RESTRICTED ACCESS

Can we rely on the access to information systems and the receipt of e-services?

Riga, 2022

Latvijas Republikas
Valsts kontrole

Audit report

26 July 2022

Performance audit “Can we rely on the access to information systems and the receipt of e-services?”
The audit was performed based on audit schedule No 2.4.1-38/2020 of 9 September 2020 of the Audit and Methodology Department of the State Audit Office.
The cover design includes a photo from website *Depositphotos: (https://depositphotos.com/41112943/stock-photo-business-strategy.html).*

Dear Reader,

Our everyday life is unimaginable without the use of information and communication technologies (ICT). The amount of e-services available to citizens continues to increase and, accordingly, the amount of information to be processed and stored in the provision of services. The spending for the maintenance and operation of information systems (IS) and related ICT infrastructure in the state administration has also been increasing from 41 million euros to 64 million euros per year in last five years.

Appropriate operation of IS and related ICT infrastructure is a prerequisite for accessibility, without which the provision of e-services is impossible.

The COVID-19 pandemic has especially brought up the possibility of receiving services provided by state institutions in a remote way (including e-services) to date. When choosing to receive an e-service, we expect it to be available at the time you make that choice. Any obstacles to receiving an e-service at the selected moment create costs both for a recipient of an e-service and also for an institution providing that e-service. However, no one has really estimated how high these costs are and in which cases they are justified.

During this performance audit, we were looking for an answer to the question – *could we rely on the access to information systems and the receipt of e-services?* Yet, we did not get an unequivocal answer because the information provided by the institutions about the level of access to information systems and e-services was mostly based on opinions, not facts, as it was not clear how to measure accessibility. There is no calculation methodology and no indicators are collected to measure it. Information on the achieved IS and e-services availability level is not collected at the national level either.

Every institution is responsible for the maintenance and security of institutional IS, as well as the continuity of the IS operation. However, information systems maintained by other institutions are often involved in ensuring the availability of e-services. Thus, in order for the recipient of the service to receive the e-service guaranteed, not only all interconnected information systems, but also the ICT infrastructure and communication channels must work correctly at the same time. This is a challenge for state institutions that they have not always overcome successfully.

Although the significance of IS accessibility (including for providing e-services) is recognized at the national level and the prerequisites for organizing the continuity of ICT operations and ensuring the availability of IS (including e-services) have been set for the state institutions in laws and regulations, the state institutions take their time over implementing the latter and verifying that the continuity of ICT operation, the access to IS and e-services is thus ensured, and that the restoration of IS accessibility can be achieved in the shortest possible time if any incident occurs.

After the audit, we have formulated and coordinated several recommendations, therefore we thank the Ministry of Environmental Protection and Regional Development, the Ministry of Defence and the state institutions that provided the necessary information for the audit to assess the situation in organizing the continuity of ICT operations and ensuring the accessibility of IS (including e-services) for their cooperation.

Respectfully
Ms Ilze Bādere
Department Director

Summary

Main conclusions

On average, the state administration spends 51 million euros per year[1] for information technology services. These are expenses to ensure the maintenance and operation of information systems (hereinafter - IS) and related information and communication technology (hereinafter - ICT) infrastructure, but not their development expenses. Appropriate operation of information system is the basis for the accessibility of e-services and IS supporting them, while the level of IS accessibility achieved by state institutions is one of the cost effectiveness indicators of IS maintenance.

The audit has detected problems not only in the assessment of achieved IS accessibility but also in the management of IS accessibility in general; therefore **auditors cannot provide an answer to the question "*Can we rely on the access to IS and the receipt of e-services?*" because it was impossible to determine unambiguously during the audit** due to the following reasons:

