DISASTER RISK MANAGEMENT SUMMARY OF ESTONIA 2020

Part I. Risk assessment

1. Risk assessment process

Describe how the risk assessment process fits into the overall disaster risk management framework. Detail legislative, procedural and institutional aspects. Please, explain whether responsibility for the risk assessment lies at national level or at an appropriate subnational level.

Crisis management together with disaster prevention, preparedness and response are regulated on national level and is binded by a legal framework. Emergency Act, which was updated in the middle of 2017. URL: https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current.

In Estonia, the crisis management system, including the risk assessment process, is decentralised. It means that, the Ministry of the Interior is responsible for coordinating the crisis management policy on national level, but every authority and person is liable for the performance of crisis management duties in their area of activity (including assessing risks). Concerning the emergency risk assessment, the requirements for an emergency risk assessment and the procedure for the preparation of a risk assessment are established by a regulation of the Minister of the Interior responsible for the coordination of crisis management. Regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" issued by the Minister of the Interior is the legal basis. Due to decentralised crisis management system, the Government of the Republic establishes by a regulation a list of events that could lead to an emergency and that are subject to a risk assessment and designates the authorities in charge of preparing an emergency risk assessment (Emergency Act section (§) 9 subsection 1). The Government regulation annex 108: "List of events that could lead to an emergency and that are subject to a risk assessment, and the authorities in charge of preparing an emergency risk assessment"[1] establish following events and authorities, who are responsible to assess the risks:

1) rescue event – the Rescue Board;
2) police event – the Police and Border Guard Board;
3) cyber incident – the Information System Authority;
4) radiological or nuclear accident – the Environmental Board;
5) health care event – the Health Board;
6) infectious animal disease – the Veterinary and Food Board;
7) event caused by the malicious or terrorist use of chemical, biological, radiological or nuclear material (added May 2020) – the Internal Security Service.

In addition, in the Emergency Act section (§) 36 has set a list on vital services: electricity supply, natural gas supply, liquid fuel supply, operability of national roads, phone service, mobile phone service, data transmission service, digital identification and digital signing (eID), emergency care, payment services, cash circulation, district heating, operability of local roads, water supply and sewerage. Disruption of these services can cause emergency. It is a reason why all vital service providers have obligation to prepare continuity risk assessment and plan of a vital service. The requirements and procedure for a continuity risk

[1] Updated version is available only in Estonian: https://www.riigiteataja.ee/akt/130052020007?leiaKehtiv

assessment and plan of a vital service are established by a regulation of the Minister of the Interior – the regulation annex 29: "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan".

2. Consultation with relevant authorities and stakeholders

Describe the range of relevant authorities and stakeholders involved in the risk assessment process.
If appropriate: Describe the nature of their involvement, specifying their roles and responsibilities.

According to the regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" a risk assessment shall be coordinated with the authorities involved in the preparation thereof, the relevant ministry and the Ministry of the Interior. Secondly, when the emergency risk assessment has been coordinated, the head of the authority in charge shall approve it by a decree. Authorities in charge of an emergency risk assessment, having the most accurate overview of the risk factors as well as knowledge to involve all the relevant stakeholders, are also the authorities responsible for resolving an emergency. Finally, the approved risk assessment shall be sent to the Internal Security Service, the Foreign Intelligence Service and the Ministry of the Interior for their information.

The guidelines for preparing a risk assessment specify which other institutions have to be invited to participate in developing risk assessments to ensure that the effects of risks on other areas are assessed. Most of the authorities responsible for preparing emergency risk assessments involved more stakeholders in the process than stipulated by the guidelines. There is also cooperation and involvement of academia and other government bodies not directly involved in of Security Science, the Environmental Research the assessment process, such as the Estonian Academy Centre, vital service providers and the Red Cross. However, the Emergency Act does not clearly set out, how should be the private sector, NGOs and other stakeholders involved.

According to the Emergency Act section (§) 40 the continuity risk assessment and plan of the vital services must be approved by the authorities organising the continuity vital services (the Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, the Bank of Estonia or local governments).

3. Identifying the key risks at national or sub-national level

Identify the key risks that could have significant adverse human, economic, environmental and political/social impacts (including security).

From the above key risks, identify:
3.1 Any key risks which could have significant adverse cross-border impacts, coming from or affecting the neighbouring country or countries.
3.2 Any key risks with a low probability and high impact.

Where appropriate:
3.3 Identify any key risks expected in future. These may include any emerging risks that could have significant adverse human, economic, environmental and political/social impacts (including impacts on security).

