Executive summary of the public audit report

MANAGEMENT OF POLICE INFORMATION RESOURCES

5 November 2015 No. VA-P-90-3-15

Full audit report in Lithuanian is available on the website of the National Audit Office: www.vkontrole.lt

SUMMARY AND DEFINITIONS

ADA – automated data processing information system

RAOTA – the Register of Administrative Offences and Traffic Accidents

ERC – the Emergency Response Centre

ERC IS – the Emergency Response Centre Information System

COBIT – ISACA methodology of IT governance and management[1]

RWW – the Register of Wanted Weapons

RWDONIA – the Register of Wanted Documents and Objects that are Numbered or with Individual Attributes

DITC – the Department of Information Technology and Communication under the Ministry of the Interior of the Republic of Lithuania

IS – Information System

IT – Information Technology

CGIT – the Coordination Group of Information Technology

RWMV – the Register of Wanted Motor Vehicles

CISD – the Committee of Information Society Development under the Ministry of Transport

CAIS – Crime Analysis Information System

OAIS – Operational Activities Informational System

DFRS – the Department of Fire and Rescue Services under the Ministry of the Interior of the Republic of Lithuania

PLAIS – Police Licensed Activity Information System

PIS – Police Information System

PFU – Police Force Unit

RPRA – the Register of Police recorded accidents

PAMIS – Preventive Action Management Information System

SPG – the Strategic Planning Group

UPFS – the Unified Police Force System

CDB MIIS – the Central Data Bank of the Ministry of Interior Information System

SBGS – the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania

PSS – the Public Security Service under the Ministry of the Interior of the Republic of Lithuania

Other terms used in this report are understood as defined in the Law on Management of State Information Resources of the Republic of Lithuania.

[1] ISACA – Information Systems Audit and Control Association. Access via the Internet: http://www.isaca.org/about-isaca/Pages/default.aspx

SUMMARY

The mission of the police in Lithuania is the efficient use of available resources to defend the Lithuanian human rights and freedoms, to protect the society and the country, to help people, their family and community. There are two kinds of the Police in Lithuania: criminal and public. This is a consistent Police organization, and its connecting link is the Police Department under the Ministry of Interior in the Republic of Lithuania.

The main tasks of the police shall be: protection of human rights and freedoms; ensuring of public order and safety; rendering of emergency assistance to persons when it is necessary because of their physical or mental helplessness, as well as to persons who have suffered from criminal acts, other violations of law, natural calamities or similar act; prevention of criminal acts and other violations of law; detection and investigation of criminal acts and other violations of law; control of traffic safety.[2]

Data, necessary to implement Police tasks, are processed in departmental registers and information systems, as well in automated data processing systems and networks for storing, processing and transfer of classified information. The Police Department is the owner all of these information resources, so the audit focused on the activities and actions of the Department aimed to ensure planning and organizing, monitoring, evaluation and coordination of the resources, and other aspects of strategic management of information systems and registers.

The audited period was 2012-2014. For the analysis, there were used previous data and data of 2015.

The objective of the audit is to evaluate information resource management and development control of the Police Department. The audit was conducted in the Police Department. The data and information were collected in specialized local police stations: the Lithuanian Criminal Police Bureau; Lithuanian Police Forensic Science Centre; senior police stations in Vilnius, Kaunas, Alytus and other districts, counties senior police stations; Regitra and the Emergency Medical Station.

In the Police Department, groups and commissions for considering IT issues are established. They are tasked with identifying IT development trends, organizing, coordinating and control of IT development and identified information security objectives and monitoring information assets threats. They work episodically and their assigned functions are not performed in full extent and overlap, therefore the adequate monitoring and control of IT implementation and evolving risks for information assets is not ensured.

The Police Department and other local police stations regularly conduct the legality of employee data (personal data reviews), and validity checks, cooperate with the State Data Protection Inspectorate. The risk of the illegal use of police databases is not well controlled in the Lithuanian Criminal Police Bureau.

In order to ensure the cohesive IT development in the Police Department and contributions to police objectives and tasks, we recommended to develop and adopt an IT strategy and on this basis to refresh and update the plans of IT development. In order to set clear responsibility for strategic decisions and proper approach to IT management, we recommended reviewing

[2] The Republic of Lithuania. Law on Police Activities, 17/10/2000 No. VIII-2048, Art. 5

activities of existing groups and commissions (responsible for IT issues) in the Police Department and police stations, to separate functions of groups and commissions, to ensure continuity of their activities and accountability. The Department should also pay more attention to assurance of system security and business continuity, and systematic approach to IT project management.

Audit conclusions and recommendations provided below and based on obtained evidence.

CONCLUSIONS

1. In the Police Department, in order to fulfil police objectives there is a lack of coherent and sustainable IT planning and development process, because strategic planning documents do not contain the main IT development directions, planned to be built or modernised the national IS or registers and priorities for their establishment (subchapter 1.1. , p. 11).
2. The Police Department does not have a common information architecture model, defining the information managed by the Department and police authorities, the classification criteria, the data of IS or registers, technology architecture. Therefore the interoperability of IS and registers, managed by the Department, the importance of the information managed by the Department and police stations, sensitivity for its publication, communication and disclosure are unclear.
3. The Police Department does not ensure compliance with regulations concerning security of information resourses and data management.
   3.1. The Police Department has established procedure for analysis, monitoring and evaluation of threats and risks related to police IS. However, the procedure is not followed, security compliance assessments are not executed periodically as requested by regulations, therefore control measures for identified risks are not adequate, and it is not verified if selected security measures are sufficient and how they operate (subchapter 1.3., p. 14).
   3.2. In the Police Department, there is no recovery testing of backup data, copies of data are stored in the same room as their servers. However, this room does not have an automatic fire extinguishing system, so, during an incident, server hardware and software can be irreversibly damaged, IS data in the databases can be lost together with their copies (subchapters 1.3., 1.4., p. 14, 17).
   3.3. The Police Department does not provided assurance that they are ready to restore activities of IS and registers during the period which does not have any negative impact on implementation of functions of the Department and relevant authorities because the business continuity plan has not been updated and tested (subchapter 1.3., p. 15).
   3.4. The Police Department does not implement all technical and organizational security measures of personal data when processing it in automatized way, there is no training for legal compliance and information security issues related to data processing, therefore required level of confidentiality of electronic information and protection of personal data from the accidental or unlawful destruction are not provided during data processing (subchapter 1.3., 1.4., p. 15, 18).
4. Conclusions, regarding automated data processing systems and networks where the classified information is stored, processed and transferred, management and protection, are provided in a separate document (classified) (subchapter 1.5., p. 18).

