






PEER REVIEW
POLAND
2016

Funded by
European Union
Civil Protection

PEER REVIEW

POLAND

2016

Programme for peer reviews in the framework of EU cooperation on civil protection and disaster risk management 2015-2016

Funded by
European Union
Civil Protection

Acknowledgements

The time and expertise dedicated by the peers were essential to the achievement of this report. The peer review team was composed of four peers:

- ***John Agius**, Critical Infrastructure Protection Directorate (CIPD), Cabinet Office, Office of the Prime Minister (OPM), Malta*
- ***Omar Harrami**, CIP and CIIP Section, Civil Contingencies Agency, Sweden*
- ***Lyubomira Raeva**, DG Fire Safety and Civil Protection, Ministry of Interior, Bulgaria*
- ***Çiğdem Tetik Bicer**, Disaster and Emergency Management Presidency, Prime Ministry, Turkey*

The European Commission was represented during the mission by Andrew Bower from DG Humanitarian Aid and Civil Protection. Laura Schmidt from DG Humanitarian Aid and Civil Protection provided guidance and support back in Brussels. A consortium led by Falck B.V. assisted the Commission in carrying out the peer review programme. The project team for Poland was formed by Nico van Os and Ruud Houdijk on behalf of consortium partner Safety Region South-Holland South and Jens Poul Madsen representing Falck. Jack Radish of the OECD also took part in the mission.

*The peer review benefited greatly from the contributions of all interviewed stakeholders and their cooperation in gathering the data and information for this project. It could not have been achieved without the full commitment of **Dorota Leduchowska** and **Beata Janowczyk** of the Polish Government Centre for Security.*

The peer review was financed by the European Commission, including through its financial contribution to the OECD High-Level Risk Forum.

Contents

Introduction

Peer review is a governance tool whereby the disaster risk management system of one country ('reviewed country') is examined by experts ('peers') from other countries. The EU programme for peer reviews in civil protection and disaster risk management was set up following two successful pilot peer reviews in the UK (2012) and Finland (2013), undertaken jointly with the Organisation for Economic Cooperation and Development (OECD) and the United Nations Office for Disaster Risk Reduction (UNISDR).

The EU peer review programme aims to facilitate the exchange of good practices and make recommendations for improving disaster management policy and operations in the reviewed countries. It encourages mutual learning and understanding and facilitates a policy dialogue both within and between countries, and among experts.

Poland informed the European Commission that it was interested in participating in a thematic peer review on **risk assessment**. It asked to be reviewed on its risk assessment capabilities in the light of the recent *EU risk management capabilities assessment guidelines*[1] and the Union's civil protection legislation (Article 6 of Decision No 1313/2013/EU).[2]

Review process

Following confirmation of Poland's participation in the thematic review on risk assessment, a call for nominations of experts was organised across countries participating in the EU Civil Protection Mechanism and eligible neighbouring countries. Four peers from Bulgaria, Malta, Sweden and Turkey participated in the review, supported by the Commission and a project team.

The peer review mission was conducted over a period of five days (25-29 January 2016).[3] Over 50 stakeholders were interviewed, from many different organisations, including central, regional and local governmental authorities and agencies, non-governmental organisations (NGOs) and academia.

Interviews took place at the following locations:

- Government Centre for Security (GCS);[4]
- City of Warsaw Municipal Office;
- National Atomic Energy Agency (PAA);
- National Headquarters of the State Fire Service;
- Main School of the Fire Service;
- Polish Transmission System Operator (PSE S.A.);
- Mazovian Voivodeship;
- City of Płock municipal office;
- Institute of Meteorology and Water Management — National Research Institute;
- National Water Management Authority (NWMA).

1 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015XC0808(01)
2 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0924:0947:EN:PDF
3 The report sets out the findings of the peer analysis of the situation in Poland in January 2016 — any more recent developments are not taken into consideration.
4 In Polish: *Rządowe Centrum Bezpieczeństwa* (RCB).

There were field trips to a landslide-prone area on the bank of the River Vistula in the city of Płock, the Płock municipal crisis management centre and the Polish oil concern PKN ORLEN (also in Płock).

By bringing together stakeholders with a variety of backgrounds, expertise and responsibilities, the peer review sessions helped to facilitate the sharing of risk assessment knowledge and foster cooperation between risk assessment stakeholders across all levels of governance.

Scope of the review

The review focuses on risk assessment capabilities in Poland and broadly follows the Commission's *EU risk management capabilities assessment guidelines*. During the review, peers focused on the policy and governance context, and the methodological approaches and cross-sectoral scope of risk assessment in Poland. Special attention was given to risk assessment capabilities in the light of Poland's main risks and the expertise of the authorities interviewed, covering a range of policy areas, including critical infrastructure protection (CIP), climate-change adaptation (CCA), flooding, extreme weather events and landslide risks.[5]

This report identifies good practices and areas for improvement and proposes a series of recommendations across the various objectives. It is up to the Polish Government and stakeholders to consider how these could best contribute to achieving their objective of a resilient society and a sustainable national policy dialogue.

Several of the main national risk assessment (NRA) and CIP documents are classified due to their sensitive content. As a result, the peer review mission based its conclusions in large part on interviews and translated summaries of documents.

In this report, definitions from the EU risk assessment and mapping guidelines for disaster management6 are used (see Annex I). The concept of 'threat assessment', as used by Poland, refers to risk assessment. 'Fragmentary reports' are sectoral and provincial risk assessment reports, which form the basis of the Report on Threats to National Security (RTNS).

[5] The peer review mission took an 'all-hazards' approach, but some specific risks were discussed in more detail.

[6] https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Key findings and recommendations

The Polish capabilities for risk assessment include a number of good practices:

- Poland has a strong framework, coordination and cooperation. The fragmentary reports mechanism helps to identify the principal risks and related impacts and ensures that different entities are involved in the risk assessment process. The two-way risk-assessment process, from local, to provincial, to NRA is conducive to the required cooperation across all levels. One main organisation (GCS) is in charge of coordinating the NRA process and thus has a general appreciation of the threats identified at national level. The private sector, academia and NGOs are involved in the risk assessment process.
- Poland has developed its own methodology for NRA, which is in conformity with EU standards. The GCS adjusts the risk assessment at national level and gives recommendations at appropriate sub-national level.
- Poland has high-quality data and uses scientific data and analysis for NRA purposes, as well as specific tailor-made software for the NRA.
- The GCS has a designated website providing information to the general public, with special manuals that give advice on how to behave in emergency situations.
- Flood-risk maps are available online and there is a flood-risk education programme.
- Poland has good expertise for risk assessment. The Main School of the Fire Service offers several study programmes; there is an adequate level of knowledge among individual stakeholders; specialist staff are employed at all levels of the administration and there is an e-learning programme to improve professionals' knowledge.
- Links are being made with risk management. A very clear division of responsibilities and risk ownership (for all four phases of crisis management) is in place. There is a direct link between plans at local/regional/provincial and national levels.
- An 'all-hazard' approach to CIP is in place. The NCIPP closely reflects the principles of shared responsibility, cooperation and trust. CIP includes business continuity planning.
- Poland promotes citizens' active participation in climate change adaptation issues.

The following high-level recommendations were identified and will be presented in more detail throughout this report:

- Ensure a clear relationship between the NRA and all four phases of crisis management.
- Encourage risk assessment at local level in order to support the work and planning of autonomous governments.
- Make use of the strong two-way process to coordinate a nationwide structure of coherent prevention strategies at all levels.

- To improve stakeholder consultation:
    - Improve inter-sectoral cooperation and coordination by organising joint meetings (classified workshops).
    - Broaden dialogue with neighbouring countries on international and cross-border cooperation.
    - Make more use of the knowledge and expertise of the private sector.
    - Consider involving CCA stakeholders more actively in the NRA process.
- Implement the ARMOR software to support the process of risk assessment and the corresponding adjustments in the assessment method in a structured manner.
- Continue developing the Polish risk assessment methodology on the basis of evaluations and feedback from Polish stakeholders. Stimulate the use of the common overall risk assessment methodology at all levels to ensure that risks that are not of national concern are also monitored. Make clear what the interlinkages are between the NRA methodology and several sectoral methods.
- Actively engage with the JRC to compare the Polish methodology with other Member States'.
- Develop a common standard on data used for risk assessment and . investigate the possibility of implementing multi-hazard risk-mapping based on standards for data exchange and GIS.
- Develop, on the basis of the NRA, a general risk communication strategy. The GCS should have the central coordination role in the strategy, ensuring its coherence and the consistency of the information. Improve the sharing of information on sensitive CIP issues and develop a general CCA communication strategy.
- Strengthen expertise through:
    - organising experience-sharing between professionals working with the national methodology for risk assessment.
    - Investigating the possibility for the GCS and Main School for the Fire Service to develop a shared systematic strategy (with concrete objectives) for further development of administrative capacity.
    - Promoting an interdisciplinary academic dialogue on risk-assessment methodologies in different sectors.
    - Developing a national strategy to coordinate research and development for risk assessment and risk management.
- Work on clear funding procedures. Develop a policy for allocating financial resources for risk assessments at all government and sectoral levels. All funding for prevention, preparedness, response and recovery should be 'risk-informed'. The continuity of important prevention- and monitoring-related projects funded under EU programmes or from other sources has to be ensured.

- Invest in the link of risk assessment with risk management. A national DRR strategy should be developed in accordance with the Sendai Framework. Recommendations from the RTNS should be included in the DRR action plans. Consider providing one body with enough power and competences to coordinate the DRR strategy, in close connection with the NRA. Provide municipalities with technical support to develop mitigation programmes.
- Ensure that the NCIPP is not solely directed at individual CIs, operators or installations, but at complete CI systems and their interdependencies. Review the mix of incentives for CIP. Distinguish between CI forum gatherings, workshops and conferences.
- Create a more direct link between the NRA and CCA strategies. Assign a clear overall priority to all climate change related short- and long-term effects from the perspective of national security and safety.

1. Framework, coordination and stakeholder involvement

1.1 Framework

Objective: risk assessments are carried out on the basis of a clear legal and/or procedural framework and the role of risk assessments in overall disaster risk management is defined at the appropriate national and/or sub-national level.

Poland's main law on risk assessment is the **Act on Crisis Management** (26 April 2007). Polish legislation defines 'crisis management' as a comprehensive process incorporating risk prevention, preparedness, response and recovery. The risk assessment process is considered *inter alia* as part of the prevention phase, informing the other phases along the way. The Act describes the planning cycle for crisis management as 'periodic implementation of the phases of analysis, programming, the development of the plan or programme, its implementation, testing and initiation'. However, the Government Centre for Security (GCS) acknowledges that the definitions in the Act will have to be aligned with those used in the *EU Civil Protection Mechanism guidelines*.

