Summary of the project "Study Mapping the Factors which Influence the Provision of Vital Services"

November 2016

Brief overview

This document is a summary of the project "Study Mapping the Factors which Influence the Provision of Vital Services", commissioned by the Estonian Information System Authority (RIA). The study was conducted from the EU structural funds support scheme "Raising Public Awareness about the Information Society", funded by the European Regional Development Fund.

The main objective of the study is to raise national awareness about important information technology-related cross and foreign dependencies influencing the continuous operation of vital services and to gain an overview of the existing alternative solutions (e.g. the capability of manual control, backup power sources, duplicated data communication service), continuous operation plans, the realisation of information technology risks, and the capability of restoring an interrupted provision of vital services. During the study, the existing processes and alternative solutions of 24 vital service providers were analysed in order to gain an overview of the assurance of the continuous operation of the services in the event of a possible interruption of the service.

As a result of the work, we prepared a mapping of the vital services necessary for the functioning of the state, where we highlighted the most important information technology-related cross dependencies of the services in Estonia and foreign dependencies outside Estonia, along with the related components of information and communications technology (ICT). We mapped the possible risks which may influence the provision of vital services in the Republic of Estonia. We ascertained the institutions which are able to ensure the provision of services with alternative solutions if the risks are realised.

The study also focused on information technology-related operating and supporting systems. An analysis of mission-critical services, infrastructure, and other components necessary for the provision of vital services was conducted in order to identify possible dependencies and threats arising from external service providers, both in and outside the Estonian territory.

Target group of the study

In conducting the study, KPMG was guided by the definition and obligations for ensuring the continuous operation of vital services provided in the Emergency Act (adopted on 15 June 2009, RT I 2009, 39, 262), the study included vital services and their providers defined in the Emergency Act. The target group included 12 areas of vital services and two service providers from each field, whose impact was considered important by the contracting entity.

The target areas of vital services were:

- power supply (production, core network, distribution network);
- natural gas supply (core network, distribution network);
- liquid fuel supply;
- drivability of national and local roads;
- telecommunication services (telephone, mobile phone, data communication);
- health services (emergency care);
- financial services (payment service, cash circulation);
- district heating supply;
- functioning of water supply and sewerage;
- functioning of the rail transport service (including carriage of passengers and goods);
- functioning of harbours, organisation of vessel traffic;

- functioning of air navigation services and airports.

The target group of vital services have a significant impact from the perspective of the state. The services are consumed by or an interruption in the provision of the services indirectly influences the entire population of the state.

The work conducted can be divided into three main stages:

1) preparatory activities;
2) conducting interviews at the providers of vital services;
3) substantive qualitative analysis.

- **Preparatory activities**

In the course of the preparatory activities, the legislative environment and requirements for the assurance of the continuous operation of the services established for the vital service providers were examined. In addition, interviews with the responsible employees of three chosen authorities organising the continuous operation of vital services were conducted.

- **Interviews**
  - Interviews with the responsible employees of three chosen authorities organising the continuous operation of vital services.
  - Interviews with the employees of the authorities responsible for providing vital services.
  - Interviews were not recorded; the content of the interviews were documented on site.
  - The interview protocols were confirmed by the interviewees right after the interviews were conducted. 24 authorities and 62 persons participated in the interviews.
  - The interviews were conducted in the rooms of the vital service providers.
- **Substantive analysis**
  - The documents of the vital service providers (including risk analyses and plans for continuous operation) were analysed. A request for documents was carried out in cooperation with RIA, the analysis was conducted in the rooms of RIA.

The main observations revealed in the course of the study, which, according to our estimation, have the greatest impact on the continuous operation of vital services and to the handling of which high priority should be assigned:

- 37% of the surveyed enterprises only use activity-based risk assessment, in the course of which, IT risks are assessed only on a general level.
- Only 33% of the enterprises have updated their risk analysis and continuous operation plans of vital services after 1 January 2015.
- By areas, information security risk management is well organised in enterprises of electricity supply, telecommunications, and financial services.
- None of the enterprises that took part in the study confirmed full compliance with the requirements of the IT Baseline Security System ISKE or the ISO 27001 standard.
- We ascertained that at the time the interviews were conducted, ICT-related foreign dependency existed in 29% of the vital service providers out of all the participants in the study; in 8% of the enterprises, to a significant extent and in 21%, to a critical extent. Therefore, all the study participants, where the foreign dependency of a vital service exists,

had assessed the accompanying risks for themselves. However, as there is a lack of a unified methodology, the level of documentation of foreign dependencies is different.

