Implementation of system of IT security measures in local governments

Is the security of data entrusted to local governments guaranteed as required?

Summary of audit results

What did we audit?

Audited local governments	
Kuusalu	Võru
Rapla	Audru
Viljandi	Kohtla-Järve
Paide	Avinurme
Valga	Vihula

The National Audit Office audited whether the data entrusted to local governments were kept securely. This involved an examination of activities both at the local government and state level. The planning of IT security and the compliance with established requirements (e.g. data backups, password use, managing user rights, performing security updates, virus protection) was assessed in 10 local governments.

In the case of four national databases, the auditors analysed what the chief administrator of the database had done to guarantee the security of data exchange in which the local government engaged. These databases were the Population Register maintained by the Ministry of the Interior, the e-File of the Ministry of Justice, the Estonian Education Information System (EHIS) of the Ministry of Education and Research and the Address Data System (ADS) of the Estonian Land Board. The activities of the State Information System Authority (RIA), the Data Protection Inspectorate (AKI) and the Ministry of Economic Affairs and Communications (MKM), who are responsible for effective supervision in IT security issues, were also analysed. The information and support given to local governments were also reviewed.

Why is this important to taxpayers?

The successful functioning of the public sector is increasingly more based on information technology and data, which are collected by the state and local government agencies. The possibility to develop better, more convenient and cheaper public services increases the quantity of data as well as the risk that the data will end up in the wrong hands, perish, become damaged, etc. Local governments are not immune to this either.

There are examples of local government information systems being targeted by denial-of-service attacks, systems being infected with malware and damage caused to websites. The results of various attacks may reach from reputational damage to court cases filed against an agency or lead to unreasonable management decisions. The databases of the state and local government exchange data via the X-Road, which means that the vulnerabilities left without attention in local governments are passed on and may cause damage on a much larger scale.

X-Road – a secure data exchange layer of information systems that must be used when exchanging data in the public sector (between databases) and also with external systems (e.g. with information systems of companies).

What did we find and conclude on the basis of the audit?

The security of the data entrusted to local governments is not guaranteed as required. Risks related to IT security are still not acknowledged by a lot of local governments and therefore, the requirements established by the state are not complied with, even though they have been in effect for almost 10 years now. The state supervision is inadequate and does not force local governments to act. Neither have the awareness raising activities and financial support by the state led to the expected development.

Key observations of the National Audit Office about the audited local governments:

- The overall information security culture of local governments is low among employees and the management alike; none of the auditees had an up-to-date information security concept; four local governments had not appointed employees responsible for IT security. There are either no guidelines for using IT tools or employees have not been informed of the existence thereof; none of the audited local governments had provided training or information to support compliance with IT requirements.

- Planning and implementation of information security in local governments is at a poor level. Efficient information security is based on a security analysis as a result of which security classes are assigned to the collected data, which, in turn, serve as a basis for choosing the measures that are to be implemented. None of the 10 audited local governments had performed a security analysis or established security classes. Problems also occurred with password policy, data backups, security updates and access rights.

- There is no comprehensive overview of the data collected by local governments. A large part of the databases has not been registered in the RIHA and those that have been registered have for the most part not been checked by assigned authorities. Only a small part of local governments' databases have been interfaced with the X-Road and in several places the same data are collected twice.

- The audited local governments do not consider themselves responsible for the security, the registration of databases in the RIHA and interfacing with the X-Road, when the collected data is stored in externally hosted databases, but do not demand this from service providers either.

RIHA is the administration system of the state information system, which checks whether necessary data are already collected within the composition of some established database or not. If they are collected, the founder of a new database can file an application, through the RIHA, with the controller of this database for making the data available in the state information system, which also means initiating the X-Road interfacing process.

Source: Subsection 6 (4) of Government of the Republic Regulation "Administration system of the state information system"

Key observations of the National Audit Office on the activities of the state:

- Considering the observations made about information security in local governments, the current organisation of supervision cannot be considered adequate. For example, the data in RIHA concerning databases administered by local governments could be considerably more organised and more databases could be interfaced with the X-Road if the Data Protection Inspectorate put more effort into checking registration and data compositions. According to what is known about the oversight activities, the agencies responsible for supervision have not issued any precepts to local governments about the poor implementation of ISKE or the disregard of the audit obligation thereof. Furthermore, the ministry responsible for ordering an audit of implementation of ISKE has no intention to order audits for local governments.