The Act on Crisis Management requires the production of a **National Crisis Management Plan (NCMP)**, designed for events where central government response is required, because regional actors are not able to act efficiently or there is a lack of capabilities and resources at regional level. These are specific national events resulting from the 20 identified threats.

The Act also governs the assessment of threats and risks. For the purposes of the NCMP, ministers in charge of the government branches, the heads of central offices and the voivodes[7] have a legal obligation to contribute to a **Report on Threats to National Security (RTNS)**, by means of **fragmentary reports**. The Director of the GCS has to ensure the overall coordination of the preparation of the RTNS, while the Head of the Internal Security Agency is responsible for the coordination and preparation of the part relating to terrorist threats. As some information may be regarded as classified for security reasons, the RTNS is restricted (lowest level of classification).

A regulation on the RTNS (30 April 2010) specifies the procedure and deadlines for its production. The report has to answer the following questions:

Diagram 1: Questions in report

[7] The voivode is the head of the voivodeship or province (first country division level).

The regulation defines the types of national security threat as follows:

a) those having a major influence on the nation's functioning and possibilities of development, in particular threats of primary importance to security, international position and economic and defence capacity;
b) those of which the effects can:
   - harm national security, constitutional order and in particular the sovereignty, independence and inviolability of the territory;
   - pose a threat to a considerable number of people's lives, health, property or environment over a sizeable area;
   - also affect other nations; and
   - relate to Polish territory or citizens, even though they might occur in another country;
c) those occurring in areas of tension, conflict and international crisis and influencing the security of the nation or that require the monitoring or elimination of results from signed contracts and international treaties; and
d) terrorist threats that could lead to a crisis situation.

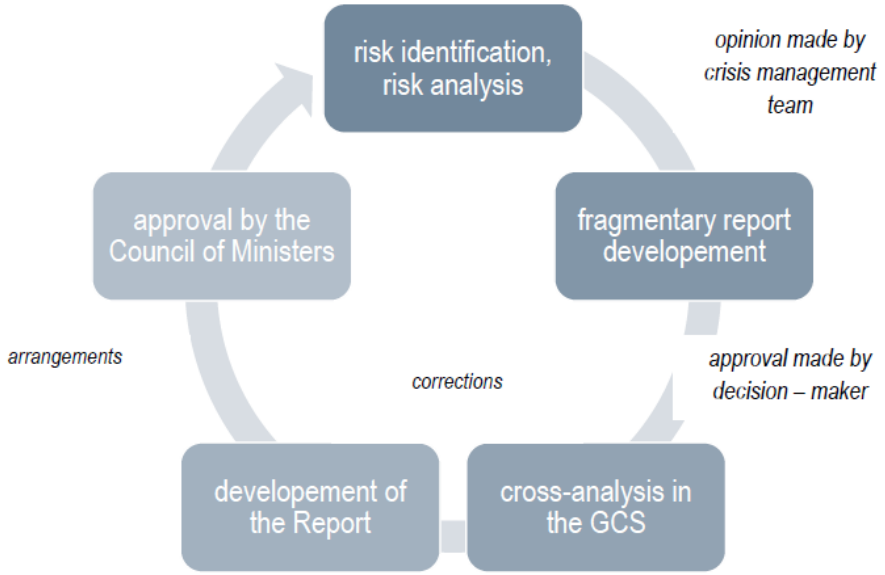


Diagram 2: risk assessment process

Risk assessment is a two-way process. First, risk assessments are shared from *gminas* (municipalities) and *poviats* (counties) to voivodeships (provinces), and second, from voivodeships to central government, with the GCS acting as the central coordinating agency. For the purposes of civil protection and security, the 16 voivodeships are responsible for policy in their geographical area. They are required to develop a fragmentary report for their area, on which the GCS provides feedback. These reports are eventually integrated into the RTNS. Lower-level entities usually follow the GCS guidelines.

Voivodeships in turn take account of assessments at *poviat* and *gmina* level. Local stakeholders carry out their own assessments, but risk assessment at local level has a weaker legal base. The Act is not explicit on assessment at local (*poviat*, *gmina*) levels. Local crisis management plans are subject to national supervision and

evaluation. There is a general risk assessment recommendation for self-governing entities to address probability, effect, scale and impact. In general, entities at the lower level of government assess a wider range of risk scenarios.

Although the RTNS outlines the 'strategic objectives' for risk management, the direct legislative link between the NRA and the NCMP gives the impression of a focus on preparedness rather than prevention (see also chapter 6).

In conclusion, it can be said that the process for conducting an NRA is clear and functions well. The legal framework is also well developed.

Good practice:

- The fragmentary reports mechanism helps to identify the principal risks and related impacts and ensures that different entities are involved in the risk assessment process. As a result, the RTNS makes it possible to cover the views of a wide spectrum of society (an 'all-hazard' risk-management approach).
- The two-way risk-assessment process, from local, to provincial, to NRA (and the feedback loop from national to provincial level) is conducive to the required cooperation across all levels. Uniformity and close coordination are evident at the crisis management planning stages. The process also creates a basis for the coordination of prevention strategies. However, there is room for improved cooperation (see recommendations).

Recommendations:

- Ensure a clear relationship between the NRA and all four phases of crisis management (i.e. prevention, preparedness, response and recovery) in the national framework and in the legislation.
- In order to support the work and planning of autonomous governments (crisis management planning, disaster risk reduction (DRR), land-use planning), risk assessment at local level should be encouraged, by a legal obligation (for *poviats*) and/or by means of more central government support for local-level assessments and plans, to ensure uniformity in approach and methodology.
- Make use of the strong two-way process and feedback loop to coordinate a nationwide structure of coherent prevention strategies at all levels.
- Adapt the Polish legal terminology to the relevant EU legislation.

1.2 Coordination

Objective: there are clearly defined responsibilities and roles/functions assigned to the relevant entities participating in the risk assessment.

The Act on Crisis Management sets out the responsibilities of all four government levels, the general principles for crisis management and the rules on financing crisis management tasks. At the highest level, the Council of Ministers is responsible for crisis management. In the event of a crisis, a Government Crisis Management Team (GCMT) is set up under the Council of Ministers, with the Prime Minister acting as

chairman. The GCMT is supported by the GCS, which is established in the form of a state budget unit under the Prime Minister and also serves as a national centre for crisis management. Its Director is appointed by the Prime Minister and acts as secretary of the GCMT.

For each of the 20 national threats, lead and support responsibilities for the four phases are clearly defined in a security matrix as part of the NCMP. The division of responsibilities for each risk is available at national and regional/local levels. This is based on an analysis of the RTNS, followed by legal acts or context analysis resulting in a proposal designating lead and support entities. However, the security matrix does not reflect co-owned and shared risks to be addressed in a multi-hazard 'whole of government' approach taking into account cascade effects and long-term consequences. If an emerging risk is not 'owned' by a specific sector, the GCS proposes to the Council of Ministers that it be assigned to a particular 'owner'. The objective is to ensure that every risk is owned by a leading stakeholder; that stakeholder is identified as the owner and is made accountable for the risk. This is different in the case of risk prevention and crisis management. The owner of the risk is noted in the 'risk register'.

The GCS coordinates:

1. the preparation of methodology and procedure for drawing up fragmentary reports,[8] so as to have a uniform methodology for all involved entities;
2. the organisation of relevant training, so as to present risk assessment methodology to, and raise awareness among, crisis management experts;
3. the drafting and editing of the RTNS; and
4. consultation of all involved entities during the legislative process and preparation of the relevant resolution of the Council of Ministers.

The GCS is a central coordinating entity. It cooperates with and coordinates all relevant public entities. The expertise to perform specific risk assessments lies with the respective stakeholders rather than with the GCS, which provides the necessary guidelines for the preparation of the fragmentary reports and checks drafts for inconsistencies and errors. All ministries, relevant national public entities and provinces are involved in the process. All stakeholders recognise the coordinating role of the GCS in the preparation of the RTNS.

Ministries and national agencies are responsible for developing fragmentary reports[9] for the areas under their competence. To date, 40 such reports have been developed. In addition, the Internal Security Agency has compiled two fragmentary reports:

- a standard fragmentary report, similar to other ministries'/agencies' reports and focusing on malicious human activities (sabotage, bribery, espionage, etc.); and
- a second report forming an integral part of the RTNS and dealing with matters relating to terrorist acts that may lead to situations of national crisis. In this regard, the Agency's role is to compile the fragmentary reports of ministries,

[8] See introduction for comments on the use of terminology.
[9] Understood here as sector-specific reports.

heads of central offices and voivodeships that focus on terrorist threats and other related information.

The GCS does not assess all risks itself, but relies on the assessment of the stakeholders involved, who are themselves responsible for identifying and assessing 'their' risks. The GCS's role is to combine the fragmentary reports in a comprehensive RTNS.

Diagram 3: Fragmentary reports

The GCS also cross-analyses the fragmentary reports to identify cross-sectoral issues. The Director of the GCS provides feedback on the degree of detail, scope and form of the fragmentary reports and recommends updates where appropriate. Where the GCS identifies a need, it recommends coordination between authorities and reports are updated on the basis of the feedback gathered from/by the various authorities and stakeholders.

Once finalised by the GCS, the draft RTNS is sent to the ministries and the heads of central offices and voivodeships, whose comments are taken on board or, if not, an explanation is given. Following any corrections and amendments, drafts of the report and of an appropriate regulation are submitted to the Council of Ministers. The RTNS is eventually approved by Council resolution, thus ensuring a high level of accountability for decisions on risk acceptance. Once it has been approved, the GCS sends the RTNS to the entities involved in the process.

The entities responsible for the fragmentary reports (where relevant) also take into account the transnational aspect of their risks. Poland has agreements with all neighbouring states, as well as Hungary, Croatia and Slovenia, on cooperation and mutual assistance in the event of disaster. It has implemented the UNECE Convention on the transboundary effects of industrial accidents. Furthermore, there is an international commission on protecting the Oder River against pollution, a multi-national flagship project under the EU's strategy for the Baltic Sea region (*From GAPS to CAPS 2015-2016*) and the BaltPrevResilience project.

Good practice:

- The tasks of all public entities with a role in the crisis management system, from local to central government level, are enshrined in legislation (Act on Crisis Management).
- The security matrix assigns responsibilities for each phase and risk. This creates a clear picture for all stakeholders. The GCS designates 'risk owners' as appropriate where risk ownership is not clearly defined.
- One main organisation (GCS) is in charge of coordinating the NRA process and thus has a general appreciation of the threats identified at national level. In addition, it provides risk assessment support to line ministries, central offices and voivodeships.
- The GCS's cross-analysis of the fragmentary reports as part of the feedback loop helps to bring together different sectoral perspectives. This represents a strong basis for the further improvement of cross-sectoral cooperation and coordination (see recommendations).
- The adoption of the NRA by Council resolution gives the right status to the final outcome and further strengthens the acceptability of the identified risks at political decision-making level.
- Poland cooperates with neighbouring countries and takes into account potential cross-border effects of scenarios (on both sides).

