Report on the Audit Results

The both economy and assets protection audit in the field of the information- communication technologies was realised in accordance with the audit activity plan of the Supreme Audit Office of the Slovak Republic (hereinafter referred to as "SAO SR") for the year 2012 and in accordance with the SAO SR Strategy.

The purpose of this audit action was the verification of economy and assets protection in the field of the information-communication technologies (hereinafter referred to as "ICT") and verification if the disposal of these assets is in compliance with the generally binding legal regulations. The audit examined also the compliance with the general statues in the field of the information systems of the public administration (hereinafter referred to as "ISPA") as far as the operation and security of these systems.

The subjects of the audit were areas as follows:

1. The state assets administration, the economy and disposal with the state assets in the field of the "ICT".
2. The observance of the general statues for the "ISPA".
3. The operation of the "ISPA".
4. The security of the "ISPA".

The audit was conducted at the Ministry of Environment of the Slovak Republic (hereinafter referred to as "auditee") for the audit period 2011 and 2012.

The auditee is the budgetary organisation, financed by the state budget of the Slovak Republic and is the central authority of state administration for the generation and protection of the environment. The auditee managed the information systems (hereinafter referred to as "IS") in the environment field while the administration and operation of the specific IS have been authorized the organizations established by the auditee with relation to the activity subject of these organizations. During the audit performance the auditee operated sixteen IS while in five cases the administration of these IS was realised by the budgetary organisation DataCentrum with the headqueaarter in Bratislava, established by the Ministry of Finance of the Slovak Republic (hereinafter referred to as "MF SR").

During the audit performance it was found:

1. The state assets administration, the economy and disposal with the state assets in the field of the ICT

In the field of the state assets administration, the economy and the state assets disposal in the field of the ICT it was found that the auditee in the year 2009 financed the purchase of the 40 pieces of the portable computers with the acquisition price 1 748.11 EUR per piece from the current expenses instead of capital expenses whereby it violated the law on public administration budget regulations.

By follow-up charging of the mentioned computer technique into usage and to balance sheet account instead of particular assets account the auditee violated the law on accounting. Moreover it was found by the audit that the assets stock-taking lists did not contain all requisites as it is obliged by the law on accounting.

Auditing the usage of the provided services by the external providers in the year 2011 and 2012 identified several shortcomings, especially:

- The auditee did not make the orders in the year 2011 on the basis of which the contractor was authorized to make out an invoice whereby there have been violated the payment conditions determined in the particular contract of work.

- From the list of *the realised works it was evident that contractor in the year 2011 performed inter alia the operations that were not listed in the contract in the Article* "The subject of a contract", i.e. the contractor performed the operations overlapping the scope of the contracted activities without reasonable conditions for the operations delivery (delivery respectively acceptance of the realised activities, determining the security criteria for the access to the IS of the auditee).

- The auditee ordered in the year 2011 the services of the application support even despite the reality that the contract was not at that time in effect and auditee had no valid document of which the subject should have been the service delivering of the economic information system operation (further only "EIS").

- The operation statements related to the conditions for the service delivering *had been agreed only formally, whereas auditee did not know how to check the real number of the man- hour for the concrete request.*

- *The auditee paid off in the year 2011 funds also for the technical support services, at which no written request was given* and to the control it was not submitted acceptance

protocol of which the acceptance subject would be technical maintenance service delivering on SW facility ORACLE. Thereby auditee dealt out in discrepancy with the law on public administration on budgetary rules according to which the financial discipline violation is the disclosure or using the public funds over the authorized scope by which the public means are spent above.

2. The observance of the general statues for the ISPA

By auditing the compliance with the provisions of the law on the ISPA was found that auditee did not update the conception of the public administration information systems development in compliance with the mentioned law.

Moreover it was found a discrepancy with the law on the ISPA because the IS of auditee did not meet the standards stated in the Edict of the MF SR on the standards for the public administration information systems namely in the fields:

- Information security management,
- Personal security,
- Risk management for the field of the information security management and security policy of the compulsory person,
- Risk management for the information security field,
- Control information security management mechanism,
- Back-up and physical back-up storage,
- Monitoring and security incident management,
- Periodical valuation of the IS vulnerability,
- Access management to the IS,
- ICT updating and
- Involvement of the third party.

The audit also indicated a discrepancy with the law on personal data protection in the personal data security field and in the field the performance of the supervision the personal data protection.

3. The operation of the ISPA

3.1 Organization and the ICT operation management

In the field of the IS operation of the auditee it had been found that *the auditee had not established any internal directives for the IS operation area inter alia the auditee had not established the internal document by which it would be determined the password policy, operating and administrator rights, administration of these rights, document adjusted*

the backup and data recovery and document regulated the performance of the restore tests and systems functionality. The auditee had not identified the critical IS. Also it was found that auditee did not establish any security directives regulating the area of the information security management of its IS, while to the computer domain of auditee also third parties entered that performed radical interventions to the IS of the auditee with the highest access rights.

Recommendations:

To establish the internal directives that would regulated the area of the operation and the IS security management of the auditee.

3.2 The business continuity and the information system recovery, backup, external archiving, data and program settings recovery.

By auditing the area of backup and external archiving was found that the auditee had not adopted any detailed principles and procedures concerning the data backup and programs. The systems administrator performed the full backup of servers every dayinclusive of the operating systems. The backups had been made in two copies *while both had been placed in technological room.* Moreover it was found that *there had not been performed continuous control of the backup functionality of the selected data media.* The audit indicated that the auditee had not defined critical, strategic IS for organization.