- Among the providers of vital services, that are dependent on ICT, which is located in a foreign country, 57% of the providers of vital services are able to ensure the provision of vital services with alternative solutions.
- 12.5% of the providers of vital services who participated in the study are in conflict with the requirement of subsection 40 (1^1) of the Emergency Act, which prescribes that if information systems ensuring the operation of a vital service are located in a foreign country, the provider of the vital service is required to ensure the continuous operation of the vital service also in a manner and by means not dependent on information systems located in foreign countries.
- None of the vital service providers have assessed ICT-related cross dependencies in sufficient detail.
- 70% of the vital service providers that participated in the study have not given their assessments regarding cross dependencies in their risk analyses by all areas included in the sample of the study.
- All the providers of vital services are dependent on electricity supply (88% consider dependency on electricity supply critical, 12% important).
- All the providers of vital services are dependent on communication, whether it be phone communication, mobile phone communication, or data communication (46% consider dependency on communication critical, 50% important).

The following may be highlighted as the main weaknesses:

- Shortage of technical facilities for providing the service by using alternative solutions in the case of an interruption.
- Risk analyses have been prepared inconsistently and in a different level of detail.
- Authorities organising the continuous operation of vital services have not determined service level requirements.
- Insufficient central coordination and preparation for crisis situations by the state.
- Small number of scenario-based joint trainings, which include different parties, such as providers of vital services.
- Currently, not enough preparations have been made for long-term blackouts.
- Necessity to train persons who are responsible for risk analyses and continuous operation plans preparation for the providers of vital services.
- Necessity to raise awareness among the providers of vital services in the field of risk assessment, cyber risk assessment, etc. (from the management to the specialist level).
- Providers of vital services find that the state needs to contribute more to the assurance of the provision of vital services and risk analysis.
- Currently, there are no common information technology solutions for the operative exchange and storage of documents. The process is time-consuming and there is no assurance that the documentation held by an authority organising the continuous operation of vital services and RIA reflects the current situation of the providers of vital service.
- There are no common information technology solutions for assessing the dependencies of vital services. Information must be collected separately for each provider of vital service, using documents previously prepared by that provider of vital service and/or making inquiries regarding this from the responsible persons of the provider of vital service.

- In future projects, the authority organising the continuous operation of vital services and/or RIA need to analyse the further dependencies of a provider of vital service on their subcontractors and organisations offering ICT-related services to the providers of vital services, because the providers of vital services have not assessed these dependencies in sufficient detail at the time of the study.

Recommendations and observations of KPMG

We would like to highlight the following observations revealed in the course of the study, which, according to our estimation, have the greatest impact on the continuous operation of vital services and to the handling of which high priority should be assigned:

- It was revealed that all the providers of vital services depend on electricity supply. 88% of the surveyed companies consider the dependency of their vital service on electricity supply critical, without which they could not provide the service and for which offering a long-term alternative solution is impossible. Autonomous battery supply systems are activated in the case of a blackout. Providers of vital services are able to temporarily ensure electricity supply in the most important places of consumption by using electric generators, but it is impossible to offer the service long-term and to all consumers. The supply of providers of vital services with electric generators is inconsistent. We recommend first preparing plans for authorities organising the continuous operation of vital services and then, on the national level, supplying high-priority places of consumption necessary for the provision of vital services with electric generators and a fuel reserve necessary for long-term (more than 12 hours) blackouts;
- We ascertained in the course of the interviews that the contribution of the organisers of the continuous operation of vital services to the assurance of the continuous operation of vital services is very inconsistent, depending on the field. We recommend that the authorities organising the continuous operation of vital services recheck that the parameters of the providers of vital services meet the requirements arising from the legislation (maximum time of service interruption, allowed recovery time, etc.) If there are no requirements, the authority organising the continuous operation of vital services should set them. If the requirements are not determined by the vital service providers or they are not in accordance with the aforementioned requirements, the provider of vital service should obtain the relevant information for the input of their continuous operation plans from the authority organising the continuous operation of vital services. Providers of vital services expect more wide-ranging assistance from the authorities organising the continuous operation of vital services in order to perform the duties related to continuous operation set for the providers of vital services by law;
- We found that providers of vital services implement security measures in risk analysis and storing continuous operation plans on very different levels. The risk analyses and continuous operation plans of vital services include sensitive information, to which access should be restricted. We recommend that the providers of vital services classify these documents as confidential and implement measures for their safe management and storage. More attention should be paid to information security measures when giving out the documents and their compilation by authorities organising the continuous operation of vital services, the Ministry of the Interior, and other related authorities;
- We ascertained that at the time when the interviews were conducted, providers of vital services had critical foreign dependencies on information systems located in foreign countries. As a result, there is a conflict with the requirement of the Emergency Act, which establishes that the provider of the vital service is required to ensure the continuous operation of the vital service also in a manner and by means not dependent on information systems located in foreign countries.

Recommendations for rectifying deficiencies of foreign dependencies

- The authority organising the continuous operation of vital services in cooperation with RIA and the Ministry of the Interior should agree upon which part of the activities of a provider of vital service is classified as vital services and which services are necessary with regard to public interest and commercial objectives. Specific requirements related to continuous operation and availability should be defined for vital services by the legislation;
- Favourable conditions should be created for providers of vital services for hosting information systems related to the provision of vital services in the planned state cloud.