Recommendations:

- Improve inter-sectoral cooperation and coordination by organising joint meetings (classified workshops) where stakeholders from different sectors can engage in cross-sectoral analysis of correlations and interdependencies between fragmentary reports. This type of dialogue and shared cross-assessment could improve the feedback loop in order better to complement the fragmentary reports, help identify interdependencies and limited resources, and better underpin estimates and assessments. Such a joint assessment also furthers understanding of the distribution of responsibilities.
- Broaden dialogue with neighbouring countries on international and cross-border cooperation. This might include sharing information on national risk-assessment processes and methodologies (especially for natural and technical, non-malicious hazards), data-sharing on cross-border hazards and vulnerabilities, and the exchange of knowledge and experiences on NRA. Consider also initiating concrete risk-assessment, prevention and preparedness projects for cross-border risks for certain border areas, with both national and local governments.[10]

[10] Taking into account *inter alia* the UNECE Convention on transboundary effects of industrial accidents (http://www.unece.org/env/teia.html) and the Convention on the protection and use of transboundary watercourses and international lakes (http://www.unece.org/env/water).

1.3 Involvement of other stakeholders

Objectives: entities carrying out risk assessments cooperate with a range of stakeholders, including from the private sector, academia and other government entities not directly involved in the assessment process.

The fragmentary reports are the principal source of information for the national risk-assessment process. This is where brain-storming and scenario development is carried out and the widest possible spectrum of experts is involved. In preparing fragmentary/sectoral reports, civil servants work together and coordinate with private-sector actors (e.g. critical infrastructure (CI) owners/operators), academics and NGOs. Experts, middle management and decision-makers, such as the crisis management teams (high-level advisory body), are also involved.

Recently, Poland has further developed its own specific risk-assessment methodology with a consortium made up of the Main School of the Fire Service, the Warsaw University of Technology, the Scientific and Research Centre for Fire Protection, the National Defence University and Medcore (an IT company).

CIP is a major area covered in the RTNS. There is a direct link between the NRA and CIP, as the National Critical Infrastructure Protection Programme (NCIPP) has by law to be based on the RTNS. On the other hand, the provincial lists of CIs are fed directly into the NRA.

At national level, each ministry is responsible for CI system integrity in the sectors for which it is competent. All CI owners/operators are obliged to cooperate with the government. CIP cooperation takes place at three levels – strategic, operational and management. At the *strategic* level, there are three forums: a national CIP forum, a systems CIP forum and regional CIP forums. At the *operational* level, a CIP mechanism is provided for information exchange, including an internet forum for non-classified information. At the *management* level, conferences are organised and newsletters and four handbooks (on explosions, biometry, the assessment of technical malfunctioning and guidelines on implementing CIP into CI crisis management plans) are published. Good practices and recommendations on CIP are set out in the annex to the NCIPP.

There are various working groups, including one on IT protection standards. Poland is still in the process of exploring how to use the CI forums more effectively. The GCS invests a lot of effort in helping entities use them effectively. In the past, forums were used to organise conferences for the various stakeholders. The regional and ministerial forums are currently regarded as less useful.

CIs are also covered at the risk identification and analysis stages of preliminary flood-risk assessment, for which the NWMA is responsible. At national level, the NWMA cooperates with the GCS. At regional level, the regional water management directorates (RWMDs) cooperate with the voivodes.

Public-private partnership in Poland is based on specific PPP legislation and concerns joint (public-private) investments in infrastructure projects. The entities involved and the GCS cooperate efficiently with the private sector.

Good practice:

- The private sector, academia and NGOs are involved in the risk assessment process, at least on a sectoral basis for different fragmentary reports.
- The Government seeks cooperation with the private sector and academia to develop its risk assessment methodology.

Recommendations:

- Make more specific and centrally (GCS-) directed use of the knowledge and expertise of the private sector (academia, research & development institutes, NGOs, CIs, companies) to supplement specific, predefined parts of the fragmentary reports and cross-cutting risks and themes.
- Consider involving CCA stakeholders more actively in the NRA process.

2. Methodology

Objective: a methodology is developed to carry out risk assessments. Expected impacts of identified risks are assessed according to an established methodology and risks prioritised accordingly.

The method for conducting risk assessments in Poland is set out in a 'procedure for drawing up the fragmentary report', prepared by the GCS with a view to facilitating the risk analysis process and standardising the information provided by the various stakeholders. In the procedure, 'risk' is defined as a combination of consequences of a hazard (threat) and the associated likelihood of its occurrence. All available historical and statistical data should be used to assess likelihood.

Each coordinating ministry develops its own fragmentary report. The risk focus and information can differ, but the sectors are provided with a unified approach and method. The methodology is based directly on the *EU risk assessment and mapping guidelines for disaster management*,[11] the Joint Research Centre report on *Risk, hazard and people's vulnerability to natural hazards: a review of definitions, concepts and data*[12] and experience acquired in Sweden, the Netherlands and Norway. The methodology, tailor-made to Polish needs, is described in a manual and supported by an Excel template (see chapter 3).

The basis of the methodology is a systemic process. All available information (i.e. past occurrences) and opinions (i.e. expert expectations) are considered and it is flexible and open to absorb new knowledge, e.g. new statistics. The methodology is applicable at all four levels of government and is easy to use. The method analyses and assesses over 20 identified threats. The categorisation of risks/threats, as set out in the guidelines for developing the fragmentary reports, identifies primary hazards, natural disasters, civil hazards, threats resulting from intentional human activities, terrorism threats and political and military threats. It was claimed that the risk register contains 164 entries in these categories.

According to the hazard identified, an appropriate team of experts is convened according to a procedure set out in the guidelines. In the first instance, a context analysis is conducted: identifying and defining the problems, involving the right stakeholders (e.g. communities, organisations, property owners, population, etc.), describing applicable legislation and policies, the political and economic circumstances, and social and cultural issues. The actual risk analysis starts by describing the scenario of a conditional risk (certain magnitude related to risk likelihood) in relation to the context. These scenarios describe what might happen and list potential impacts/consequences. A 'fault-tree' analysis is used to understand the probability/likelihood of the scenario. Other methods of probability analysis include 'event tree' (partial likelihood of specific consequence paths), statistical data, historical data, reliability and uncertainty analysis, and expert judgment.

[11] https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf
[12] JRC EUR 21410 (2004).

Following the assessment of the occurrence of a critical event, it is necessary to describe the consequences using event-tree analysis. For each scenario, possible impacts are examined in terms of the population, the economy, property, infrastructure and the environment. For each of these categories, both direct and indirect effects are indicated. In accordance with the *EU risk assessment and mapping guidelines*, human, economic, environmental and social-political impacts are taken into consideration (the latter form a subdivision under human impacts).

Human impacts

When analysing the human impacts of a scenario, the methodology adopted in Poland takes into consideration the following factors:

- potential number of fatalities;
- potential number of hospitalised (severely injured or ill) persons; and
- potential number of evacuees.

In a second phase, the potential impact on everyday life is indicated. Also, the indirect social effects (such as an increase in unemployment and permanent incapacity for work) and negative psychological effects are considered. In addition, consideration is given to protecting the most vulnerable, e.g. the elderly and young children.

Economic/property/infrastructure impacts

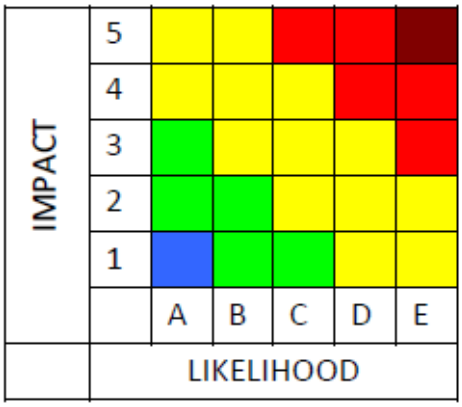
Potential damage to property and infrastructure is taken into account, as well as direct and indirect costs (e.g. direct costs of restoration of a damaged building, indirect costs of business interruption resulting from damaged premises).

Environmental impacts

Potential harm to fauna and flora and to air, soil and water must be described. An indication is given as to whether an adverse impact of a scenario is reversible or not (i.e. causing permanent or long-term degradation of the environment).

For these types of impact, an average score is estimated on the basis of pre-established criteria. The weight of each criterion is calculated according to probability level. The method is a mix of a quantitative and a qualitative approach.

All risks detailed in the RTNS are presented in a risk matrix in terms of their likelihood and impact. A separate 5x5 risk matrix is prepared for each part of the RTNS.



The risk value is determined by the colour:

- **minimum** (blue),
- **low** (green),
- **medium** (yellow),
- **large** (red),
- **extreme** (brown).

Finally, the level of risk acceptance for each scenario must be justified. There are four categories of risk acceptance:

- acceptable (A) — no additional measures are required. Current solutions and assigned capabilities and resources are sufficient. No action is required in addition to monitoring activities;
- tolerable (T) — the alternatives must be assessed as to whether the introduction of small organisational (legal or functional) changes contribute to the improvement of safety or feeling of safety;
- conditionally tolerable risk (WT) — additional security measures are to be introduced within six months and the solutions used must be improved; and
- unacceptable risk (N) — immediate action should be taken to enhance security; additional/new solutions should be introduced/provided.

The RTNS provides for the risk acceptance level of the national government and of the voivodeships to be established for each scenario. The levels might differ, depending on perceived risks at national and provincial level. While the national government considers whether the country as a whole is prepared, local governments' perceptions relate to their organisations and the territory for which they are responsible. It is natural that the local governments lack a nationwide perspective. A risk that is acceptable at provincial level might, in combination with the consequences in another voivodeship, be unacceptable for the nation. On the other hand, a risk that is acceptable at national level might be unacceptable at the level of a specific voivodeship. The GCS measures the risk levels objectively and communicates its judgment to the respective stakeholders.

Another element of the analysis is to determine for what kind of function a given scenario might require the involvement of an institution (in a leading, coordinating or supporting role). This part of the analysis should be supported by all available data, i.e. graphical and tabular data, charts, programmes, maps, diagrams, tables or other data from simulation programs on the basis of which the specific scenario has been described. For each scenario, a decision is taken as to whether it should be included in the NCMP. For capability development and preparedness, the GCS does not focus on a specific risk but on the modules of activities and resources that need to be addressed during the preparation of the NCMP. Some activities and resources could be the same for different types of risk, so it has to be ensured that all risks with the relevant activities are considered while developing the NCMP.

Recently, Poland has further developed its own specific risk assessment methodology with a consortium made up by the GCS, the Main School of the Fire Service, the Warsaw University of Technology, the Scientific and Research Centre for Fire Protection, the National Defence University and Medcore (an IT company). This resulted *inter alia* in the design of the ARMOR software (see paragraph 3.2).