Auditing the area of business continity and the IS restoring of the auditee was found that *there had not been adopted any inter-organizational directives which would define activity description that is necessary to perform for accidents, malfunctions and other special situations in the auditee´s IS. Moreover also had not been adopted documents that would define preventative measures for reducing the generation special situations and would describe the possibilities of effective restoring of the state of the IS before accident thereon to save the continuity of the organization´s activity.*

Moreover it was found that back-up power supply (UPS) of the key elements of the auditee´s IS had not been sufficient for the performance of powering up the key elements of the auditee´s IS.

Recommendations:

To establish and keep the backup copies of the files of the main key, the key applications programs backup copies and documentations for those and operating system programs backup copiesbesides operating place.

To elaborate and adopt the restore plan of the auditee´s IS for case of events circumstances and to save the copies of this plan for the case of unpredictable events on the distant place. To elaborate and perform the restoring tests and the IS restarting inclusive the quick restore of damaged files and to elaborate the formal reports of these tests.

4. The security of the ISPA

4.1 Logical access into the IS

By auditing the logical access to the IS auditee it was found that in the access accounts database in group "Domain Admins" there had been also *active user´s accounts of persons with which the employment relation, actually the finished contract cooperation,* while some these accounts *had the highest access rights.*

Moreover it was found by audit the *insufficient set up system secure policy* in the auditee´s IS, mainly the attributes of the authentication means as it is the change password periodicity, duration of the password, control of the number of the last created passwords, the number of unsuccessful trials on log in where consequently there will occur the temporal or permanent blocking the access account by which the users access to domain of the auditee and others.

Recommendations:

To accept the internal directive which will define the parameters and unified regulations of the access management policy and on its basis to implement these attributes for access to the IS of the auditee. This policy would be documented and revised on the basis of the working and security requests for the access management. Also it is useful to establish the procedure for management of the access to the IS of the auditee by the unique user´s identification form.

4.2 The passwords policy, user´s and administrator´s rights, management of the user rights

By auditing it was found that *internal instructions did not regulat the security policy area* that resulted that the parameters of domain policy passwords as the saving password history, maximal and minimal password vitality and others, had not been regulated by any internal instructionsof the auditee.

By auditing it was found that in the computer domain of the auditee existed the administrator´s accounts, i.e. access accounts with the highest rights which did not have forced password change over fixed period. Also it was found that *the system contained the access accounts with privileged rights access also for employees the work duties of which and working position did not meet approved access rights.*

Moreover it was found by auditing that in domain group "Domain Admins" which had the highest rights in the computer´s network of the auditee, there had been existed the active *administrator´s accounts which had been established for the several external ICT services suppliers.* These third parties accessed to computer domain of the auditee through the Virtual

Private Network (further only "VPN connection") while they had *unrestricted access* to every computer inclusive the server and domain controllers. By auditing it was found that the activity of these accounts *was not evaluated (analysed)* by means of individual systems audit records (logs).

Also it was found that in the IS of the auditee there *existed an active domain administrator´s and user´s accounts of the users which had finished their employment with the auditee.*

Recommendations:

To adopt the internal directive in which it will be determined the security parameters of the domain policyand on its base to implement these attributes for the access to the IS. The passwords dispatching would be managed through the formal managing process. The regular user activities would not be performed under the privileged accounts. The dispatching of the privileges would be managed through the formal authorized process.

4.3 The access of the third parties to the auditee´s information systems

In the field of the third parties access to the IS of the auditee it was found that auditee had not approved internal directives which would define the conditions for the access of the third parties to its IS. In one case it was found that the third party performed also administration activities in the databases and the systems over the scope of the contract subject.

Several external companies – third parties - had the remoteaccess through the VPN services into the IS of the auditee. Another checking from the point of view of the access to the auditee´s IS disclosed that some third parties had access to the IS of the auditee through the administration domain account while in the time of audit performance there had been mentioned administration accounts active.

The SAO SR´s audit found that *in the time of audit performance one of the ICT external service contractors* had the active administration account to the IS of the auditee also *inspite of that the service delivery had been finished in the year 2010.*

Moreover it was found that another ICT external service contractor on the basis of the work sheets inter alia performed also *the activities that had not been the subject of the contract.*

In both cases *the access management, security risk analysis, audit records evaluation etc. had been missed from the side of the auditee.*

Recommendations:

To adopt the internal document by which the access conditions for the third parties would be defined to the IS of the auditee. Monitoring and services revision provided by the third parties would be able to guarantee the conditions and regulations concerning the information security will be adherence and the security problems and incidents will be properly managed.

It is suitable to create mutual guidance relation relative the delivering services, between the organization and the third party that enables:

- Monitoring service performance level by which it is verified the compliance with the conditions determined by contract,
- Providing the information on information security and their revision.

In the case of the contracts with the external service delivers to specify exactly the security conditions for the delivering services (far access, access management, generating the audit records of the third parties activities and their regular evaluating etc.)

4.4 Physical security of the ICT

By auditing the physical security of the technological room, containing the key elements of the IS of the auditee, has been found *inadequate physical security of this place and also there had been the matters directly unrelated with the purposeof this room.*

Recommendations:

Ensure the physical security of the technological room in compliance with its purpose. Further to remove the inflammable materials from the server room place and relocate from this server room the matters directly unrelated with the purpose of the server room. Also establish hand-held warehouse in the suitable closeness of the server room for the needs related with the work performance in the server room.

Totally, it had been found 83 findings while the SAO SR suggested the recommendations on the solution of the found shortcomings which had been notified to the responsible persons
of the auditee.