- Information about the achieved accessibility level of e-services and the IS supporting them is not collected and analysed together. Also, the information that is at the disposal of certain leading e-government and IS security institutions, the Ministry of Environmental Protection and Regional Development (MEPRD) for state IS and technical resources, CERT.LV for IT security incidents, State Regional Development Agency (SRDA) for malfunctions and unavailability of e-services on the *Latvija.lv* portal, is also not analysed together;
- It is not clear what to measure, in what way, and there is no calculation methodology either. Institutions understand the IS accessibility achieved in different ways, as they do not measure anything and do not even highlight IS accessibility as a necessity, they only measure the accessibility of databases (which is one of the components for IS and e-service to function), interpret IS security incidents in different ways;
- There are also shortcomings in the field of development planning because the need to identify and evaluate the situation in the accessibility of e-services and the IS supporting them has not been determined. Also, regarding the quality of services provided by the state administration, the accessibility of e-services is not put forward as a quality indicator;
- It is not clear how to ensure and what to monitor in order to reach the level of accessibility specified in the laws and regulations: for integrated national IS (98%), integrators (99%) and e-services (98%). In addition, the organizational prerequisites set forth in the laws and regulations for ensuring the accessibility of IS and restoring the continuity of operations in the institutions have not been fully implemented;
- The set matched operating time of IS and the attainable level of accessibility are not coordinated among all the components involved in the provision of the e-service: the supporting IS, ICT infrastructure, integrated IS and also with regard to the place where the e-service is hosted (an institution's website or the *Latvija.lv* portal);
- It is not defined what the working hours of e-services are, i.e., whether the accessibility of the e-service can be expected during the working hours of the institution or in a 24/7 operating mode.

Many cases of malfunctions and unavailability of e-services show that there are problems to be solved in managing the IS accessibility and e-services. (According to auditors' observations on the *Latvija.lv* portal from January to March 2022, at least 84 thousand potential users of e-services could have encountered problems with the accessibility of e-services of (technical problems were observed resulting in the missing e-service), of which the e-service could not be requested at all in 10,000 cases. Also according to the SRDA, which ensures the operation of the *Latvija.lv* portal, the number of observed errors in e-services requests for individual - the most unstable services - tends to reach 40-60%. Thus, one can conclude that the actual number of e-service recipients who encounter e-service malfunctions or their unavailability could be higher than the estimated by auditors (based on e-service usage statistics in 2020).

In Latvia, no estimates have been made so far of how much the unavailability of IS has cost and what consequences it has had for private individuals or, more broadly, for the national economy. According to the auditors, the consequences for the unavailability of IS and e-services could be significant, because, for example, according to the information gathered by *CERT.LV*[2] about IS security incidents in the state administration, the operation of [RA] websites of state and municipal institutions was affected in one of the incidents alone. In its turn, the unavailability of e-services has consequences both for the service recipient, who has to look for an alternative solution for receiving the service or spend time checking whether the service availability has been restored, and also for the state administration, serving a private individual in a less automated service provision channel. According to the estimate made during the audit (Table 2), receiving an e-service in a different, rather than remote, way may incur costs of 15.40 euros for a recipient of the service and may require an average of an hour and half to receive it in person. In case the service is unavailable, institutions are also forced to spend resources (1.83 euro per service), which they could use to provide other, less automated functions.

In addition, if information systems are unavailable, the consequences could arise not only for the institution itself, but also for other institutions that did not receive the necessary information in time and could not provide their services.

The requirement to provide accessibility does not ensure accessibility in itself. One requires both to create an appropriate internal control environment, to implement IS security and ICT management, and to measure the achieved result. The audit has discovered that there are still problems in this area, as well as many questions about how to organise accessibility properly, by concluding that in general, the accessibility of e-services and the IS supporting them is not well managed and monitored. Moreover, this action must be mutually coordinated between the institutions, because several institutions and the IS maintained by them are involved in its execution very often for an e-service to function. It means that all these components must be available and even a malfunction of one component will affect the receipt of the e-service. For example, for an individual to receive an e-service on the *Latvija.lv* portal, one requires the following to operate:

- The *Latvija.lv* portal maintained by the SRDA;
- User authentication mechanism provided by the LSRTC or one of the commercial banks;
- IS itself and e-service performing services maintained by an institution;

- Related IS and services required, for example, for checking personal data in the Population Register maintained by the Office of Citizenship and Migration Affairs;
- Data exchange channels and an integrator maintained by the SRDA.

The requirement for the attainable level of accessibility of e-services has been determined, but the mechanism for monitoring its implementation is not introduced

Although the requirements for the attainable level of accessibility for the integrated national IS and the integrator have been set in 2012 and for e-services in 2017, and state development planning documents emphasise the need for the access to IS and e-services, the state administration has not carried out an analysis of the actually achieved accessibility level of e-services and the IS supporting them. There is also no designated responsible authority that should carry out the collection and analysis of such information. The laws and regulations in the field of IT security, nor in the field of public administration services provide for that. Although one of the principles of public administration is that the public administration constantly checks and improves the quality of services provided to the public in its activities, and there are certain indicators that must be measured and published on the Service Provision and Management Platform, they do not include e-service accessibility indicators, which are one of the most important indicators of service quality. Therefore, whether or not the institution provides e-services and the IS supporting them is only a matter of the institution’s agenda.