According to the regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" a risk assessment shall consist of the general part, analysis, capability analysis and conclusions.

Analysis of a risk assessment shall present:

1) the event types that could lead to an emergency;
2) the definition of the emergency;
3) an analysis of the events that have taken place and national and international statistics, maps, forecast, expert assessment or other information which all support the analysis;
4) the event scenario and its description;
5) an assessment of the probability and consequences of the scenario;
6) the risk category of the scenario.

The authority in charge shall compile the information necessary for analysing an event and on the basis of the information obtained and an expert assessment shall prepare the probable worst-case scenario of the event which shall be supplemented by regional or other parts, if necessary. Several scenarios may be prepared for one event, if necessary. If it is discovered in the course of the analysis that the effects and consequences of two or more events are similar, the scenarios may be combined and one scenario may be prepared for the events.

When assessing the probability of a scenario, the relevant statistical data, surveys, analyses, expert assessments or other relevant information have to be taken into account. The probability of a scenario is assessed according to the probability assessment table:

Value in Words	very low	Low	average	high	very high
Criterion	less than once every 100 years	once every 50–100 years	once every 20–50 years	once every 5–20 years	more than once every 5 years

The consequences of a scenario is calculated using the following table:

Severity	1	2	3	4	5
Value in words	insignificant	minor	severe	very severe	catastrophic
I Life and health					
Deceased (number)	≤ 5	6−15	16−50	51−200	> 200
Injured or taken ill (number)	≤ 15	16−45	46−150	151−600	> 600
Evacuated (number)	≤ 50	51−200	201−500	501−2000	> 2000
II Property					
Direct financial cost (MEUR)	< 1	1−10	11−50	51−100	> 100
Indirect financial cost	insignificant	low	high	very high	catastrophic
III Natural environment					

Impact range (km^2)	< 1	1−10	11−100	101−1000	> 1000
Impact duration	<1 month	1−6 months	6–12 months	1–3 years	> 3 years
IV Vital services					
Number of services directly affected	0−1	2−3	4−5	6−7	≥ 8
Duration	< day	1−6 days	1–2 weeks	2 weeks to 1 month	longer than 1 month
Overall assessment of consequences (calculated)[2]					
Overall assessment of consequences (by decision of working group):					

In 2020, the authorities analysed all risks and 20 probable worst-case scenarios were created:

National risk assessment	No	Probable worst-case scenario	Cross-border impact	HILP risk[3]	Future risk
Rescue event	1	Flood together with storm	Yes	Yes	Yes
	2	Domino effect accident in enterprise liable to be affected by major accident	No	Yes	Yes
Police event	3	Mass Immigration	Yes	No	Yes
	4	Sudden attack in a public space	No	No	Yes
	5	Sudden attack in a passenger ship sailing in the Estonian rescue area	No	No	Yes
	6	Mass disorder	No	Yes	Yes
	7	Marine pollution (passenger ship and oil tanker accident in the Estonian rescue area)	Yes	No	Yes
Cyber incident	8	Interruption of eID service (security errors in the cryptographic algorithm)	No	No	Yes
	9	Interruption of eID service (eID interruption as an interruption of vital service)	No	No	Yes
	10	Violation of the integrity of the data essential for the functioning of the state	No	No	Yes
	11	Cyber-attack together with electricity blackout	No	No	Yes

[2] The overall assessment is calculated as the arithmetic mean.

[3] The probability was valued very low or low, but the consequences were valuated severe, very severe or catastrophic

	12	Interruption of data transmission service	No	No	Yes
	13	Major denial-of-service attack (disruption of critical services)	No	No	Yes
Radiological or nuclear accident	14	Nuclear accident in Loviisa or Leningrad Nuclear Power Plant	Yes	Yes	Yes
	15	Radiation accident in Estonia	No	No	Yes
Health care event	16	Epidemic	Yes	No	Yes
	17	Mass intoxication	No	No	Yes
Infectious animal disease	18	Outbreak of dangerous infectious animal disease	Yes	No	Yes
Event caused by the malicious or terrorist use of chemical, biological, radiological or nuclear material	18	Attack in a crowded place using biological materials	No	No	Yes
	19	Attack on a passenger ship using radiological/nuclear materials	No	No	Yes
	20	Attack a passenger plane using chemicals	No	No	Yes

According to the regulation annex 29: "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan" the continuity risk assessment of a vital service shall present:

1) description of minimum service level in every situation, including in emergency (based on organising authority´s requirements), number of users and the area of providing the service;
2) critical activities for providing vital service;
3) critical recourses for ensuring critical activities;
4) risks that could lead to an interruptions of the critical activity;
5) the probability of the risk and describing the consequences of an interruptions;
6) measures for preventing interruptions.

