

Meeting of the OECD Council at Ministerial Level

Paris, 6-7 May 2014

RECOMMENDATION OF THE COUNCIL ON THE GOVERNANCE OF CRITICAL RISKS

Adopted on 6 May 2014

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;

- iv) 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) 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 policymakers 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).

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

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

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

X. 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.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

OECD WEEK 2014

www.oecd.org

OECD Paris
2, rue André-Pascal, 75775 Paris Cedex 16
Tel.: +33 (0) 1 45 24 82 00