Recommendations for rectifying deficiencies of cross dependencies

- Providers of vital services should additionally analyse, for which sites electricity supply is critically important. If there is no generator on site, there should be a plan, from whom electric generators could be temporarily borrowed. The study team feels that for this, the Ministry of Economic Affairs and Communications and other authorities organising the continuous operation of vital services should have the relevant information and agreements, so that they could react in a timely manner and help the providers of vital services;
- The providers of vital services, who participated in the study and whose dependency on communication links are critical, should ensure double communication links or connections at their most important sites. The organisers of the study find that each provider of vital service should regularly assess the risks resulting from the interruption of data communication connection and the impacts of the realisation of the risk. The double connection links should be set up in such a manner that they are not dependent on one communications service provider or cables in one communications network. If there is risk of interruption of a local cable communications connection, it may be practical to use a mobile data communications network as a backup option. Possible risk scenarios should be outlined in cooperation with authorities organising the continuous operation of vital services, RIA, and the Ministry of the Interior, which the providers of vital services could test either independently or in the course of organised joint trainings. We recommend that the authorities organising the continuous operation analyse establishing requirements of double data communication connections for the sites necessary for the provision of vital services. If necessary, proposals for preparing or updating the relevant legal acts should be made on the state level.

Recommendations for the action plan of the state:

1. Ensure that all the necessary and affected parties (should be previously fixed in the continuous operation documents by the providers of vital services and the authority organising the continuous operation of vital services) are aware of the relevant information that has been verified by the authority organising the continuous operation of vital services regarding interruptions in the service of a provider of vital service, including the realisation of IT risks, which results in a discontinuance of the work of ICT components.
2. If necessary, offer assistance to a provider of vital service after the recovery of service interruption for the collection of more information regarding the performed activities, and allow preparing a primary general incident report by electronic means.
3. Incident report analysis in cooperation with the provider of vital service, further investigation of the cause of interruption. Preparing a scenario for avoiding future interruptions (risk assessments and state scenarios, which the providers of vital services should consider); if necessary, prepare recommendations for changing the processes. The state can offer extra resources for sharing experiences.

4. Confirming amendments to the recommended action plan on the level of the management of the provider of vital service. The provider of vital service should appoint a person in charge, who will be responsible for implementing improvement activities. The state could offer support to the provider of vital service for implementing the necessary amendment to the process and simultaneously begin implementing activities related to the amendments by the state.

Recommendations for the systematic management of materials (risk analyses, continuous operation plans, plans resolving emergency situations, etc.) prepared by the providers of vital services:

- **We recommend considering the creation of a common safe electronic environment. In the created environment, state authorities related to organising vital services (authorities organising the continuous operation of vital services and other relevant authorities) can see the latest versions of the documents and use the input of other providers of vital services for analysis.** As the information included in the risk analyses and continuous operation plans is sensitive and confidential, special attention should be given to implementing information security measures in the created environment. We recommend separating the created environment from the external network in order to avoid possible risks. **Before commencing development works, we recommend carrying out a separate analysis for identifying the benefits and possible additional security risks arising from creating the respective environment.**
- **We recommend creating a centrally managed table of ICT component dependencies of providers of vital services, which includes the ICT components of their subcontractors in addition to the providers of vital services. Not all subcontractors may be providers of vital services but the service they provide may affect the functioning of the ICT components of a provider of vital service to a significant extent; therefore, an assessment should also be given to the security of the subcontractors systems.** A centrally managed structure helps to ensure that the information is documented on uniform conditions.
- A safe encrypted channel should be created for providers of vital services for uploading documents and the use of all other communication channels should be forbidden (e.g. sending continuous operation plans as an e-mail attachment, since providers of vital services may forget to encrypt the document);
- All risk analyses and continuous operation plans that include activities related to third parties (partners, other service providers, state authorities) should be shared with the corresponding parties to the extent which reflects the activity of that party. An authority organising the continuous operation of vital services should have the full documentation with the latest upgrades at any given time;
- In order to allow the assessment and planning of operation stockpiles necessary for the functioning of vital services in an emergency, a common form should be prepared for providers of vital services for submitting the respective plan and application about to what extent and which resources are needed in the case of a long-term interruption of a vital service. In order to optimise the use of resources, these plans should be managed and resources shared centrally based on previously fixed conditions (including price agreements) and pursuant to the priorities set by the state;
- An information system may be created for the management of the cross and foreign dependencies of vital services and their components that would allow analysing the connections between different services and components necessary for the provision of

services. In addition, the corresponding system should allow visualising different connections. **Considering the weaknesses revealed as a result of this study in describing, documenting, and analysing the dependencies of vital services, it can be concluded that creating this system is necessary.**

Contact information

Teet Raidma
Head of IT counselling services
+372 6 676 814
traidma@kpmg.com

KPMG Baltics OÜ
Narva mnt 5
10117 Tallinn
Estonia

Tel. +372 6 268 700
Fax +372 6 268 777

www.kpmg.com