promotion of incentives for businesses and individuals to support local voluntary organisations that reinforce professional first responder capacities;
    iv. support for the recruitment, retention, training, equipping and maintenance of paid and unpaid personnel in all aspects of civil protection to strengthen national capacity to respond to and recover from contingencies and for the effective management and employment, including the encouragement of spontaneous volunteers where appropriate.
4. Build institutional capacity to design and oversee recovery and reconstruction plans by:
    i. seizing economic opportunities, reducing vulnerability to future events and strengthening long term resilience with a view to balance short-term fixes and long term investments in sustainability.
    ii. establishing multi-stakeholder governance arrangements that facilitate agile implementation, the efficient use of public funds and transparent disbursements to protect undue influence and corruption.

VI. RECOMMENDS that Members demonstrate transparency and accountability in risk-related decision making by incorporating good governance practices and continuously learning from experience and science.

To this effect, Members should:

1. Ensure transparency regarding the information used to ensure risk management decisions are better accepted by stakeholders to facilitate policy implementation and limit reputational damage by:
    i. fostering honest and realistic dialogue between stakeholders about the nature and likelihood/ plausibility of hazards and threats, as well as the potential impacts and the cost-effectiveness of various mitigation, response and recovery options;
    ii. providing public access to risk information and measures to validate the integrity of the risk management decision making process;
    iii. encouraging openness about assumptions behind analyses and an opportunity to evaluate the drivers of uncertainty. Although circumstances may require restricted access to sensitive or classified information, the processes and methodologies used for management of critical risks should be shared even if certain types of intelligence is not.
2. Enhance government capacity to make the most of resources dedicated to public safety, national security, preparedness and resilience by:
    i. strengthening the ability of government, in conjunction with third sector and private sector entities, to make explicit trade-off and prioritisation decisions informed by the full country portfolio of critical risks;
    ii. adopting strong frameworks for implementation that provide incentives to conduct risk analysis, ensure the results are made available to decision makers, and develop review mechanisms to monitor implementation.
3. Continuously share knowledge, including lessons learned from previous events, research and science through post-event reviews, to evaluate the effectiveness of prevention and preparedness activities, as well as response and recovery operations by:
    i. incorporating the findings from events and research into improved preparedness and resilience planning, guarding against unintended adverse impacts, such as the creation of additional risks or the failure to recognise changes in risk characteristics;
    ii. identifying the lessons learned for policy makers as a first step in a process that includes adapting critical systems, recurrent monitoring of capability levels, evaluating the performance of response and recovery actions, and undertaking peer reviews to share insights across countries;
    iii. organising briefings for stakeholders (e.g. the media, the third sector, academics, business associations).

VI. INVITES the Secretary-General to disseminate this Recommendation.

VII. INVITES Members to disseminate this Recommendation at all levels of government.

VIII. INVITES non-Members to take account of and adhere to this Recommendation.

IX. INSTRUCTS the Public Governance Committee to monitor the implementation of this Recommendation and to report thereon to the Council no later than three years following its adoption and regularly thereafter, in consultation with other relevant OECD Committees.

