ANNEX 26

Assessment report on the Information Technology (IT) systems at the SSPF

Analyse was performed by expert within the time period November 3-7 2014 for implementation of the activity Activity 2.1 “Thorough assessment of management processes and IT systems of the SSPF” sub-activity 2.1.2 Analysis of the IT systems.

Analyse consists of two parts

1. IT infrustructure analyse been held as defined by The Information Technology Infrastructure Library rules (ITIL). ITIL is covering all the processes that monitors all events that occur through the IT infrastructure.

2. IS (information systems) security analyse been held in accordance with ISO 17799:2005 standards.

The analyse results related to ITIL best practices and accordance to the international standard ISO 17799: 2005 requirements show IS weaknesses and failures. The results represent the view of the experts for the overall analyse compliance requirements. The analyse results are based on the situation at the time of the audit and the information provided by the interviewees base.

1. Description of IS infrastructure and architecture

Azerbaijan Republic Social State Protection Fund’s headquaters are located in Baku and there are more than 80 SSPF’s branch offices in the regional centers. Information Technology had always played a key role in processing of information and serving clients.

Current IT infrastructure consists of Data center located in Baku HQ and more than 80 local system/networks. There are 2500 users of IT infrustructure being supprted by 15 IT specialists as well as outsourced companies. Management of IT infrastructure is centralized. Users are equiped with approximatelly 2500 PCs and thin clients; there are 600 printers.

Systems in use: Recordkeeping, Accountancy and Personnel administration system, all developed in Azerbaijan.

Azerbaijan Republic Social State Protection Fund’s Business System (Oracle based systems) has been developed in order to ensure pension calculation and payment.

Systems consist of:

* Personal Accounting system,

* Portal,

* Social contributon system,

* Pension system

Finanse

Organization budget

Fund budget	2012	2013	2014
Annual budget	18 431 645,16	22 719 296,34	

IT budget

	2012	2013
IT budget, including	261 599,21	1 476 121,89
Network services	9 847,20	19 835,00
Services	36 367,60	50 820,24
Equipment	215 384,41	1 367 966,65

2. The Information Technology Infrastructure Library

ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

NR	PROCESS	STATEMENT
1.	**Incident management** The first goal of the incident management process is to restore a normal service operation as quickly as	Incident management is performed and incident records are kept by the outsourced service provider, who is also providing incident solving solutions.

	possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.	
2.	**Problem management** Problem management aims to resolve the root causes of incidents and thus to minimise the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.	Problem management is performed by the outsourced service provider who is interested in preventing the problems since the payment is made on the principle of a fixed amount regardless of the number of problems, hense the interest to reduce their costs.
3.	**Change management** Change management aims to ensure that standardised methods and procedures are used for efficient handling of all changes.	Change management is performed, but not fully documented. There is a risk that a shortage of qualified personnel may affect the operational management. Changes in the systems can be centralized with the help of Microsoft management tools.
4.	**Version control** Version control aims to ensure that all the changes to IS are tracked and documented. Version control provides the function to have the opportunity to return to a certain version of the system.	Version management is performed, but not fully documented. There is a risk that a shortage of qualified personnel may affect the operational management. Version control of the systems can be centralized with the help of Microsoft management tools.
5.	**Configuration management** Configuration management is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships.	Configuration management is performed, but not fully documented. There is a risk that a shortage of qualified personnel may affect the operational management. Configuration management is provided by the backup-building principles.
6.	**Service-level management** Service-level management provides continual identification,	Some elements of the service-level management are implemented, but are not used in full view of the concept of service. Service quality key points are not

	coordination, monitoring, planing and review of the quality of IT services.	defined. IT services are not defined in the Service-level agreements (SLAs)
7.	**Financial Management** of the services comprises the discipline of ensuring that the IT infrastructure is obtained at the most effective price to achieve the necessary quality of service.	Financial Management of the services is performed since most of the services are provided by outsourced companies through the a purchase procedure (lowest price criteria)
8.	**Capacity management**. Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands.	Capacity management is performed, but no methodological materials(instructions) have been developed in order to ensure and plan resource capacity.
9.	**IT service continuity management** IT service continuity management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs. It is not just about reactive measures, but also about proactive measures – reducing the risk of a disaster in the first instance.	IT service continuity management: An assigned personnel is responsible for the continued operation of the system/equipment. Outsourced service providers contracts include penalties in case of failure of system operation.
10.	Availability and reliability of IT infrastructure and organizational optimization, to ensure fulfillment of business requirements.	Availability management is performed by the outsourced service provider, who is interested in the availability of the system to be close to 100%.

3. ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

NR.	PROCESS	STATEMENT
1.	**Organization of Information Security**	Institution carries out security policy and Institutional management is interested in the IS security aspects, but not fully documented. Governmental security authority is responsible for setting safety and security requirements and is performing necessary checks.
2.	**Privacy and security policies**	Users are informed about their rights and obligations. User data protection rules are respected.
3.	**Risk assessment and treatment**	Risk assessment and treatment is provided by governmental security authority.
4.	**Human resources security**	Users regulary go through trainings.
5.	**Physical and environmental security**	Physical and environmental security is performed. There are server rooms with air conditioning and cooling, extra power supply and other necessary safety features.
6.	**Asset management**	Asset Management identifies both material and security responsibilities.
7.	**Asset acquisition, development and maintenance**	IS are equiped with antivirus software, security tests are perfomed on a centralized basis.
8.	**Authentication and access control**	User authentication and access control is performed.
9.	**Mobile computing and tele-working**	Use of portable devices(mobile computing) is restricted, therefore it is considered that the riski s managed.
10.	**Operations management**	IS perimeter is secured with firewall, internal network is motiroed, security checks are performed by outsourced company.
11.	**Data lifecycle management**	Regular scheduled backups: Data center – daily

		Branch offices – weekly
12.	**Monitoring and audit logging**	User actions are monitored in order to trace the incidents. Oracle based security log is used in order to protect the information.
13.	**Information security incident management**	Information security incident management along with incident analysis is performed.
14.	**Business continuity (disaster recovery) management**	Business continuity (disaster recovery) management is taken into consideration, but since the processes and regulations are not documented there's a risk that in case of incident user viewpoints/opinions will vary.
15.	**Compliance with external and internal requirements**	External security requirements are met since regular external controls/checks take place.
16.	**Data sensitivity classification**	Data is not classified, but considering the internal work culture and external security requirements of the institution, it can be said that Institution information is sufficiently protected.

4. Recommendations

4.1. The Information Technology Infrastructure Library

4.1.1. Develop information systems maintenance and development plan - IT architecture, which describes the existing ICT infrastructure maintenance and replacement rules, the principles of information systems maintenance and development, necessary financial and ICT capacity calculations.

IS maintenance and development plan would allow the Fund management:
- get the IT costs in the long term,
- be confident about their spending is justified,
- deliberately push IT resource development.

IT costs has to be planned at least for 5 years.
This task is necessary to attract external consultants to prepare the first documents versions that it can maintain by IT Department.

4.1.2. Document incident and problem-solving management; implement incident and problem tracking system - set up a help desk.

This task is necessary to attract external consultants to develop the Fund IS processes according ITIL, to train the management of the Fund and IT Department, to develop Service Desk system technical specifications and help implement the Service Desk system (Staff and Information system).
Help desk staff should be to coordinate all ICT problems management. With Help desk information system the Fund management – known as the IS works, what are the problems, what are the reasons for business activity and problems (bad working IS, IS users do not have sufficient competence, IS users are not sufficiently precise legislative acts of violence, etc.) in the operation of the business. Developing and implementing

ITIL principles the Fund management to ascertain the criteria by which to assess the significance of the information system and in the operation of the Fund, which is reaching a critical situation to take appropriate decisions.

4.1.3. Develop requirements for external service providers in order to precisely define the level of service received (response time, acceptable downtime, etc.). Such requirements to permit more accurate to procurement procedures, to procure external service providers, to define the Fund for external service providers and easier to gain confidence in the quality of service delivery.

This objective is closely related to the implementation and operation of the task 4.1.2. and can perform the same consultants who develop the previous point.

4.1.4. Document system configuration, develop configuration and release management plans.

This package will enable the management of IT systems, be sure that the IT provider control the situation in critical situations and will be able to restore system operation.
This document must be attached to the development of advisers who trained IT Department staff how to develop such documents. The same documents shall be drawn up either in the IT department or system external suppliers, according the specification of IT Department.

4.2. IS Security Management

4.2.1. Perform risk analysis and develop results-based security policies that can be described in the following documents:

4.2.1.1. IS security regulations;

4.2.1.2. IS user security instructions;

4.2.1.3. Information classification regulations;

4.2.1.4. Resource classification rules;

4.2.1.5. Physical Security Regulations;

4.2.1.6. User Rights Assignment procedure;

4.2.1.7. Others

4.2.2. Introduce developed IS security policy, appoint responsible personnel, implement information and resources classification, perform user training.

4.2.3. Develop IS sevice continuity plans, perform IS service continuity plan testing.

This task is necessary to attract the consultants. After risk analysis and the training of the IS security principles the Fund management will be able to assess the necessary steps must be taken to improve the IS security.