The authorities organising the continuity vital services shall establish requirements for the continuity of a vital service, including list of threats that have to be analysed in the continuity risk assessment (the Emergency Act section (§) 37 subsection 2). Example the Ministry of Social Affairs required that the emergency care providers have to analyse in their risk assessment threats like the interruptions of other vital services, epidemics, cyber-attacks, lack of stocks etc.

Estonia does not have European Critical Infrastructure, which is regulated by Directive on European Critical Infrastructure (2008/114/EC), therefore there is no direct cross-border impact to other Member States. The probability of the interruptions of vital services in Estonia is over average and depending from the vital service the consequences could be up to catastrophic.

4. Identifying climate change impacts

Determine which of the above-mentioned key risks are directly linked to climate change impacts. Please take into consideration the existing national and sub-national climate change adaptation strategy and/or action plans or any relevant climate risk and vulnerability assessments, where appropriate.

According to Estonian Climate Change Adaptation Development Plan until 2030, the climate change may cause following risks:

- Flood together with storm
- Epidemic
- Outbreak of dangerous infectious animal disease
- Mass Immigration
- Interruptions of vital services (example electricity or operability of national/local roads might be interrupted by storms, emergency care might be disrupted due to epidemic, drinking water might be not usable due to flooding etc.)

5. Risk analysis

Describe the scale of levels of probability and impact of the key risks identified (in Q3) including the key cross-border and key risks with a low probability and a high impact and, where appropriate, future and/or emerging risks. Display the results in a single risk matrix or other visualised graph/model as well, if applicable.
If appropriate: Outline the methods, models and techniques used to assess the probability and impacts of the different risks or risk scenarios.

A risk category is assigned for each scenario on the basis of the probability of its occurrence and the severity of the consequence according to following risk matrix:

		CONSEQUENCE				
PROBABILITY		**insignificant (1)**	**minor (2)**	**severe (3)**	**very severe (4)**	**catastrophic (5)**
	Very high	average	significant	high	very high	very high
	High	average	significant	significant	high	very high
	Average	Low	average	significant	high	high
	Low	Low	average	significant	significant	high
	Very low	Low	low	average	significant	high

In 2020, for all 20 probable worst-case scenario, both probability and consequences were assessed and a common risk matrix was formed. Results are shown in a following risk matrix:

		insignificant (1)	**minor (2)**	**severe (3)**	**very severe (4)**	**catastrophic (5)**
PROBABILITY	**Very high**			13) Major denial-of-service attack 18) Dangerous infectious animal disease	9) Interruption of eID service (as a vital service) 10) Violation of the integrity of the data	

	High			3) Mass Immigration 4) Sudden attack in a public space 15) Radiation accident 17) Mass intoxication	8) Interruption of eID service (security errors) 11) Cyber-attack with electricity blackout 12) Interruption of data transmission service 16) Epidemic 18) Attack with biological materials 19) Attack with radiological/nuclear materials 20) Attack with chemicals	
	Average				5) Sudden attack in a passenger ship	7) Marine pollution (passenger ship and oil tanker accident)
	Low			1) Flood together with storm		6) Mass disorder 14) Nuclear accident
	Very low				2) Domino effect accident	

6. Risk mapping

State whether any risk maps have been produced showing the expected spatial distribution of the key risks as identified at the identification and analysis stages (Q3, Q4 and Q5). If so, include them as appropriate.

- Flood hazards areas - https://xgis.maaamet.ee/xgis2/page/app/yua
- Inland waters (rivers and lakes) levels – https://www.ilmateenistus.ee/siseveed/vaatlusandmed/kaart/?lang=en
- Weather warnings – https://www.ilmateenistus.ee/ilm/prognoosid/hoiatused/?lang=en
- Snow thickness and ice - http://ilm.pri.ee/lumikatte-paksus-ja-j%C3%A4%C3%A4kaart (only in Estonian)
- Fire hazard - http://ilm.pri.ee/tuleohukaart (only in Estonian)
- Precipitation - http://ilm.pri.ee/sademetekaart (only in Estonian)
- Road condition - https://tarktee.mnt.ee/#/en