Methodology for assessment of critical infrastructures

The RTNS addresses threats, vulnerabilities and impacts for CIs, as well as upstream and downstream interdependencies. Upstream risks are risks that a system depends on, i.e. that impact the operations (direct risks) of that system. Downstream risks are risks emerging from the actions/operations that impact an end-user/dependent. When analysing negative impacts of a scenario, one needs to determine whether a CI

might be affected. The Excel template for the national threat assessment (see paragraph 3.2) should state, and describe in detail, the extent to which the relevant CI systems are affected.

The assessment of CI is based on an 'all-hazard' approach and no distinction is made between technical causes and malicious acts. CIP is understood as ensuring physical security, technical security, personal security, IT/OT security, legal security, business continuity management and recovery. Private CIs are at liberty to choose their own methodology, but the GCS gives guidelines and recommendations on risk assessment and how to implement CIP in crisis management plans specific to CIs. Moreover, the GCS promotes business continuity management, for different CIs to identify whether they depend on the same subcontractor. A special working group is currently working on identifying a common risk assessment methodology and integrating CIP concerns into crisis management plans. In general, the GCS refers CI owners/operators to ISO standards.

The GCS reviews the risk assessments made by private sector CIs and makes recommendations as required (review identified threats, check interdependencies and recommend exercising). Whenever the quality of the risk assessment is questioned, CI owners/operators are invited to the GCS on a one-to-one basis (organisation) to discuss differences. In such cases, the GCS questions and challenges the assessment process and makes recommendations. In the event that certain hazards have not been taken into consideration or if certain impacts/consequences are missing, the GCS seeks clarification. In addition, it seeks to identify reasons/justifications/explanation when in disagreement with the CI's or local government's assessment. The GCS has, as yet, no authority to review CI operators' plans. All potential stakeholders such as ministries, voivodeships, etc. will be invited for discussions and a compromise negotiated. Exercising is used to challenge the quality of the risk assessments.

Methodology for assessment of climate change related risks

In the assessment of climate change scenarios, all (e.g. social, economic, etc.) aspects of impact and vulnerability are taken into consideration.

The NWMA coordinates implementation of the EU Floods Directive (2007/60/EC).[13] All EU obligations have been incorporated into Polish regulations. Preliminary flood-risk assessments are developed that provide a general view of flood risk and a GIS analysis. Flood-risk maps have been produced in compliance with the Directive. The assessment involves collecting data, creating a database, identifying significant risks and selecting areas of potentially significant flood risk (APSFRs). Flood-risk impact criteria take the following factors into consideration:

1. direct impact;
2. economic impact;
3. effectiveness of existing flood protection; and
4. impact of spatial development.

[13] http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:32007L0060

Vulnerabilities taken into account include human life and health, environment, cultural heritage and economic activity. A mechanism is in place for the purposes of investment prioritisation.

Methodology for assessment of cyber risk

The assessment of cyber risks is based on ISO 31000 and ISO 27005. Probability and value of loss are combined in the calculation of the level of risk. When this is below 20 % of the maximum, the risks are automatically accepted. When it is above 20 % of the maximum, the next phase of the risk assessment is triggered, control measures are taken and the level of risk is then recalculated and re-evaluated. If the new level is below 20 % of the maximum, the risk is accepted, but remains under the supervision of the owner so that it can be monitored. Risks at levels between 20 % and 80 % are subject to approval according to the principles laid down by the entity or are re-evaluated. Risks at levels of over 80 % are presented for approval to the top-level management of the entity. Every year, public entities have to report the risk analysis outcome to the ministry competent for the implementation of IT solutions.

Good practice:

- Poland has developed its own methodology for NRA, which is in conformity with EU standards (e.g. it reflects all aspects of vulnerability — social, physical, economic and political). It takes into account lessons from other countries, but is tailor-made for the Polish context. Some elements (two-way process, feedback loop, sectoral reports, a combination of qualitative, quantitative and semi-quantitative methods, a questionnaire that can be used by non-experts) are particularly noteworthy.
- The GCS adjusts the risk assessment at national level and gives recommendations at appropriate sub-national level. In the event of a discrepancy between central and provincial risk acceptance levels, a two-way phase level is adopted whereby a discussion is entered into and some kind of compromise is reached.
- The Polish Geological Institute (PGI) — National Research Institute has a picture of impacted sites with landslides in Poland, using a qualitative approach to risk estimation and methodology incorporating high-level data.
- The GCS refers CI operators/owners to ISO standards.

Recommendations:

- Implement the ARMOR software and the corresponding adjustments in the assessment method in a structured manner.[14]
- Continue developing the Polish risk assessment methodology on the basis of evaluations and feedback from Polish stakeholders.

[14] Poland expects ARMOR to be implemented before mid-2017.

- Actively engage with the JRC to compare the Polish methodology with other Member States', in order to explore how its innovative features can add value to the overall risk assessment methodology currently in use in the EU.
- Stimulate the use of the common overall risk assessment methodology at all levels to ensure that risks that are not of national concern are also monitored.
- Consider adapting the national methodology for local (*gmina* and *poviat*) use.
- Consider how the assessment of local and regional vulnerabilities and capabilities could be reflected in the methodology, because that determines the point at which decentralised coping capacities are exceeded (thus creating a need for national involvement).[15]
- Make clear what the interlinkages are between the NRA methodology and several sectoral methods, e.g. for CIP, CCA, flood-risk assessment, etc. Consider developing a concise guide on how the RTNS could help specific sectoral assessment.
- Consider ways to give more attention in the methodology to the international and cross-border dimension of risks, in order to facilitate dialogue with neighbouring countries (see paragraph 1.2).
- Use standardised definitions (EU, ISO, UNISDR) for all relevant concepts.

[15] The Main School of the Fire Service is currently (mid-2016) working to identify systemic barriers, including local and regional capabilities, and studying the possibilities of quantifying these.

3. Information and communication

3.1 Information-sharing

Objective: the infrastructure and appropriate information is available to carry out the risk assessment.

The procedure for drawing up fragmentary reports identifies the following means of acquiring data:

- analysis of statistical data;
- analysis of historical data;
- professional judgments of experts;
- field studies;
- assessment of the international situation;
- mathematical modelling;
- analysis of data from threat monitoring systems;
- analysis of trends;
- test cases ('case studies'); and
- environmental diagnosis, etc.

The RTNS collates and analyses all such data in a uniform way. Some of the data are classified and therefore not available for all stakeholders (or the general public).

In 2011, a procedure was put in place as regards historical data for the needs of risk assessment, but there seems to be no common data quality standard in use. The quality of information is assured by the professionals from the stakeholder entities. Recently, several ministries have launched an initiative to develop a methodology on the collection of loss data, in accordance with EU guidelines. Historical data for different sectors are not comparable and depend on the entity and region concerned. For the estimation of disaster losses, a specific department dealing with assessment in the Ministry of the Interior and Administration is trying to unify information.

Critical infrastructure protection

The legislation requires CI owners/operators to share information with the government. CIs are obliged to share and report information with/to public authorities whenever this is evidently valuable and the information is considered to impact the nation. The NCIPP requires the appointment of CI contact points for designated CIs. Similarly, local crisis management plans require the appointment of local governmental contact points within public CI entities. The GCS is the coordinating first contact point among designated CIs. GCS guidelines provide direction on the sharing of information between CIs, particularly on issues relating to interdependencies. Local contact points act as a channel for the sharing of information and knowledge between CIs, local authorities and the GCS. The GCS is considered as the first level of contact in emergency situations. There is a CIP mechanism at operational level for the sharing of information. It is web-based for the sharing of general unclassified information.

The GCS shares information with voivodeships and CI owners/operators. The sharing of classified information between CIs and GCS is kept confidential. CI operators can share classified information with the GCS, ministries and voivodeships. The government is able to receive classified information. The Internal Security Agency shares information directly with CIs in respect of terrorist threats. Although the sharing of information is obligatory, it is the CI owners/operators who decide what information to share. The GCS has no guarantee that 100 % of information is shared. Thus, it is the GCS's role to evaluate the completeness of the information received and it needs to improve the system of information-sharing between CIs and central authorities. CI operators are not keen on sharing all information, claiming that classified information relating to market and commercial issues might be misused by competitors. This requires the GCS to work harder to build confidence and trust among the designated CIs. Although Poland's CIP model does not involve sanctions, the operators generally take their responsibility for CIP seriously. However, while information-sharing between private operators and the public sector is obligatory, the level of trust is not yet sufficient to ensure that all information is shared.

Nonetheless, a specific procedure is in place for the exchange of information between CIs, local governments and the GCS, specific to threats from landslides and other natural hazards. The GCS aims to ensure that all stakeholders adhere to this procedure.

Climate-change adaptation

The Institute of Meteorology and Water Management — National Research Institute cooperates closely with the GCS, the Fire Service, etc. It focuses primarily on issuing warnings of events potentially occurring in the short term. In addition, it researches potential forecasts of long-term events. In terms of forecasting, it has basic scientific limitations for predicting events. The time factor for a reasonable forecast/prediction is 10 days. The Institute is not yet equipped to provide reliable long-term predictions. It is currently going through a learning curve. With further investment in research, it could be in a position to provide longer-term predictions in the future. It is also learning from the process of assessing and forecasting risks. At the Institute, there are no regulations for the assessment and management of risks from droughts, but it is making an effort to catch up in this respect too.

The Institute cooperates closely with the GCS and GCS risk assessments take account of its data, e.g. on potential severe weather events and the impact of adverse weather events on citizens, the economy and national security. Various tools are used for the exchange of data with these organisations and the public in general. The Institute evaluates and provides data relating to hazards and passes data on for further analysis to enable others to identify potential risks and distinguish between hazards, threats and risks.

A flood management strategy document is currently in the final stages of approval. The Institute follows developments in other countries and learns from their good practices. The NWMA has flood records going back to the 20th century. The database does not take losses into consideration, but the NWMA gathers loss management

data. The Commission is working closely with Poland to improve the recording of losses relating to floods.

Landslides

One of the main root cause of landslides in Poland is human activity. The key triggers are rainwater and/or meltwater, exacerbated by human activities/investments. There is a qualitative approach to risk assessment. Under the SOPO project, a landslide inventory with maps of landslides and terrains prone to failures has been developed and every commune receives a map of landslides. Heads of *poviats* are obliged to maintain a register of areas at risk of mass movement.

Good practice:

- Poland has high-quality data and uses scientific data and analysis for NRA purposes, as well as other statistical data analysis of events.
- CI newsletters, workshops and conferences on specialised issues, such as technical failures, biometric data, explosions, etc.