It has not been assessed in the country whether the accessibility level of e-services and the IS supporting them has been reached.

Most of the institutions included in the audit scope admit that they have neither data nor tools to monitor and measure the accessibility of IS and e-services, nor do they have a methodology to calculate the accessibility of e-services and the IS supporting them.

Only three institutions among the ones included in the audit sample have measured the actually achieved level of accessibility for e-services or IS maintained by institutions. The other six institutions state that the IS maintained by them have operated with a high level of accessibility, justifying this not by data, but by the fact that no significant ICT security incidents have been observed that would have affected IS accessibility.

State institutions lack both methodology and data to determine the accessibility level of e-services and the IS supporting them.

At the same time, the six institutions out of the nine included in the audit scope have indicated that there may be cases when interruptions in the operation of the e-service are not recorded and registered in an incident register, while only three institutions have implemented accumulating information in practice about all planned technical work dates in the incident register or some other separate register and the duration of interruptions, thus the registers do not provide complete information about planned and unplanned malfunctions or interruptions of e-services and the IS supporting them and their duration.

Regarding the accessibility of e-services hosted on the *Latvija.lv* portal, the auditors have performed analysis[3] and have found that notices were published about 21 e-services that the e-service was not working. Of these, eight e-services were down from 1 to 23 days. Thus, one can conclude that those e-services have been available in the range of 26% to 96.8% in the given month, which is less than the 98% attainable level of e-services defined in the law.

At the national level, *CERT.LV* collects information about IT security incidents that have occurred in state institutions, however, CERT.LV is not notified of all incidents that have occurred because there is no uniform approach in state institutions when information must be provided to *CERT.LV*.

The auditors also could not get a comprehensive picture of the actual number of IT security incidents and the affected institutions from the information indicated in the reports of *CERT.LV*, as the information in the reports was reflected in a different perspective. The reports include information about the affected IP addresses, and the situation (IT security incidents) in specific institutions has been examined only in some cases. In the restricted access reports submitted to the Ministry of Defence, [RA] of incidents in state administrative institutions, municipalities or state-owned or municipal enterprises are related to malfunctions of the accessibility to service.

Although individual items of information relating to the accessibility of IS are collected in the state administration (*CERT.LV* on IT security incidents, SRDA on the accessibility of e-services hosted by the *Latvija.lv* portal), information on problems in ensuring the level of accessibility is not collected in a centralized way in the country, as nor has the causes and consequences of the problem of not reaching the specified level of accessibility been analysed. When not all the identified problems are recorded and their causes are not evaluated, providing reasonable proposals for improvements is impossible, hence, state institutions continue to maintain e-services in the long-term, but nothing contributes to improving their accessibility.

The prerequisites for ensuring the accessibility of e-services and IS supporting them have not been implemented in the institutions

The Regulation[4] (including the best practice[5]) contains prerequisites, the fulfillment of which is necessary for facilitating the continuity of IS accessibility and related ICT infrastructure in state institutions. Although all nine institutions included in the audit sample maintain enhanced security IS, none of them have fully implemented all prerequisites. The most frequent problems are related to the fact that the planning documents of the institution (in three institutions) do not include a goal for ensuring the accessibility of IS. Without setting goals and tasks for ensuring the accessibility of IS, the access to information systems is not determined as an essential necessity for ensuring the institution’s functions.

Nevertheless ICT resources (infrastructure, IS, software, communication channels) have been identified in five institutions out of the ones included in the audit scope, which is essential in providing support for the performance of the institution's functions, the essential ICT resources have been partially identified in other four state institutions, for example, by identifying only IS. Thus, all subsequent operational continuity planning activities are focused only on IS operational continuity planning, which is only a part of the ICT resources involved in the institution's performance. In addition, the institution will not be able to respond quickly enough and eliminate problems in non-IS resources in case of incidents (in case of damage to ICT infrastructure or communication services).

The auditors have assessed the prerequisites that the institutions included in the audit sample stipulated in agreements when outsourcing IS maintenance to an external service provider and have established that IS accessibility requirements are general and do not set the achievable accessibility level of IS. This, in its turn, creates a risk that the accessibility level of IS set by the regulation will not be reached for the outsourced IS and the outsourced systems will not contribute to the achievement of the accessibility level set in state administration as a whole.