- Dangerous enterprises and enterprises with major hazard - https://xgis.maaamet.ee/maps/XGis?app_id=MA11AH5&user_id=at&LANG=1&WIDTH=980&HEIGHT=578&zlevel=0,552500,6505000
- Electricity interruptions - https://www.elektrilevi.ee/en/katkestused/katkestuste-kaart
- Telecommunication service interruptions - https://www.telia.ee/abi/service-status

7. Monitoring and reviewing risk assessment

Outline the system in place for monitoring and reviewing risk assessment so as to factor in new developments

Regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" stipulates that the authority in charge shall assess together with the authorities involved in the preparation of a risk assessment whether the risk assessment is up to date on a regular basis, but no less than once every three years and, if necessary, shall improve the risk assessment. The Ministry of the Interior supervises the preparation and updating of the risk assessments. If the authority in charge fails to start to renew the risk assessment, the Ministry of the Interior has the right to demand that the renewal of the risk assessment be started and the renewed risk assessment be presented.

Regulation annex 29: "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan" stipulates that the vital service provider shall assess whether a risk assessment and a plan are up to date at least once every two years or whenever critical activities, threats or other significant circumstances affecting the provision of the vital service change. The authorities organising the continuity of the vital services (the Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, the Bank of Estonia and local governments – roles specified in Emergency Act) have to supervise the preparation of continuity risk assessment and plan. If the service provider has failed to update the risk assessment and the plan, the organising authority has the right to demand that the service provider initiate the updating of the risk assessment and the plan.

8. Communicating risk assessment results

Describe the process of communicating and disseminating the results of the national risk assessment. Outline how the risk assessment results are shared among policymakers, various public authorities with different types of responsibility, different levels of administration, and other relevant stakeholders. State whether and how the general public is informed about the results of risk assessment, to make them aware of risks in their country or region and/or enable them to take informed decisions to protect themselves.

According to the Emergency Act, the Government of the Republic establishes by a regulation a list of those emergencies for which risk communication is organised and designates the authorities responsible for the organisation thereof. Risk communication for an emergency caused by an interruption with severe consequences or prolonged interruption of a vital service is organised by the authority organising the continuity of the vital service.

Risk communication means notifying the public of threats that could lead to an emergency and of the consequences of an emergency and giving people conduct instructions to raise awareness of and increase readiness for emergencies. After risk assessments have been approved, the authority responsible has to publish the risk form. The risk form shall include short description of the scenarios analysed, what are the probabilities and consequences of the scenarios analysed, and share practical advice how to prepare and how to behave in crisis

(codes of conduct). The authority in charge shall publish the risk form on the authority's website no later than within two weeks as of the approval of the risk assessment and shall introduce the most important conclusions of the risk assessment to the public. The authorities are also organising regularly various risk communication campaigns on media (TV, the press), social media, share various information leaflets/publications etc.

In 2018 Government Office of Estonia in cooperation with the Ministry of the Interior prepared the concept of civil protection. One part of this conception is increasing public awareness and therefore the Ministry of the Interior developed a unified risk communication platform: https://www.olevalmis.ee/en, where all authorities can notify the public of the threats and share codes of conduct, and the mobile app is available.

In addition, the risk assessment results are also presented to the Crisis Management Committee of the Government of the Republic, which is chaired by the Minister of the Interior and the members are permanent secretaries of ministries, directors general of government authorities and representatives from Government Office and Defence Forces. The Rescue Board, who is general civil protection authority, together with other competent authorities share risk assessment results to the regional and local level.

Part II. Risk management capability assessment

9. Legislative, procedural and/or institutional framework

Describe the framework in place for the risk management capability assessment process(es). State whether it is based on a legal act, a strategic plan, an implementation plan or other procedural frameworks.
If appropriate: State how often risk management capability is assessed. State whether the risk management capability assessment(s) is used for decision-making purposes.

The risk management capability assessment is one part of the risk assessment process, which is regulated by the Emergency Act and its sub-acts.

Regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" stipulates that a national capability analysis shall be prepared for each scenario. The capability analysis shall describe:

1) the activities necessary to prevent, prepare for and resolve an emergency (including the activities related to managing an emergency, protecting the people in danger and risk communication), and for each activity shall be analysed:
    - the existence and sufficiency of technology and equipment, including operation stock;
    - the existence and sufficiency of the personnel necessary to resolve the situation;
    - the existence of the skills and knowledge necessary to resolve the situation and, if necessary, the need for training;
    - whether rules and instructions exist and are up to date.
2) the readiness and existing capabilities of the authorities resolving the emergency and the related parties;
3) the capability caps;
4) measures for overcoming the capability caps;
5) the estimated cost of the measures;

6) authorities liable for compliance with the measures.