References

Almannavarnir (2017), La Protection Civile en Islande, www.almannavarnir.is/france/
Cabinet Office (2016), White Paper on Disaster Management 2016, www.bousai.go.jp/kyoiku/panf/pdf/WP2016_DM_Full_Version.pdf
Comisión Nacional de Emergencias (CNE) (2017), Inicio, https://www.cne.go.cr/
Criminal Intelligence Service Canada (2014), Organized Crime in Canada – Backgrounder, www.cisc.gc.ca/media/2014/2014-08-22-eng.htm
Danish Emergency Management Agency (DEMA) (2017), Emergency management, http://brs.dk/eng/emergency_management/Pages/emergency_management.aspx
Departamento de Seguridad Nacional (DNS) (2017), El Sistema de Seguridad Nacional, www.dsn.gob.es/es/sistema-seguridad-nacional
Department of Homeland Security (2017), Disasters, https://www.dhs.gov/topic/disasters
Department of the Prime Minister and Cabinet (2017), Ministry of Civil Defence & Emergency Management (MCDEM), https://www.dpmc.govt.nz/our-business-units/ministry-civil-defence-emergency-management
Disaster and Emergency Management Authority (AFAD) (2017), About us, https://www.afad.gov.tr/en/2572/About-Us
EM-DAT: The CRED/OFDA International Disaster Database – Université Catholique de Louvain – Brussels – Belgium (2016) [Data file]. Retrieved from: www.emdat.be
Estonian Ministry of the Interior (2017), Crisis Management, HTTPS://WWW.SISEMINISTEERIUM.EE/EN/ACTIVITIES/CRISIS-MANAGEMENT
EUROPOL (2017), SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA), https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2
Federal Office of Civil Protection and Disaster Assistance (BBK) (2017), Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/DE/DasBBK/UeberdasBBK/ueberdasbbk_node.html
Global Water Partnership Central and Eastern Europe (2016), Integrated Drought Management Programme, www.gwp.org/globalassets/global/gwp-cee_files/idmp-cee/idmp-act.5.4-report-1.2.pdf
Government of Australia – Attorney-General's Department (2017), Emergency management, https://www.ag.gov.au/EmergencyManagement/Pages/default.aspx
Government of Australia (2017), Natural disasters in Australia, www.australia.gov.au/about-australia/australian-story/natural-disasters
Haut-Commissariat à la protection nationale (HCPN) (2017), Organisation, www.gouvernement.lu/5509104/organisation
Italian Civil Protection Department (2017), Civil Protection Department, www.protezionecivile.gov.it/jcms/en/dipartimento.wp
Ministry of Interior of the Slovak Republic (2017), About Ministry of Interior, https://www.minv.sk/?ministry-of-interior
Ministry of the Interior and Safety (MOIS) (2017), About the Ministry, www.mois.go.kr/eng/sub/a02/aboutMinistry/screen.do
MSB – Swedish Civil Contingencies Agency (MSB) (2017), About MSB, https://www.msb.se/en/About-MSB/
National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Data file]. Retrieved from www.start.umd.edu/gtd
National Office of Emergency (ONEMI) (2017), ONEMI | Misión y Visión, www.onemi.cl/mision-y-vision/
Norwegian Directorate for Civil Protection (DSB) (2014), National Risk Analysis 2014, https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014_english.pdf

Norwegian Directorate for Civil Protection (DSB) (2017), DSB, https://www.dsb.no/en/
OECD (2006). Japan: Earthquakes, OECD Publishing, Paris
OECD (2010), Review of the Italian National Civil protection System, OECD Publishing, Paris
OECD (2014), Review of the Mexican National Civil Protection System, OECD Publishing, Paris
OECD (forthcoming), Harnessing innovation to reduce disaster risk in Austria, France and Switzerland, OECD Publishing, Paris, OECD Publishing, Paris
OECD (forthcoming), Risk Governance report
OECD Statistics (2017), http://data.oecd.org/
OECD Survey on the Governance of Critical Risks, 2016;
Public Safety Canada (2017)\, Natural Hazards of Canada, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/ntrl-hzrds/index-en.aspx
Security Committee (2017), What is the Security Committee?, https://turvallisuuskomitea.fi/index.php/en/
Slovenian Ministry of Defense (2017), Administration of the Republic of Slovenia for Civil Protection and Disaster , www.mo.gov.si/en/about_the_ministry/organization/administration_of_the_republic_of_slovenia_for_civil_protection_and_disaster_relief/
Swedish Civil Contingencies Agency (2012), Swedish National Risk Assessment 2012, https://www.msb.se/RibData/Filer/pdf/26621.pdf
Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD) (2017), Objetivos y Funciones de la Unidad Nacional para la Gestión del Riesgo de Desastres, http://portal.gestiondelriesgo.gov.co/Paginas/Objetivos.aspx
United Nations Office on Drugs and Crime (UNODC) (2017), Statistics, www.unodc.org/unodc/en/data-and-analysis/statistics.html
World Bank (2017), Population data, https://data.worldbank.org/indicator/SP.POP.TOTL