Recommendations:

- Develop a common standard on data used for risk assessment.
- The Commission's *Guidance on recording and sharing disaster damage and loss data* could be very helpful in the process of developing a methodology on loss data.
- Efforts should be made to improve the sharing of information on sensitive CIP issues. Market and competition issues are obstacles that need to be managed through persuasion and the building of confidence and trust, but also by means of a clear *modus operandi* for the exchange of sensitive information (see also the recommendations in paragraph 6.2).
- Build trust between private operators and the public sector in the process of information-sharing, taking into account the economic value of the risk for individual operators. Risk assessment could include an estimate of the potential economic loss for the operator in the event of disruption of operations. That information could be used to prioritise public-sector support for private operators in business continuity management.
- Encourage authorities (*poviats* and *gminas*) to implement the approach and results of the SOPO project in all landslide-prone areas in Poland.
- Pay more attention to human activity as a major factor in slope failures when assessing local level landslide risk.

3.2 ICT infrastructure

Objective: an effective information and communication system for the assessment of risk is available.

Excel for risk assessment

A special Excel template/form has been developed to assist NRA. The following have to be entered in the template:

- 'threats' – where hazards/threats are indicated; scenarios are developed and risks are assessed;
- 'prevention' – where strategic objectives are determined, together with detailed actions and the capabilities and resources required to achieve them;
- 'preparation' – where programmes aimed at improving security and safety are indicated, together with their duration, funding source and responsible institution;
- 'response' – where priorities and principles for responding are described;
- 'historical data' – where previous emergencies are described according to the following parameters: date or duration, time, place of occurrence/affected area, consequences and losses;
- 'conclusions' – where all additional conclusions, remarks and findings are included.

The methodology document includes a CD-ROM with 795 glossary entries of scenarios in this Excel template.

ARMOR

ARMOR is a software instrument that has been developed to support the process of risk assessment. Still in its initial test phase, ARMOR requires the identification, compilation and input of a set of parameters, which differ according to threats listed in the risk register. Input is by means of a questionnaire with yes/no answers (during the threat identification phase) and other open questions on the number of people or geographical data.

The questions are pre-set into ARMOR, which interprets the replies to the questionnaire. Once a question is answered, the systems will know and will not raise the same question again. The outcome is presented directly on a risk matrix. The result is also mapped. Scenarios can be shown on a map and made available to all government levels. Each voivodeship can see all its own county and municipal scenarios, but only aggregate information for other voivodeships.

Risk acceptance levels are set by the risk owners. ARMOR users can make recommendations for development of the tool and these, if valid, will be incorporated into the system. Users can also add information to the system directly.

In its present version, ARMOR is only an IT tool for state agencies. It is not yet available at the other lower levels of government, e.g. voivodeship, *poviat* and *gmina*. It can also be used for CIP purposes. The selection of stakeholders/experts is not part of the tool, but non-experts can use it by means of Q&A with expert users.

Entities decide who to include, but it is recommended that they include entities/ministries at national, voivodeship, *poviat*, municipality and commune level. A very strict security policy applies. However, the tool is still in its test phase (not yet live).

ISOK

The Meteorological Institute has a number of systems, including ISOK, which has been developed through an EU project by a consortium headed by the NWMA. It is an IT system developed to protect society, the economy and the environment against extreme hazards and to support decision-making in the event of dangerous occurrences. ISOK is currently in its fifth stage of implementation. It includes local hazard maps. It is part of the National Infrastructure of Spatial Information and makes intensive use of reference data from the Main Office of Geodesy and Cartography (GUGiK). It is equipped with portals used for the advanced presentation of information and spatial data (maps) from a variety of sources (created in the system, but also from external sources).

ISOK presents *inter alia* preliminary flood-risk assessment, flood-hazard and flood-risk maps, and geo-spatial data relating to meteorological hazards, etc. Thanks to the additional data in the system (e.g. warnings of the National Hydrological and Meteorological Service, communications, table data, diagrams), it is possible quickly to identify the scale and range of a hazard, which supports the taking of appropriate preparatory and rescue action.

Good practice:

- Specific tailor-made software is developed for the NRA: the summary spreadsheet (Excel table with risk degree chart) and the newly developed ARMOR software with a questionnaire for non-experts.

Recommendation:

- Investigate the possibility of implementing multi-hazard risk-mapping based on standards for data exchange and GIS that can integrate existing mapping on different scales.[16] Risk-mapping can be done on different scales depending on the objective, but if the same GIS standards are used, the results of all risk-mapping projects could be implemented in a single mapping system or coherent set of systems.

3.3 Risk communication

Objective: the necessary administrative capacity is available to communicate the results of risk assessments to the public.

The RTNS is a classified document, but the NCMP is publicly available. For the future, the objective is to publish the NCMP on a website showing the interconnections

[16] See also Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE); http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007L0002

between the various sections. However, this is more for professionals and interested people than for ordinary citizens. Poland is trying to set up a website to inform the public and involve it in emergency management. This will contain information for citizens on how to protect themselves in emergency situations. For now, the GCS publicises this kind of information on social media (Facebook and Twitter).

The GCS encourages government bodies to make their crisis-management plans public. In principle, reports/plans are public except for classified CI issues. As far as CIs are concerned, no information is made public. Actual practice may differ across regions and agencies. During the peer review mission, several good examples were shown of how the public is informed (e.g. by the PAA, the Meteorology Institute and the NWMA) of the results of the risk assessment in order to understand their role and take preventive and preparatory measures. Also, the Mazovian Voivodeship, the City of Warsaw and the City of Płock have systems, routines and activities to inform their

citizens of identified and assessed risks. Various kinds of risk information (including maps) are available for the public. Usually, this comes from local risk assessments and fragmentary reports, rather than from the RTNS itself. However, the focus of public awareness policy is more on exercises than on plans. No national exercising involving the public is organised. Poland involves stakeholder organisations in exercises, but not the public in general.

The Meteorological Institute provides information to a free mobile application for weather events and other threat warnings. This regional warning system is used by the emergency services to inform the general public. It contains special instructions for the civilian population on how to behave in different emergency situations.

The Warsaw Safety Centre[17] provides the public with generic information on events of public importance. The public can also get in touch with it online. Its website is intended to inform the public and has lots of information that might be of interest to citizens at large. A free mobile application available for download on mobile phones provides information on 'problematic events'. The Centre also sends public early warnings of serious emergency events. Agreements with media operators and TV stations, etc. are in place that allow the early communication of emergency information for onward broadcasting to the general public.

The PAA is involved in public communication in the event of radiation emergencies and provides expert assistance to decision-makers (Minister of Internal Affairs, voivodes). It has developed and implemented a communication strategy and maintains close contacts with the media, in order to clarify information on nuclear and radiation safety in the event of a crisis. In the preparedness phase, the PAA also gives information to universities and students, as needed, in order to raise awareness among young people (students) of its responsibilities and tasks, and existing arrangements in the field of emergency preparedness and response to nuclear accidents or radiological emergencies.

[17] The Centre was visited during the peer review mission, so we include some specific observations on it here, whereas other cities and similar agencies that were not visited are not described.

Urban spatial policy addresses the protection of citizens. It aims to inform different groups (i.e. children, the elderly) on how to behave in any emergency situation, to ensure that government plans are useful and meet the needs of the public, and gauge whether the information is sufficiently understandable by citizens.

The public has access to information on landslides that has been gathered by the PGI in the SOPO database. In the event of prospective public investments, information on terrains prone to landsliding can be obtained via self-government units and should be corroborated by the PGI. Before they build in slide-endangered areas, members of the public are encouraged to approach self-government. Heads of *poviats* are obliged to monitor areas/locations prone to landslides, where there is a threat to human life, lifelines and the transportation network, and inform the public accordingly.

Critical infrastructure protection

Most CIP information is classified. This is regarded as an obstacle to achieving a sufficient level of risk-governance transparency *vis-à-vis* the general public. One way of raising risk awareness among the general public, without sharing classified information, is to involve interested stakeholders in the process of consequence management.

Climate-change adaptation

Flood-risk assessment maps are available online. The NWMA has drawn up 12 draft flood-risk management plans after public consultations involving some 3 000 persons through the National Water Forum: local authorities, academics and threatened property owners. It delivers flood-risk education programmes, promotional material (e.g. a video entitled *It's not my problem*) and advertising material on various topics.

The Infrastructure Office in the City of Warsaw uses a board game to communicate information on climate change to youngsters. Primary school curricula include special classes on climate change. Activities and games are organised for different age groups, as are a number of educational campaigns. Brochures are also published to teach children at an early age. Poland has just started on this work and needs to do more to pass on such information to the general public.

Good practice:

- The GCS publishes various brochures on its website, as well as several manuals on how to prepare and protect against certain hazards.
- Flood-risk maps are available online and there is a flood-risk education programme. The accessibility of information leads to more participation by the various stakeholders and the public in general.
- The ISOK risk maps will be available to all citizens.
- The GCS has a designated website providing information to the general public, with special manuals that give advice on how to behave in emergency situations.
- There is a free mobile application for weather events and other threat warnings.

Recommendations:

- Develop, on the basis of the NRA, a general risk communication strategy (incorporating CIs) to improve ordinary citizens' knowledge and awareness of, and participation in, prevention, preparedness, response and recovery activities. This should assign responsibilities for communication (based on the security matrix), but also ensure the coherence and integration of communication activities (e.g. a national website, bulletins, information campaigns, etc.) by different ministries, national agencies and other government bodies at all levels and in all sectors.
- The GCS should have the central coordination role in the strategy, ensuring its coherence and the consistency of the information. The existing GCS brochures on how to behave in specific emergencies could be integrated into the overall strategy. The publication of additional brochures and information could be prioritised on the basis of the RTNS.
- Also develop (as part of general risk communication or at least in direct correlation with it) a general CCA communication strategy, bringing together the communication activities of the Ministry of Education, Ministry of Environment, the GCS, etc.

4. Expertise

Objective: the experts carrying out the national risk assessment have the requisite competencies and responsibilities and have received appropriate training.

The GCS has coordinated the development of the NRA methodology. It has also issued concrete guidance on the procedure for drawing up fragmentary reports. The role of the GCS includes organising relevant training and workshops for the bodies involved in the process. Its aim is to present the risk assessment methodology being adopted and to raise awareness among crisis management experts.

The ARMOR software for the NRA is user-friendly. It asks simple questions and non-experts do not need a technical understanding of the methodology, i.e. it can be used at commune, municipality, voivodeship and national levels by users without technical knowledge or understanding and can still achieve set objectives. Some could have expert background and expertise in risk assessment; others may simply be administrators, collecting data based on statistical records without the need for specific expertise. A trained officer will be asking the questions as indicated by ARMOR and the local experts have to provide the answers. Replies are then entered in ARMOR, which interprets them accordingly. In complex scenarios, specialist parameters are incorporated into the system in layman's terms, whereby an administrator with no real technical/scientific knowledge can question stakeholders, collect necessary input data and let ARMOR interpret the data and provide a meaningful interpretation.