National risk management capability is assessed together with national risk analyse no less than once every three years or whenever if some capability or other significant circumstances change. Risk management capability assessment is also one of the input for planning the annual state budget.

Regulation annex 29: "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan" stipulates that for every critical activity[4], the service provider shall identify the resources indispensable for the functioning thereof and when identifying the critical activity resources, the service provider shall proceed from the following types of resources:

1) staff – the optimum and minimum number of staff necessary for the functioning of the critical activity and which skills and knowledge must the staff have;
2) buildings and territory – which buildings and territory are indispensable for the functioning of the critical activity and which alternative building or territory can be used;
3) pieces of equipment and information technology systems – which pieces of equipment and information technology systems, including databases and communications systems, are important to the functioning of the critical activity;
4) information necessary for the functioning of the critical activity – which information is necessary for the functioning of the critical activity and how is it stored;
5) funds – what are the service provider's everyday funds for the functioning of the critical activity;
6) other services, including vital services – the interruption of or interference with which other services may affect the functioning of the critical activities of the service provider;
7) suppliers and partners – who are important suppliers and partners on whom the functioning of critical activities depends.

The risk management capabilities of the vital service providers is assessed together with risk analyse no less than once every two years or other significant circumstances change. The risk management capabilities of the vital service providers is also one of the input for planning companies budgets for investments, staff, trainings etc.

10. Roles and responsibilities of the competent authorities

Describe the roles and responsibilities of the competent authorities at national or sub-national level (as appropriate), distinguishing between risk assessment, prevention, preparedness, and response, and focusing on the management of the key risks identified. Describe how horizontal coordination (the cross-sectoral approach) is ensured among these competent authorities, focusing on the management of the key risks identified.

The Ministry of the Interior is responsible for coordinating the crisis management policy on national and horizontal (cross-sectoral) level, but every authority and person is liable for the performance of crisis management duties in their area of activity (including assessing the risk management capabilities).

[4] Critical activity means the activities of a service provider, the lack of which leads to an interruption of or interference with the vital service.

The Government of the Republic has designated the authorities in charge of preparing an emergency risk assessment together with the risk management capability assessment (the Rescue Board; the Police and Border Guard Board; the Information System Authority; the Environmental Board; the Health Board; the Veterinary and Food Board; the Internal Security Service). The risk assessments (including capability assessment) shall be coordinated with the authorities involved in the preparation of the risk and capability assessment, the relevant ministry and the Ministry of the Interior.

The Emergency Act has set a list on vital services and designed the service providers, who shall prepare continuity risk assessment (including capability assessment) and plan of a vital service. The authorities organising the continuity vital services (the Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, the Bank of Estonia or local governments) must approve provider's risk and capability assessment.

11. Roles of relevant stakeholders

State whether relevant stakeholders are informed about and involved in the disaster risk management process(es) for the key risks identified. If they are, describe how.

Estonian national risk assessments are carried out in close cooperation with the relevant stakeholders as described in Q10. Stakeholders, who are directly not involved, receive information through risk communication as described in Q8.

12. Procedures and measures at national, sub-national and local level

Describe the established procedures to ensure vertical cooperation between the national, sub-national and local level authorities involved in disaster risk management process(es) for the identified key risks.

According to the Emergency Act, there is three-level crisis management committee system for organising crisis management, including introducing results of risk and capability assessment and planning activities/measures.

The Crisis Management Committee of the Government of the Republic has been formed at national level. The chair is the Minister of the Interior and the members are permanent secretaries of ministries, directors general of the government authorities and representatives from the Government Office and the Defence Forces. The Crisis Management Committee of the Government coordinates the performance of the crisis management duties of authorities of executive power, where necessary imposes on them duties for preventing and preparing for emergencies and monitors the performance of duties imposed.

Four regional crisis management committees have been formed at regional level. The chairs are the heads of the Rescue Board regional offices and the members are representatives from other governmental authorities' regional offices and local authorities. The regional crisis management committees coordinates in their region the performance of crisis management duties of regional structural units of authorities of executive power and local authorities.

79 crisis management committees of local authorities have been formed at local level. The chairs are the rural municipality's mayors or the city´s mayors. The crisis management committees of local authorities coordinates crisis management within the local authority; submits to the regional crisis management committee annual summaries of the

activities of the crisis management committee of the local authority and the schedule of work for next year.