- So long as no ISKE audits have been ordered in local governments, the chief administers of databases cannot rely on the opinion of a certified auditor about the compliance with the security needs. Therefore, keepers of state registers must conduct separate checks to confirm the security of their data before it is handed over to local governments. However, none of the audited administrators of state registers has conducted such checks.

ISKE – a three-level baseline security system for information systems used for processing data compositions in the databases of the state and local governments. ISKE defines three levels of security – low (L), medium (M) and high (H). The appropriate level of security is determined through the assignment of security classes (security subclasses) to data.

Source: ISKE implementation guide 8.0

- Until today, the maintenance of information security level in local governments has been somewhat campaign-based and has depended on the availability of foreign funds. Although the state has provided local governments with information (including training, circular letters, instructions, etc.) and subsidised activities for intended purposes, these activities have not had the expected long-term lasting impact.

- The audit did not indicate as if ISKE were unsuitable for local governments, but more flexibility should be allowed upon implementation thereof, considering the specificities in keeping databases of local governments. For example, local governments often keep databases by using standardised software solutions (84% of the databases registered in the RIHA) whose security issues could be solved, to a certain extent, in a uniform and one-off manner (e.g. assignment of security classes, registrations in the RIHA and data composition checks, auditing).

What did we recommend as a result of the audit?

The National Audit Office recommended that the audited local governments appoint a person who performs the duties of an information security manager or outsource the management of information security; establish requirements for the standard software solutions used to keep databases in accordance with the security needs of the entered data; make sure that it would be possible to interface the solution with the X-Road, if necessary; and agree on the organisation of audits of security measures in the contract with the service provider.

In their responses to the audit report, **the audited local governments** are generally of the opinion that the recommendations of the National Audit Office can be implemented and steps have already been taken in several local governments for improving the situation. During the completion of the audit, a person who performs the duties of an information security manager has been appointed at least in Võru, Rapla, Mustvee, Valga and Haljala Municipality and in Pärnu City.

The National Audit Office recommended that the Minister of Entrepreneurship and Information Technology think over the guidelines concerning compliance with the legal requirements of the RIHA, the X-Road and the system of security measures in the context of the local governments' practice of keeping databases. In addition to this, reasons for the long delay in the implementation of the system of security measures in local governments must be analysed and, based on that, activities must be developed for making the implementation of ISKE in local governments more flexible. The National Audit Office recommended that the procedure for ordering an ISKE audit be amended so that such audits would be ordered consistently. As concerns measures meant for supporting information security, it must be taken into consideration that they should motivate local governments to adopt solutions that the state or another local government has already created with the taxpayer's money.

The Minister of Entrepreneurship and Information Technology agreed to the recommendations and noted in her letter of reply that security classes should be assigned to similar or uniform databases on the same grounds and the procedures should not duplicate each other. In addition, the MKM agreed that the current procedure for ordering ISKE audits of local governments had been a failure. It is planned to discuss the recommendations of the National Audit Office upon updating the RIHA process and the observations made on the implementation and auditing of ISKE along with the amendments arising from the Cybersecurity Act. The terms and conditions of interfacing with the X-Road will be specified in the course of updating Government of the Republic Regulation No. 105 "Data exchange layer of information systems". Already today the MKM prepares and reviews the terms and conditions of support measures according to the principle that prefers joint use and development of IT solutions.

The National Audit Office recommended that both supervisory agencies (i.e. the RIA and the AKI) improve control, according to their authority, in local governments over the implementation of ISKE, joining the X-Road and registration in the RIHA. The National Audit Office recommended that

besides the training meant for IT specialists it is necessary for the RIA to promote more the training aimed at the management of local governments and engage in wider notification work.

The Director General of the Data Protection Inspectorate generally agreed to the recommendation made in the course of the audit and promised to take it into consideration in the future work, if possible. The Director pointed out that it is difficult to implement the recommendation in the nearest years as, in addition to the large number of subjects of supervision, the workload increases due to the entry into force of the General Data Protection Regulation in May and, along with it, the new Personal Data Protection Act. Another obstacle mentioned by the Director is the fact that no list of security measures to be implemented for the protection of internally restricted information has been established.

The Director General of the State Information System Authority agreed to the recommendations and notified that the recommendations were already being implemented at the time the audit was completed. It is planned to check local governments after the administrative reform. Training aimed at senior managers started in 2017 and in 2018 it is also planned to organise training on increasing information security awareness to local governments and management thereof. The RIA also pointed out that since the motivation of senior managers of local governments in engaging in information security and attending training could be higher, the recommendation made by the National Audit Office could rather be aimed at heads of local governments.