There is a wide scientific community that develops, trains and supports governmental bodies in their assessments (the Main School of the Fire Service, Warsaw University of Technology, the National Defence University, etc.). There is no formal programme to train all risk-assessment professionals in the government sector, but there are diplomas, graduate and post-graduate courses, in addition to the general courses provided by the Main School of the Fire Service. The Main School is a university supervised by the Ministry of the Interior which prepares employees to ensure fire safety and civil protection. It has many bilateral agreements with counterparts in other countries. It also provides special courses for other civil sector employees. Students are currently being trained in using the established method for NRA. An e-learning programme for administrators has been developed (risko.e.ucz.pl), the objective of which is to streamline the level of knowledge among risk-assessment and risk-management staff employed by public institutions. Also, the Main School is currently developing a full curriculum for the NRA method. In this way, it is developing the administrative capacity for risk assessment, but the approach is more systems- than policy-oriented and relies heavily on individual capacities.

There are numerous risk assessment and risk management related projects in Poland that help to create a high level of knowledge and expertise among participants.

Good practice:

- The Main School of the Fire Service offers studies in fire safety engineering, civil protection engineering and internal security. Each degree course covers risk assessment or quantitative and qualitative risk assessment methodology.
- There is already an adequate level of knowledge among individual stakeholders involved in the risk-assessment process. Specialist staff are employed at all levels of the administration.
- There is an e-learning programme to improve professionals' knowledge of risk assessment at governmental level.

Recommendations:

- In addition to education, organise experience-sharing between professionals working with the national methodology for risk assessment.
- Investigate the possibility for the GCS and e.g. Main School for the Fire Service to develop a shared systematic strategy (with concrete objectives) for further development of administrative capacity (expertise) to perform risk assessment at all levels of government. Rather than depending on professionals to sign up individually for courses or students to start following an education programme, develop a targeted approach to identify and address weaknesses across government.
- As part of the above programme, good use can be made of the existing e-learning tools. Also, training on risk assessment and decision-making can be organised at all levels of government, with a view to standardising risk-assessment methodology in the country.
- Promote an interdisciplinary academic dialogue on risk-assessment methodologies in different sectors, to keep improving the methodology in future.
- Consider developing a national strategy to coordinate research and development for risk assessment and risk management, as a basis for joint action by academia, NGOs and the private sector, whereby all research on the topic of risk assessment and management is shared, communicated and used by all stakeholders in the country.

5. Financing

Objective: financing includes the identification, estimation and setting-aside of funds required to carry out and update risk assessments.

The financing of action to manage catastrophes is a complex area. In accordance with the Act on Crisis Management, the state budget provides for the financing of crisis management tasks at national level, including some funds at the disposal of the voivodes. *Gminas*, *poviats* and voivodeships have to finance their tasks in the field of crisis management from their own budget, but can receive subsidies from the state budget. The state budget provides for an annual reserve for prevention and recovery of around PLN 1 billion (EUR 230 million). In the general part of this amount, the share set aside for recovery is increasing. In 2016, Poland plans to use about 50 % of the budget for catastrophe prevention. The reserve is also used for the rebuilding of anti-flood infrastructure, direct help for the population and protection from landslides. Article 26(4) of the Act on Crisis Management requires local government to reserve 0.5 % of its budget for prevention and recovery.

The Ministry of Interior and Administration manages the following anti-flood projects:

1. the Oder River Basin Flood Protection Project (total cost: EUR 712 million), which includes construction of the Racibórz dry polder and reconstruction of the Wrocław waterway junction. Completion of the project will directly improve flood protection for about 2.5 million people; and
2. the Oder and Vistula River Basin Flood Protection Project (total cost: EUR 1.2 billion), which includes building new reservoirs and the reconstruction of floodbanks around the Central and Lower Oder River, the Kłodzka Valley and the Upper Vistula River. Completion of the project will directly improve flood protection for about 5.2 million people.

Both projects are financed from the state budget, the National Fund for Environment Protection, water management loans from the European Bank for Reconstruction and Development and the Council of Europe Development Bank, and EU funds.

Poland supports various instruments at regional and local levels, but there is a need for an integrated financial assessment instrument (e.g. to assess whether buying a flu vaccine is justified). There is as yet no clear procedure for prioritising funding for prevention measures and linking this to the risk assessment in the RTNS. A methodology for evaluating financial resources for risk reduction has been developed in cooperation with the GCS. Ultimately it has to be used as part of the strategic document dealing with matters of risk management and should be approved by the Council of Ministers.

Furthermore, no funds have been allocated for developing risk-assessment capacity. However, the GCS does have its own budget for performing its tasks, including coordination of the RTNS.

The Department of Civil Protection and Crisis Management (former Department of Disaster Prevention and Recovery) in the Ministry of the Interior and Administration

has special reserve funds for prevention and recovery from 'acts of God'; these can be allocated to government administrations, local governments and citizens. In the case of citizens, financial relief is granted under the Act on Social Relief by means of administrative decisions by local government (which are subject to appeal).

Good practice:

- Use of special reserve funds to finance reconstruction of technical infrastructure (of self-government units) and flood-protection infrastructure. Self-government entities have to satisfy certain criteria in order to receive funds. Plans have to be established to determine how to return infrastructure to its original state and introduce systems to avoid a repeat of similar adverse events.

Recommendations:

- Develop a policy for allocating financial resources for risk assessments at all government and sectoral levels. As 'understanding risk' is a key priority in the Sendai Framework, it seems logical to allocate specific budget in a national DRR strategy (see paragraph 6.1) to improving risk-assessment capabilities.
- All funding for prevention, preparedness, response and recovery should be 'risk-informed', i.e. based on the NRA or specific (sectoral) assessment. For EU funding, a clear risk assessment is required, indicating the relevance and degree of priority of the proposed project.
- The continuity of important prevention- and monitoring-related projects funded under EU programmes or from other sources has to be ensured. There should be a stronger link between relevant national and regional projects and the state budget in order to avoid double funding for similar measures or priorities.
- Stakeholders at all levels should be encouraged to explore direct opportunities to seek and make use of EU funding in addition, or as an alternative, to state funding for the purpose of managing risks and contingency/emergency planning at organisational, local and/or regional levels.

6. Interface with risk management

Objective: following the development of the national risk assessment and maps, the authorities concerned should seek to interface in an appropriate way with the ensuing processes of risk management.

6.1 Interface with risk management in general

The legislation defines 'crisis management' as a comprehensive concept that includes risk prevention, preparedness, response and recovery. The RTNS is the basis for civil emergency planning and strategic DRR policies. All GCS documents (the NCMP and the NCIPP) are based on the National Threats Assessment.

The conclusions of the RTNS are not only part of the NCMP, but are also included in all other crisis-management plans at all levels of government. Each ministry and public agency referred to in the Act on Crisis Management has to develop its own sectoral crisis management plan taking account of the RTNS. In some cases, detailed requirements on emergency preparedness and response to specific hazards are also laid down in legislation, such as the Regulation on emergency plans for radiation emergencies.[18] According to the Act, the other three government levels each have to develop their own crisis management plans, which have to include 'the characterisation of threats and risk assessment of their occurrence, including those relating to CI, risk maps and maps of threats', i.e. the RTNS. To link central and local planning processes, the crisis management plans (and the risk assessments on which they are based) have to be approved at higher government level (in the case of municipalities/*poviats*, by the voivodeship; in the case of voivodeships, by central government, etc.).

The philosophy is not to have too much detailed crisis management planning. Rather, the planning is modular, focused on prepared generic response capabilities and the competence of professionals (through training and exercises). The GCS focuses on the process of preparing the NCMP, rather than on the plan itself. It thus concentrates on training, preparedness and national/cross-border exercises. Procedures are tested at all levels.

The RTNS outlines 'strategic objectives' for risk management. Risk management capabilities are defined as measures to reduce, adapt to or mitigate risks. The objectives envisage ideal actions intended either to minimise the likelihood of a potential threat or to mitigate its adverse consequences. An indication must be given of the resources and capabilities necessary for the fulfilment of all strategic objectives. The next step is to outline all the action that has to be taken.

[18] The PAA is a central government body competent for matters of nuclear safety and radiological protection (regulatory body). Its activity is regulated by the Atomic Law of 29 November 2000 (*Journal of Laws*, 2014, item 1512) and the relevant secondary legislation. In order to facilitate the early notification of nuclear accidents or radiological emergencies, Poland has signed intergovernmental bilateral agreements with 10 countries, including all neighbouring states. The radiation emergency plans developed and maintained at voivoideship and national level are attached to relevant (provincial or national) crisis management plans.

The RTNS should include programmes intended to improve security and safety at national, regional and local levels. It should identify entities responsible for each programme and specify timeframes. It makes it possible to determine what kind of preventive and preparedness action is in place. It identifies gaps and overlaps and informs decision-makers about the economic value of appropriate risk-management measures and sufficient investment in risk reduction.

Specific indicators are established to monitor the implementation of DRR action. For the near future, a scoreboard with more detailed information is envisaged, based on a questionnaire.

A national strategy on regional development to 2023 is in place, but it seems that this is not related to risk-management policy.

The risk-management cycle is closed by evaluation. The recovery phase is not only about rebuilding, but also about evaluation for a new planning cycle and re-assessment of risks: if something has failed, an available alternative needs to be in place.

Good practice:

- A very clear division of responsibilities and risk ownership (for all four phases of crisis management) is in place, based on a security matrix prepared by the GCS.
- A direct link is in place between plans at local/regional/provincial and national levels.
- All DRR projects relating to flood risks are managed by the NWMA. All regional authorities affected by the impacts of the projects are involved.

Recommendations:

- Ensure that the NRA feeds into all four phases of crisis management: prevention, preparedness, response and recovery. A national DRR strategy should be developed in accordance with the Sendai Framework. Recommendations from the RTNS should be included in the DRR action plans.
- Consider providing one body with enough power and competences to coordinate the DRR strategy, in close connection with the NRA.
- Provide municipalities with technical support to develop mitigation programmes, information-gathering and -sharing, and awareness-raising activities. Different scenarios could be developed for decision-makers and communities to undertake the right prevention measures as regards population and urban infrastructures.
- Evaluate existing planning and reporting documentation from the various public and private entities, in order to review and improve risk-management performance. Create Build a direct link between risk management, urban and land-use planning and make use of available risk maps for urban planning. It is equally important to plan an effective programme to reduce and/or minimise risk through better use of spatial planning.
- Involve citizens in emergency exercising (rather than just informing them).

6.2 Interface with critical infrastructure protection

The Act on Crisis Management defines CIs as systems and interrelated functional objects comprising such systems, including facilities, devices, installations and services of key significance for the security of the state and its citizens, as well as those ensuring the efficient functioning of public administration authorities, institutions and enterprises. CI comprises the following systems (sectors):

- energy, fuel and energy resources supply system;
- communication system;
- tele-information network system;
- financial system;
- food supply system;
- water supply system;
- health protection system;
- transport system;
- rescue system;
- system ensuring the continuity of public administration activities; and
- systems for the production, storage and use of chemical and radioactive substances, including pipelines for hazardous substances.