13. Procedures and measures at cross-border, inter-regional and international level

Describe the procedures established to ensure cooperation at the cross-border, inter-regional and international levels for the disaster risk management of identified key risks. Describe measures in place to ensure disaster risk management for the key risks identified. If appropriate: State whether disaster risk management policies are developed in a way that takes account of international commitments, such as the 2015-2030 Sendai Framework for Disaster Risk Reduction and the Sustainable Development Goals of the 2030 Agenda for Sustainable Development.

Internationally Estonia is committed to the UN Sendai Framework and of course to the SDGs of the 2030 Agenda for Sustainable Development. Additionally, Estonia is part of several regional cooperation frameworks in disaster risk reduction and civil protection via our Rescue Board, such as the Council for Baltic Sea States (CBSS). Not to mention, we are part of the EU commitments through the UCPM. In Estonian policy planning we derive largely from the OECD and NATO suggestions, for instance the OECD' Natural Hazard Awareness and Disaster Risk Reduction, Risk Communication Guidelines and NATO' Civil Preparedness instructions.

14. Focus on climate change adaptation measure

State whether synergies between disaster risk reduction and climate change adaptation measures are established at national or subnational level (as appropriate) for the key risks identified that are linked to climate change (Q4). If so, describe how.

Risk management planning, including risk reduction, is part of different strategies and action plans (e.g. national strategy for adaptation to climate change, flood risk management plans, the national emergency plan for epidemics, etc.). Such strategies and plans are prepared in cooperation between different institutions by the relevant experts. The Estonian Climate Change Adaptation Development Plan until 2030 are a good example of risk management planning. The strategy was prepared by the Environmental Research Centre in cooperation with the Environmental Board and the Norwegian civil protection authorities, with the financial support of the EU. The plan sets out the different areas of responsibility and the budget required to implement the strategy is under development. The results included national climate change scenarios, which is taken into account also in risk assessment. The action plan prioritises policy fields such as spatial planning, infrastructure, health, etc. Experts planning the prevention and preparedness are informed about the policy goals and priorities mostly via information shared at the interministerial in working groups.

15. Focus on critical infrastructure protection measures

State whether there are measures in place to protect critical infrastructure regarded as relevant for the continuation of vital societal functions.

The Ministry of the Interior has developed guidelines for preparing vital service risk and capability assessments and action plans. The requirements and procedure for a continuity risk assessment and plan of a vital service are established by a regulation of the minister responsible for the coordination of crisis management. Regulation annex 29 "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan". Estonia does not have any infrastructures that

would qualify as European Critical Infrastructure. However, Estonia has introduced the term "vital service" into domestic legislation. A vital service is a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health of people or to the operation of another vital service or service of general interest. A vital service is regarded in its entirety together with a building, piece of equipment, staff, reserves and other similar facilities indispensable to the operation of the vital service.

The methodology for the emergency risk assessment considers the aspects of vital services by analysing an emergency's consequences on the continuous operation of vital services (all 14 vital services). In addition, if it is necessary governmental institutions shall give advice for vital service providers. Vital services providers must take into account their dependencies on other services and public part of national risk assessment results.

16. Source(s) of funding

State whether the budget allows for resources to be allocated flexibly in case of urgent need and to what extent disaster funds promote preventive action. Describe the funding sources used (e.g. national, sub-national, public, private, including insurance, EU and other international funding) to take priority measures in the field of disaster risk management when assessing, preventing, preparing for and responding to the key risks identified.

Budgeting for risk management covers a 4-year period and focuses on the main topics laid down by the Government. The annual state budget is more detailed, but does not allocate separate funds to crisis management because each ministry is responsible for planning sufficient human and financial resources for crisis management in its own area of responsibility. Measures indicated in national risk assessments (like capacity gaps) include estimated costs, however additional applications from the state budget have to be lodged in case of larger cases. If the amount is smaller, usually the financing comes from the authority' budget. State reserve is used only in case of emergencies.

National planning includes also EU and other international funding for instance DG HOME ISF, but also Structural Funds. Additionally, national authorities responsible for DRR can apply for specific funding's and grants like the ones open under the UCPM annual work programme. So far there have been a few exercises organised via the UCPM grants like CREMEX 2011, but last year (2020) Estonian Rescue Board and the MOI both applied for a specific prevention and preparedness grant under the Track 1 projects, and both of them were successful.

17. Infrastructure, assets and equipment

Describe what is done to ensure that enough assets are available to mitigate the impact of disasters and respond promptly to disasters associated with the key risks identified.