Among the six audited entities that have developed an IS restoration plan, there have been no checks of the compliance of the plan for restoration of IS accessibility, which would reduce the risk that ensuring the restoration of ICT operations and IS accessibility in a sufficiently short time or at all would be impossible in case of incidents. IS operation restoration plans developed in the institutions have not been tested by checking their completeness, that is, the institutions have not verified whether the accessibility of IS can be restored with the available technical resources, stored backup copies and the competence of employees according to the plan at the institution in the time specified.

State institutions rely primarily on built-in backup controls that report at the time of backup whether a copy has been created and whether it is error-free. The backup copy system does not perform the data recovery check from the backup copy, therefore the institutions' reliance only on the backup copy system reports about the fact of making a copy and the actual failure to check the IS data recovery is contrary to the Regulation[6] that the last full backup copy and subsequent incremental copy restoration checks must be performed for integrated national IS in test environment no less than once per calendar year.

The institutions have not verified whether and when the accessibility of their IS can be restored in the event of an incident.

In the field of development planning, there is no identified framework for ensuring the accessibility of information systems

Although the development planning documents[7] have recognised the significance of IS accessibility at the national level, including for the provision of e-services, the development planning documents do not specify the specific goals and tasks to be achieved to ensure the accessibility of IS in general, and no performance indicators have been set to measure and evaluate the achieved IS accessibility with the exception of one achievable result in Digital Transformation Guidelines for 2021-2027.

In Digital Transformation Guidelines for 2021-2027, the achievable result and performance indicator related to ensuring the continuity of ICT operation and the accessibility of IS are determined. The indicator assumes that 85% of all high-security systems and platforms are securely backed up and recoverable. However, no specific tasks have been set for the achievement of this indicator, and neither the MEPRD (as the executor of the policy planning document), nor the Ministry of Defence (as the leading institution in IS security policy) was yet clear at the beginning of 2022 who and in what way would ensure, as well as monitor and measure the achievement of the set policy result.

Thus, there is no identifiable action framework in the development planning documents for ensuring IS accessibility, and the state administration does not have a common understanding of what must be achieved in the field of IS accessibility, and no targeted actions are taken to achieve it.

In the auditors' opinion, identifying the framework of action for ensuring the accessibility of IS at the national level or identifying those IS that must ensure the levels of accessibility defined in the laws and regulations requires analysis of the data collected in the national IS and ICT resource accounting system (*VIRSIS*); however, the data recorded in this information system is also incomplete.

Accumulated data on national IS and ICT resources are incomplete.

The *VIRSIS* has been developed and implemented since 1 January 2020, however, the state institutions have recorded data only about 127 out of 181 national IS, which had already been recorded in the previously maintained "Register of State Information Systems" (hereinafter - *VISR*). For the majority of IS (123 IS), their managers have indicated that IS are designed to meet the internal needs of the institution, so they do not provide data exchange with other systems or the provision of services, which suggests that the systems are not classified correctly.

The VIRSIS has not accumulated data that could indicate the exchange of IS data with other ISs and whether an information system is an integrated national IS, which is essential for establish whether an information system affects other ISs. The lack of qualitative accounting data does not allow identifying such ISs that should ensure a higher level of accessibility than is determined by national laws and regulations and require planning additional measures and funding to ensure an appropriate level of accessibility. For instance, those ISs at the national level that exchange data with information systems of other countries and for which the attainable IS accessibility level, which is higher than that stipulated in Latvian laws and regulations, has been determined by the EU/EEA.

The auditors consider that deficiencies in information accounting affect the MEPRD's ability to plan a unified national policy for the development and maintenance of IS and ICT resources and services necessary for their operation, as well as to ensure the establishment of an evidence-based policy in the field of ICT management successfully. According to the auditors, appropriate and sufficient information about the national IS and related ICT infrastructure is a prerequisite for planning, determining and monitoring uniform principles of IS accessibility and ICT continuity management.

Simultaneously with the identification of the action framework for ensuring the accessibility of IS at the national level, it is also necessary to review the requirements set in the national laws and regulations for achieving the accessibility level of IS and e-services by harmonising them with each other. The audit has detected the cases when the average accessibility indicators of IS are determined in the laws and regulations regulating the operation of the integrated national IS lower than those determined in the Cabinet Regulations, which define the basic requirement for ensuring the accessibility of IS, for example, one must ensure the average accessibility of IS of 97.47% per year, although the basic requirement stipulates that the accessibility must be ensured for 98% of the system's operating time per year.