Disruption scenarios are identified in terms of costs, casualties, etc. CIP is based on Deming's cycle.[19] The CIP system does not involve sanctions, but is based on shared responsibility, cooperation and trust.

Criteria are established for designating CI objects in each system. CI designation is a three-stage process:

- CIs are pre-selected on the basis of established sectoral criteria (for each of 11 systems);
- an evaluation is carried out to establish whether CIs are vital to the functioning of society; and
- the CIs are assessed on cross-cutting criteria, taking into consideration casualties, economic effects, the need for evacuation, service loss, recovery time, international effects and uniqueness. To qualify as CI, a system must meet a minimum of two of the criteria.

The criteria and the resulting list of designated CIs are classified. The voivodeships integrate the list of CIs located on their territory into their crisis management plans. Certain local government systems and assets are regarded as CIs.

There are no special procedures or legislation concerning CIs owned by foreign entities. Each CI owner entity is registered in Poland and is obliged to abide by Polish law. The same obligations apply to all designated CIs.

Article 2 of the CIP Directive[20] defines 'European critical infrastructures' (ECIs) as critical systems that are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or

[19] 'Plan, Do, Check, Act'.
[20] 2008/114/EC.

destruction of which would have a significant impact on at least two Member States. The Director of the GCS distinguishes between ECIs located on Polish territory and those in other Member States which could have a significant impact on Poland. For the identification of ECIs, account is taken of the thresholds whereby the Commission and the Member States determine characteristic parameters or functions of ECI objects, facilities and installations. Information on CIs and ECIs is classified, in accordance with Article 9 of the Directive. The GCS functions as the ECIP contact point, in line with its Article 10.

It was stated that Poland is dependent on a number of CIs located in other countries. Poland addresses this in its crisis management plans.

The Council of Ministers has adopted a Resolution approving the NCIPP, which aims to create conditions for improving the security of CI, in particular by:
1) preventing the malfunctioning of CI;
2) preparing for crisis situations that could adversely affect CI;
3) responding in the event of CI destruction or disruption of its functioning; and
4) the reconstruction of impacted CI.

The NCIPP focuses on national CIs (local and/or regional CIs are covered in the relevant crisis management plans). The NCIPP identifies:
1) national priorities, objectives, requirements and standards to ensure the smooth functioning of CI;
2) the ministers in charge of government administration units and heads of central offices responsible for the systems; and
3) the detailed criteria for identifying objects, installations, facilities and services included in the CI systems, taking account of their importance for the functioning of the state and meeting the needs of citizens.

The NCIPP was prepared by the Director of the GCS in close cooperation with the ministers and heads of central offices responsible for the systems. In cooperation with the relevant ministers, the Director prepares a list of objects, installations, facilities and services in designated CIs.

The NCIPP is evaluated through internal audits, structural and budget changes, and exercising. Joint training events and exercises by government bodies and regular cyber exercises are carried out every year (since 2012)[21] in various sectors. Under the Act of 18 March 2010 on special powers of the Minister of Treasury and their performance in certain capital companies or groups operating in the electricity, oil and gas fuel sectors, a report on the state of CIP is compiled every three months.

[21] Cyber-EXE™ Polska exercises are organised by the Cybersecurity Foundation and co-organised by the GCS.

CIP is primarily an owner/operator duty, with the GCS acting as a coordinating body. CI providers (public or private) are required to prepare CIP plans on the basis of the risk assessment. The plans, which are subject to evaluation and approval by the Director of the GCS, include:

1. characteristics of CI;
2. a risk assessment based on the sectoral and cross-cutting criteria (see chapter 2);
3. reaction (procedures); and
4. cooperation with the authorities.

Identified authorities with specialised expertise (e.g. the water management authority, etc.) are involved in the process of approving CIP plans.

Guidelines are in place for all entities on how to integrate information on CIP in the respective crisis management plans. A CIP working group on crisis management planning oversees the NCIPP process.

A practical example is the private oil concern PKN ORLEN in Płock, which is considered a high-risk plant. PKN ORLEN cooperates with the GCS in the process of preparing the crisis management plans. The Płock fire service participates in joint exercises with PKN ORLEN and the municipal office informs the citizens about the exercises. PKN ORLEN has its own local early warning system which is tested twice a year.

Good practice:

- An 'all-hazard' approach to CIP is in place. The NCIPP closely reflects the principles of shared responsibility, cooperation and trust. CIP includes business continuity planning.
- The process of designating national CIs comprises three clear stages and follows well-defined fixed criteria.
- The creation of CI forums at the strategic national, regional and systems levels ensures the necessary representation of the various stakeholders.
- The CI mechanism at the operational level facilitates the exchange of information and includes an internet platform for the sharing of information on various CI topics.
- All CI operators prepare CIP plans and these are approved by the GCS.
- The GCS recommends and encourages the exercising of identified scenarios in both the public and private sectors.

Recommendations:

- Ensure that the NCIPP is not solely directed at individual CIs, operators or installations, but at complete CI systems and their interdependencies. Having all individual CI operator plans submitted to the GCS is an excellent basis for preventing and planning for (upstream and downstream cascading) disruption events that could impact the country as a whole.

- Review the mix of incentives for CIP. The current principles of shared responsibility, cooperation and trust are an excellent basis, but this might, in some instances, fall short of achieving its objectives. The use of additional incentives such as funding, tax benefits, CIP requirements in public procurement procedures and ultimately also sanctions could be considered in certain circumstances.
- It should be ensured that CI owners/operators share information that is relevant to the NRA process, in accordance with the CIP Directive.[22] In the case of classified information, there should be no (perceived) obstacle to sharing information in confidence with the regulator (i.e. the GCS in the case of Poland).
- Distinguish between CI forum gatherings, workshops and conferences. Forums are best focused on the sharing of good practices, networking between Security Liaison Officers and stakeholders' points of contact at sectoral and cross-sectoral levels (in order to identify interdependencies) and building trust between the various CIs. Workshops and conferences should focus on information-sharing and networking between stakeholder representatives.

6.3 Interface with climate-change adaptation

A CCA strategy is in place which has taken into account EU policies and documents in the field: the National Strategy for Adaptation to Climate Change (NAS) involves the preparation of specific risk management strategies at national, regional and local levels. The NAS is a general document indicating where the government wants to go and the developments it expects; it does not address specific risks. It takes account of some aspects of DRR and has a short-term and a long-term objective. The former is primarily related to response (to crisis situations resulting from climate-related events), which could be seen as development of coping capacity. The latter is to develop infrastructure and adapting capacity, i.e. CCA. The NAS includes action such as insulating buildings to protect against the effects of climate change. Poland also considers potential EU projects for funding purposes.

The NAS has a set of indicators to monitor progress in implementation, but there is no mechanism or system for reporting implementation. Statistics and other general information are used. Nevertheless, Poland is working towards developing a detailed questionnaire to help record progress. For climate-risk assessment, Poland has developed a guide on investment preparation as regards climate-change mitigation, CCA and resilience to natural disasters. This provides methodologies and hints as to how climate issues should be covered in the process of developing investments and projects at all stages, including project preparation, feasibility study, environmental impact assessment, project implementation and cancellation.

For the past 10 years, Poland has been engaged in updating and amending its legislation and transposing EU water management directives. All EU obligations have been transposed and future plans will be adjusted in line with EU developments.

[22] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ajl0013

The NWMA is responsible for flood-risk assessment. At national level, it cooperates with the GCS. At regional level, the RWMDs (non-integrated government administration bodies) cooperate with the voivodes and set up task forces to prepare flood-risk management plans.

Preliminary flood-risk assessments do not apply criteria for impact on spatial development. There is no clear evidence that they cover side-effects that do not have a direct impact. However, land-use planning may take them into account and the directors of RWMDs are consulted on land-use plans.

Good practice:

- The creation of an informal working group for the implementation of the NAS and providing support for the 100 000+ cities.
- Promotion of citizens' active participation in CCA issues. Individual citizens are protected in the same way as CIs: Poland divides citizens into groups, e.g. children, old people, etc. and communicates on how different groups should respond to particular events (e.g. heat waves, etc.).

Recommendations:

- Create a more direct link between the NRA and CCA strategies. The NAS and the regional development strategy could be better linked to the RTNS, given that they address areas such as investment policies and development issues.
- Ensure that the criteria for investments in development and the development of adaptive capacity take account of the NRA.
- Make concrete proposals in the assessment as to which hazards and vulnerabilities might be affected by climate change.
- Assign a clear overall priority to all climate change related short- and long-term effects from the perspective of national security and safety. In doing so, also make clear the relationship between the five-year planning period for the NRA and the planning periods of CCA strategies. As CCA requires a long-term strategy, this should cover a series of equal time horizons (e.g. short, medium and long term), with tangible objectives for each.
- Foster participation in the UNISDR 'making cities resilient' campaign by raising local governments' interest in and awareness of DRR focusing on urban risk.
- As regards implementation of the NAS, it is important to ask relevant stakeholders for information based on the indicators and to produce annual implementation reports in order to improve monitoring of progress towards the short- and long-term objectives.

Annex I Terminology and abbreviations

The following definitions are working definitions for the purpose of the peer review documents only. They are based largely on EU legislation and guidelines. Where official EU definitions were not available, UNISDR definitions have been used.[23]

Definitions

Contingency planning – a management process that analyses specific potential events or emerging situations that might threaten society or the environment and establishes arrangements in advance to enable timely, effective and appropriate responses to such events and situations.

Disaster refers to any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage.

Hazard is a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage.

Emergency services refer to a set of specialised agencies that have specific responsibilities and objectives in serving and protecting people and property in emergency situations.

Fragmentary reports refer to sectoral and provincial risk assessment reports, which are the basis of the RTNS.

Peer review is a governance tool by which the performance of one country in a specific area (in this case risk management / civil protection) is examined on an equal basis by peers who are experts from other countries.

Preparedness is a state of readiness and capability of human and material resources, structures, communities and organisations enabling them to ensure an effective rapid response to a disaster, achieved as a result of action taken in advance.

Prevention is any action aimed at reducing risks or mitigating adverse consequences of a disaster for people, the environment and property, including cultural heritage.

Risk is a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence.

Resilience is the ability of a system, community or society exposed to hazards to resist, absorb, adapt to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential structures and functions.

Response is any action taken at national or sub-national level in the event of an imminent disaster, or during or after a disaster, to address its immediate adverse consequences.

Risk management capability is the ability of a Member State or its regions to reduce, adapt to or mitigate risks (impacts and likelihood of a disaster), as identified in its

[23] http://www.unisdr.org/we/inform/terminology

risk assessments, to levels that are acceptable in that Member State. Risk management capability is assessed in terms of the technical, financial and administrative capacity to carry out adequate:

(a) risk assessments;
(b) risk management planning for prevention and preparedness; and
(c) risk prevention and preparedness measures.