Regulation annex 28: "Requirements for an emergency risk assessment and procedure for the preparation of a risk assessment" stipulates that the national capability analysis shall identify among other things if there is sufficient technology and equipment, including operation stock, to prevent, prepare and resolve an emergency. If there are capability caps, then the measures for overcoming the capability caps shall be planned and the authorities liable for compliance with the measures shall be designated. Risk management capability assessment is also one of the input for planning the annual state budget.

Regulation annex 29: "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan" stipulates that vital service provider shall identify among other things if there is sufficiently buildings and territory/infrastructure and equipment to ensure that the service is provided in all situations (including in emergency). The risk management capabilities of the vital service providers is also one of the input for planning companies budgets for investments.

18. Focus on disaster loss data collection and procedures

State whether a system is in place to collect disaster loss data. Describe how data is collected on the key risks identified.

For each national risk assessment, the authority required to prepare the risk assessment currently collects its own data and analyses the data using its own database(s) and/or ICT infrastructure. The authorities gather risk-monitoring data and information about incidents and analyse it. There is no centralised database or interface that could be used to combine individually gathered information. Therefore, each participating institution uses its own data for the risk assessments, which it collects using its own methods. Example under the Rescue Act, the Ministry of the Interior has to establish a database called the 'rescue information system'. One of the six obligatory datasets focuses on supervision and prevention work. The Rescue Act determines:

- which institutions have the right to obtain data from the rescue information system;
- which dataset has to be available for these institutions; and
- why data are needed.

The following institutions have the right to obtain data from the specific datasets of the rescue information system: the Emergency Response Centre, the MoI, the Police and Border Guard Board, the Health Board, prosecutors' offices, the Ministry of Economic Affairs and Communications, the Technical Surveillance Authority and the Roads Administration. Data gathered for the rescue information system have multiple purposes, including for risk assessments, assessing resources, evaluating the effectiveness of prevention measures and planning new ones.

The same principle applies also for collecting the vital service interruptions data.

19. Focus on early warning systems equipment and procedures

Describe the systems in place for early hazard detection and monitoring of the key risks identified. State whether forecasting methodologies are integrated into the system.

Estonian national risk assessments concluded that early warning procedures together with preventive early warning systems are needed. One of the solutions that was given, was an sms-alert system that shall reach a wider range of people. Additionally, enterprises that are prone to a higher disaster risk have to have functioning alert systems on their own territory.

20. Risk information and communication to raise public awareness

Describe how the public is informed of what action to take when facing risks. For example, state whether a strategy is in place to educate the public and raise awareness. State whether and how target groups are involved in the definition of prevention and preparedness measures and in the implementation of the risk information and communication activities.

Described in Q8.

Part III. Priority prevention and preparedness measures addressing key risks with cross-border impacts and, where appropriate, low probability risks with a high impact

21. Key risks with cross-border impact
List the key risks with cross-border impacts.

- Flood together with storm;
- Mass Immigration;
- Marine pollution (passenger ship and oil tanker accident in the Estonian rescue area);
- Nuclear accident in Loviisa or Leningrad Nuclear Power Plant;
- Epidemic;
- Outbreak of dangerous infectious animal disease.

For each key risk with cross-border impacts, please complete the following box:

22. Priority prevention and preparedness measures
22.1 Describe existing priority prevention measures and any that are planned.
22.2 Describe existing priority preparedness measures and any that are planned. If EU legislation or policies already require reporting on priority prevention and preparedness measures addressing this risk, please simply refer to any reports already sent to the Commission.

Prevention and preparedness measures for scenario "Flood together with storm"
Each EU Member State, including Estonia, is obliged to implement the Flood directive (2007/60/ec) on the basis of river basin districts; this is complemented by the initial estimate on risks related to the danger of flood, danger lists and risk charts, as well as management plans. The initial estimate on flood-related risks, maps on the danger of flood and the respective risk areas, and the management plan on flood-related risks will be reviewed and, if necessary, updated every six years, while updating river basin management plans. Estonia has established the River Basin Management plans for 2016-2021 and is currently in the middle of updating process.

Prevention and preparedness measures for scenario "Mass Immigration"
To prevent and prepare for the mass immigration the leading authority (the Police and Border Guard Board) together with other involved parties is monitoring the situation 24/7 for early warning; is ready to strengthen border controls if necessary; is raising public awareness of potential risks; is ready to respond to the crisis 24/7; has cooperation agreements to involve external assistance (FRONTEX, EASO, UNHCR); is organizing exercises and trainings.