Since 2017, an administrative burden in the amount of 3.84 million euros has probably been created due to the inconsistent requirements for the accessibility of e-services and the *Latvija.lv* portal.

A similar situation has also been found in relation to the hosting of e-services, because when an e-service is hosted on the *Latvija.lv* portal, its accessibility is possible only during the accessibility times determined and ensured by the SRDA, the operator of the *Latvija.lv* portal. Taking into account that the accessibility of the portal must be ensured on average 97.49% per year under the statutory requirements, there is a risk that state institutions will not ensure the attainable level of accessibility for e-services (98% per month) when hosting e-services on the *Latvija.lv* portal. According to the auditor's calculations, this means that an institution's e-service can be provided for almost four hours per month less than the general regulation for e-service accessibility provides. This circumstance poses a risk that due to inconsistent statutory requirements, an administrative burden of up to 64,000 euros[8] can be caused every month. Since the regulatory framework stipulating the requirements for the accessibility of e-services and the *Latvija.lv* portal has been in force since 2017, one can conclude that an administrative burden of 3.84 million euros over five years might have been caused, which the population or the state administration could have spent in a different way.

Key recommendations

Based on the audit conclusions, the MEPRD and the Ministry of Defence are provided with recommendations for improving the access to e-services and information systems supporting them in cooperation with *CERT.LV*:

- The MEPRD shall perform a quality check of the data recorded in the *VIRSIS* system, develop a methodology for calculating the achieved accessibility of e-services and the IS supporting them and facilitate the achievement of the indicator set in the Digital Transformation Guidelines for 2021-2027 of 85% of increased security IS are restorable;

- The Ministry of Defence and the MEPRD shall develop a data exchange mechanism and a single information accumulation point in order to disclose information about the affected IS and e-services promptly and provide information about downtime in the long term;
- The MEPRD shall collect information about the achieved accessibility level of e-services and the IS supporting them and perform an analysis of the consequences of the unavailability of IS and e-services;
- The MEPRD shall harmonize the requirements for the achievable accessibility level of e-services and the *Latvija.lv* portal, including the operating time;
- In cooperation with *CERT.LV*, the Ministry of Defence shall determine the recommended volume and structure of information to be submitted on IT security incidents;
- For improving the monitoring of the electronic environment of the state administration, in cooperation with *CERT.LV*, the Ministry of Defence shall develop criteria to identify institutions where *CERT.LV* should deploy security sensors and shall develop a strategy for broader installation and use of security sensors in cooperation with the MEPRD.

References

[1] Data from the State Treasury's State Budget and Municipal Budget Reporting System on the spent funding for IT services: in 2017 – 41,135,463 euros, in 2018 – 47,372,778 euros, in 2019 – 48,163,508 euros, in 2020 – 52,967,430 euros, and in 2021 – 64,129,828 euros.

[2] *CERT.LV* "Public report on the performance of CERT.LV tasks" for the 4th quarter of 2021 (Internet resource: https://cert.lv/uploads/parskati/cert-ceturksna-C4-atskaite-2021-LV.pdf viewed on 1 June 2022)

[3] The analysis was carried out for October 2021 from January to March 2022.

[4] Article 8.1, 8.4, 8.5, 27.2 of Cabinet Regulation No 442 "The procedure for ensuring compliance of ICT systems with the minimum security requirements" of 28 July 2015.

[5] Best practice – COBIT, ITIL.

[6] Article 10.6 of Cabinet Regulation No 421 "Requirements for the protection of state information system integrators and integrated state information systems" of 19 June 2012.

[7] Latvia's National Development Plan for 2021-2027 (approved by decision No. 418/Lm13 of the Saeima of the Republic of Latvia of 2 July 2020); Digital Transformation Guidelines for 2021-2027 (adopted by the Cabinet of Ministers on 6 July 2021); Informative Report "Latvia's Cyber Security Strategy for 2019-2022" (approved by the Cabinet of Ministers on 17 September 2019).

[8] Auditor's estimate: administrative burden of one hour for the *Latvija.lv* portal * four hours per month = 16,000 euros/h * 4 h = 64,000 euros.