Stakeholders with an interest in disaster risk management include *inter alia* scientific communities (including engineering, geographical, social, health, economic and environmental sciences), practitioners, businesses, policy-makers, central, regional or local levels of government, and the public at large.

Sub-national level refers to regional, provincial or local government actors tasked with disaster risk management.

Threat is a potentially damaging physical event, phenomenon or activity of an intentional / malicious character.

Threat assessment (in the Polish case) refers to risk assessment.

Abbreviations

Abbreviation	Definition
APSFR	Area of Potentially Significant Flood Risk
CCA	Climate Change Adaptation
CI(s)	Critical Infrastructure(s)
CIP	Critical Infrastructure Protection
DRR	Disaster Risk Reduction
ECI	European Critical Infrastructure
GCMT	Government Crisis Management Team
GIS	Geographic Information System
GCS	Government Centre for Security (RCB in Polish)
GUGiK	Main Office of Geodesy and Cartography
ISOK	IT System of the Country's Protection against extreme hazards
JRC	EU Joint Research Centre
LCS	Landslide Counteracting System
NAS	National Strategy for Adaptation to Climate Change
NCIPP	National Critical Infrastructure Protection Programme
NCMP	National Crisis Management Plan
NRA	national risk assessment
NWMA	National Water Management Authority
PAA	National Atomic Energy Agency
PGI	Polish Geological Institute
PSE S.A.	Polish Transmission System Operator
RTNS	Report on Threats to National Security
RWM	Regional Water Management directorate
SOPO	Land slide counter acting system
UNISDR	UN International Strategy for Disaster Risk Reduction

Annex II Overview of stakeholders

Representatives of the following institutions were involved in the peer review:

- Chief Inspectorate for Environmental Protection
- City of Płock Municipal Office and Municipal Risk Management Team
- City of Warsaw Municipal Office — Security and Crisis Management Office and Infrastructure Office
- Government Centre for Security
- Head Office of Geodesy and Cartography
- Institute of Meteorology and Water Management — National Research Institute
- Institute of Telecommunications
- Internal Security Agency
- Main School of the Fire Service
- Mazovian Voivodeship Office
- Ministry of the Interior and Administration
- Ministry of Development
- Ministry of Digital Affairs
- Ministry of Energy
- Ministry of Environment
- Ministry of Finance
- Ministry of Infrastructure and Construction
- Ministry of National Education
- National Atomic Energy Agency
- National Defence University
- National Headquarters of the State Fire Service
- National Security Bureau
- National Water Management Authority
- PKN ORLEN S.A.
- Polish Geological Institute — National Research Institute
- Polish Transmission System Operator (PSE S.A.)
- Scientific and Research Centre for Fire Protection — National Research Institute
- Warsaw University of Technology

Annex III Documentation

The following documentation was used to prepare for the review:

Nr	Type of document	Title	Version
1	Law/regulation	Act on Crisis Management	2007
2	Law/regulation	Regulation concerning the Report on Threats to National Security	2010
3	Law/regulation	Atomic Law	2015 (last amendment)
4	Law/regulation	Regulation on emergency plans for radiation emergency	2007 (last amendment)
5	Procedure	Procedure for drawing up the fragmentary report for the RTNS	2010
6	Report	National Risk assessment - RTNS	2013
7	Article	Summary of landslide counteracting system SOPO project and its relation to risk reduction goals	2008
8	Brochure	Flood? It's not my problem. Check whether you are in a risk group	
9	Brochure	Flood-risk management plans for river basin districts and water regions	
10	Presentation	Flood Directive implementation in Poland	
11	Factsheet	Information about the KLIMAT project	2015
12	Report	Polish National Strategy for Adaptation to Climate Change (NAS 2020) for the period to 2030	2013
13	Article	Climatologically based warning system against meteorological hazards and weather extremes: Poland	2014
14	Report	Strengthening the legal and policy framework for international disaster response	2014
15	Presentation	IT system dedicated to the country's protection against extreme hazards (ISOK)	2014
15a	Maps	ISOK map of other hazards	2014
15b	Maps	ISOK — maps of other hazards (short characterisation)	2014
15c	Maps	ISOK — meteorological hazards (visualisation system for national protection against extreme hazards)	2014
15d	Maps	ISOK – warning maps against extreme meteorological hazards	2014

Annex IV Thematic review framework

Peer reviews are conducted using standard frameworks that guide the peers in collecting information and analysing the disaster risk management structure in the country under review and how policies are implemented. The standard frameworks consist of objectives, requirements and indicators relating to various disaster risk management areas. Example questions in the frameworks can be used to guide the peer review team in the preparatory phase and during the mission. The teams can develop further questions during their review.

For the review of Poland, the thematic framework for risk assessment was redesigned to adapt to the requested focus on risk assessment capabilities. The structure of the framework and of the report is based on the *EU Risk Management Capabilities Assessment Guidelines*, although some topics are merged into one chapter (chapters 1 and 3). Also, the interface with risk management has been added as chapter 6.

Each chapter and paragraph starts from its objective, as mentioned below in the overview of the framework. The self-assessment questions for the relevant guideline were used to operationalise each objective into requirements. The objectives and, to a lesser extent, the requirements are the essential policy components under review. From the initial thematic framework for risk assessment, several key indicators were used as a basis for the review questions during the mission. The review questions therefore relate closely to the objectives, particularly those where the preliminary information received was not sufficiently clear or showed gaps. The indicators cover a wide area of policies, tools and methodologies and can be used by peers to help them identify examples of good practice, areas for improvement or possible gaps. The indicators do not represent a 'checklist' against which the country is formally assessed.

1.1	**Framework:** The risk assessment fits within an overall framework
Q1. Risk assessments are carried out on the basis of a clear legal and/or procedural framework. The role of risk assessments in overall disaster risk management is defined at the appropriate national and/or sub-national level.	
1.2	**Coordination:** A risk management structure assigns clear responsibilities to all entities involved in the risk assessment so that overlaps or mismatches between responsibility and capability are avoided
Q2.There are clearly defined responsibilities and roles/functions assigned to the relevant entities participating in the risk assessment	
	At the beginning of the NRA process, one authority must be designated for the task of coordinating the work
	(Political) risk criteria are set to determine whether the risk and/or its magnitude is acceptable or tolerable
	A political decision is made about the acceptability of risks and the prioritisation of risk prevention and preparation

Q3. The responsibilities for assessing specific risks are assigned to relevant entities	
Q4.The cross-sectoral dimension of risks has been integrated in the risk assessments	
	Risk assessments are linked to CCA strategies
	The risk assessments on other government levels and in different sectors are taken into account in the NRA
	The national government encourages and stimulates risk assessments by other levels of government and in different sectors
Q5. The distribution of responsibilities for the assessment of the risks regularly is reviewed	
1.3	**Other stakeholders:** Entities carrying out risk assessments cooperate with a range of stakeholders, including from the private sector, academia and other government entities not directly involved in the assessment process
Q7. The relevant stakeholders are involved in the risk assessment process	
	The risk assessment method is developed in cooperation with the relevant authorities, such as scientific communities, including social, health, economic and environmental sciences, practitioners, businesses, people at risk and policy-makers
	A stakeholder assessment is made before starting the risk assessment process and kept up to date (MiSRaR – Mitigation of Spatial Relevant Risks in European Regions and Towns) [The stakeholders (public, private and at different levels of government) to be involved in the assessment are identified and invited to participate]
	There is cooperation with the private sector where their risk assessments complement the efforts of public authorities
	The risk assessment is published and announced to stakeholders for consultation
	The stakeholders are informed on the particular risks they face
	Interested parties are consulted on flood-risk management plans at catchment level
	Flood maps and plans are made publicly available
2.	**Methodology:** A methodology is developed to carry out risk assessments. Expected impacts of identified risks are assessed according to an established methodology and risks prioritised accordingly
Q11. The national or sub-national entity has developed a methodology for risk assessment	
	The concept of 'risk' and the main factors of risk which have to be taken into account in the risk assessment are defined and accepted
	The scope or width of the risk assessment (and the justification for including or excluding specific risks) is defined and accepted
	A categorisation of types of risk is defined and accepted
	The scoring criteria for the risk assessment are defined and accepted
	The methods used for the risk assessment are defined and accepted
	A protocol for the use of expert opinions is defined and accepted
	The uncertainty of the methods is justified

	There is a listing of separate risks and risk scenarios, with their description
	For each risk, there is a separate risk map showing the spatial distribution of the hazard and the vulnerabilities
	The risk analysis includes probability and impact estimates, as well as a vulnerability analysis
	The impact analysis includes human, economic, environmental, political and social impacts
	The separate impact scores of each risk are recorded and justified, with clearly identified and substantiated assumptions
	The outcome of the risk analysis can be presented in a risk matrix for impact and probability
Q12. The cross-border dimension of risks has been integrated in the risk assessments	
	An (inter)national cooperation network for the formation of macro-regional risk analysis is established. Neighbouring countries are involved in the compilation of risk analyses and their risk analyses are taken into account.
Q13. The risk assessment considers CI.	
3.1	**Information and communication:** An effective information and communication system for the assessment of risk is available
Q9. The necessary administrative capacity is available at national and/or appropriate sub-national level to communicate internally the results of risk assessments, including scenarios, lessons learnt, etc.	
3.2	**ICT infrastructure:** The infrastructure and appropriate information is available to carry out the risk assessment
Q14. ICT infrastructure is available to carry out risk assessments	
Q15. Appropriate information and data (including historical data) are available to carry out risk assessments	
3.3	**Risk communication:** The necessary administrative capacity is available to communicate the results of risk assessments to the public.
Q8. The necessary administrative capacity is available to communicate the results of risk assessments to the public	
Q10. The results of risk assessments are integrated in a risk communication strategy	
	The risk assessment and the scenarios therein are published openly for the public
	Specific information is provided about the particular risks the population faces (in certain areas)
	The publication of the risk assessment includes an overview of the government's preparatory measures
	The publication of the risk assessment includes advice on how the general public could be better prepared
	The competent public body has decided which information from the NRA is sensitive and will therefore not be published

4.	**Expertise:** The experts carrying out the risk assessment have the requisite competencies and responsibilities and have received appropriate training
Q6. The experts responsible for the risk assessment(s) are adequately informed, trained and experienced in the assessment of risks	
5.	**Financing:** Financing includes the identification, estimation and setting-aside of funds required to carry out and update risk assessments
Q16*.* The appropriate financial capacity is available to carry out and update work on risk assessments	
6.	**Interface with risk management**: following the development of the NRA and maps, the authorities concerned should seek to interface in an appropriate way with the ensuing processes of risk management
	There is a plan or programme to perform a capacity analysis and develop capability planning on the basis of the NRA.
	The risk assessment results in specific recommendations for related policy fields.
	Agreement is reached on an implementation plan or programme.
	There is interconnection between national, decentralised and sectoral plans.