Prevention and preparedness measures for scenario "Marine pollution (passenger ship and oil tanker accident in the Estonian rescue area)"
To prevent and prepare for the marine pollution the leading authority (the Police and Border Guard Board) together with other involved parties is monitoring the situation 24/7 for early warning; is conducting surveillance flights to detect pollution at sea and in transboundary waters; is raising public awareness of potential risks; is ready to respond to the crisis 24/7; is

ensuring marine pollution modeling capacity; has cooperation agreements to involve external assistance (IMO, HELCOM, ERCC); is organizing exercises and trainings.

Prevention and preparedness measures for scenario "Nuclear accident in Loviisa or Leningrad Nuclear Power Plant"
The prevention measures are not available, because the scenario does not start from Estonia, but it will affect Estonia and other countries. To prepare for the nuclear accident in Loviisa or Leningrad the leading authority (the Environmental Board) together with other involved parties is ready to give early warning of radiation risks (monitoring the situation 24/7, information exchange with IAEA and ECURIE); is preparing risk assessments of the current situation; is raising public awareness of potential risks; is ready to respond to the crisis 24/7; has cooperation agreements to involve external assistance; is ready to give psychological assistance; is organizing exercises and trainings.

Prevention and preparedness measures for scenario "Epidemic"
To prevent and prepare for the epidemic the leading authority (the Health Board) together with other involved parties is conducting epidemiological surveillance of communicable diseases; is monitoring the situation (information exchange with ECDC and IHR); is organising vaccination of the population (especially children) by the state on the basis of an immunization plan; is raising public awareness of potential risks; is increasing ability for laboratory detection of infectious diseases; is coordinating healthcare providers readiness to response to the epidemic; is ensuring the availability of state stocks; is ready to respond to the crisis 24/7; has cooperation agreements to involve external assistance (ERCC); is organising exercises and trainings.

In addition, both the food business operator and the drinking water operator have a legal obligation to provide food and drinking water safety.

Prevention and preparedness measures for scenario "Outbreak of dangerous infectious animal disease"
To prevent and prepare for outbreak of dangerous infectious animal disease the leading authority (the Veterinary and Food Board) together with other involved parties is monitoring the situation (requests information from OIE and ADNS databases); is preparing prepares risk assessments of the current situation; is supervising imports of goods subject to veterinary and food controls; is conducting surveillance studies to detect infectious animal diseases; is raising public (incl. farmers) awareness of potential risks; is ready to respond to the crisis 24/7; has cooperation agreements to involve external assistance (Nordic-Baltic Veterinary Contingency Group); is ready to give psychological assistance; is organising exercises and trainings.

Where appropriate:

23. Low probability risks with a high impact
List any low probability risks with a high impact.

- Flood together with storm;
- Domino effect accident in enterprise liable to be affected by major accident;
- Mass disorder;
- Nuclear accident in Loviisa or Leningrad Nuclear Power Plant.

For each low probability risk with a high impact, please complete the following box:

24. Priority prevention and preparedness measures

24.1 Describe the existing priority prevention measures and any that are planned.

24.2 Describe the existing priority preparedness measures and any that are planned. If EU legislation or policies already require reporting on priority prevention and preparedness measures addressing this risk, please simply refer to any reports already sent to the Commission.

Prevention and preparedness measures for scenario "Flood together with storm" are described in Q22.

Prevention and preparedness measures for scenario "Domino effect accident in enterprise liable to be affected by major accident"

To prevent and prepare for domino effect accident the leading authority (the Rescue Board) together with other involved parties is supervising the risk management and planning of dangerous enterprises and enterprises with major hazard; is assessing the risk of a domino effect and inform relevant stakeholders (incl. enterprises); is approving investment plans of dangerous enterprises and enterprises with major hazard; is raising public awareness of potential risks; is ready to respond to the crisis 24/7; is organising exercises and trainings; is preparing for mass evacuation.

Prevention and preparedness measures for scenario "Mass disorder"

To prevent and prepare for the mass disorder the leading authority (the Police and Border Guard Board) together with other involved parties is monitoring the situation 24/7; is profiling of persons entering and leaving the country at international transport hubs; is applying randomly Schengen compensatory measures; is raising public awareness of potential risks; is ready to respond to the crisis 24/7; has temporary detention facilities for detainees; is ready to detect unmanned aircraft; is organising exercises and trainings.

Prevention and preparedness measures for scenario "Nuclear accident in Loviisa or Leningrad Nuclear Power Plant" are described in Q22.