5. The Police Department has no approved procedures for IT change management, no practices for unified IT change requests, substantiating need and benefit of the request, priority of the change, arranging changes into categories according to the type of change, so the Department wasted additional time and resources in evaluating and summarizing the IT changes, their expediency and validity (subchapter 1.6., p. 18, 19).
6. Internal auditors of the Police Department do not monitor and evaluate the information resource management, and it constitutes preconditions for internal control deficiencies of potential management information systems. There are also found discrepancies that do not meet the external requirements (subchapter 1.7., p. 20).
7. The organizational structure of IT management should be improved. There are established working groups and commissions in the Department and police stations in order to link the needs of main activities with opportunities offered by IT, but not all groups and commissions carry out the functions assigned to the full extent, groups and commissions work irregularly (episodically), therefore an adequate control of IT implementation and monitoring of evolving threats is not assured (subchapter 1.8., p. 20, 21).
8. The applied principles of project management in the Department of Police failed to ensure the quality and risk management of UPFS project because:
   8.1. The UPFS was modernized without legal requirements having been met: mandatory documentation, regulations and specification of the UPFS, were approved after the closure of the project. When the phase of the modernization was completed, the UPFS transfer-acceptance act was uncertified (subchapter 2.1., 2.2, p. 24, 28).
   8.2. In order to implement the project of UPFS modernization, no integrated plan of UPFS project management was used which would include time schedules, financial and human resources, points of related project links or activities, the delivery time schedule of IS project components was not properly set, leaving the critically short time for improving the UPFS (20 days only) (subchapter 2.1., p. 24).
   8.3. The Ministry of Interior which coordinated the UPFS project did not ensure a reliable data exchange between the Police Department and the Emergency Response Centre, therefore only one-way interface between the RPRA, the UPFS and ERC IS was created (subchapter 2.1., p. 25).
   8.4. Project development control mechanisms were not applied, development of UPFS was carried out hastily, process of testing, training adoption of project results was inconsistent, pilot promotion to production of UPFS and project post-implementation review were not conducted, therefore it was not ensured if the functions of UPFS were operational in the real operational environment, and, after closing the project, if all the functions of UPFS were used (subchapter 2.1., 2.2., p. 26, 27).

   The recommendations of the implementation of the plan are presented in the annex 2.

RECOMMENDATIONS

1. In order to assure consistent and focussed development of IS and registers, taking into account needs of the whole organization, to develop and adopt an IT strategy and, on its basis, to create and constantly update the IT development plans (conclusion 1).

2. To create the information architecture model involving the information managed by the Police Department and police authorities, the data of IS or registers and technology architecture indicating components of each layer (used technologies, data, data flows between external and internal IS) (conclusion 2).
3. In order to ensure the safety of managed information resources it is recommended:
   3.1. Perform a periodic security conformity assessment of the information resources managed by the Department of Police and ensure the control of removing identified deficiencies (conclusion 3.1.).
   3.2. Improve risk management process, comply with description of procedures established for analysis, monitoring and evaluation of possible treats and risks of IS of the Department, ensure implementation of mitigation measures for identified risk (conclusion 3.1.).
   3.3. Reconcile procedures and plans of backup data storage and data recovery with the Ministry of Interior, taking into account the action plan for infrastructure consolidation of the state information resources (conclusion 3.2.).
   3.4. Update the IS continuity management plan of the Department and test it (conclusion 3.3.).
   3.5. Periodically organize trainings for employees on legitimacy of data processing and information security issues (conclusion 3.4.).
   3.6. Report the State Data Protection Inspectorate about automatic processing of personal data and purpose of the processing performed in information resources of the Department, in order to update the information in the Register of Personal Data Controllers (conclusions 3.4).
   3.7. Review and update IS data processing rules and registers: there are set out personal data protection measures that are applied as determined by the Law on Legal Protection of Personal Data (conclusion 3.4).
   4. Recommendations for information management and protection related to automated data processing systems and networks where the classified information is stored, processed and transferred, are provided in the separate document (classified) (conclusion 4).
   5. To ensure efficient and systematic change management, review the existing change management process and set (approve) procedure of IT change management determining IT change management planning and ensuring control of the procedure (conclusion 5).
   6. Periodically monitor and evaluate the status of information systems and internal control (conclusion 6).
   7. Review the activities of groups and commissions of the Police Department and police stations (that are tasked to discuss IT issues), clearly separate their functions and ensure the continuity of their activities and functions (conclusion 7).
   8. In order to ensure quality and risk management of IT projects:
   8.1. Review and update the principles of IT management in the Department of Police in order to provide the integrated project plan. Under this plan, project implementation and control are organized during full life-cycle of the project, and in case of deviations, structures responsible for control of implementation are informed (conclusions 8.2., 8.3., 8.4.).
   8.2. To develop and approve regulations of information resources and specifications, validate operational systems and registers (conclusion 8.1., annex 4).