ANNEX 28

Annex1 of Annex 4

***Twinning Project** AZ/13/ENP/SO/24*

Valdis Supe

Expert

IT system analysis

The 17th of June, 2015

MINISTRY OF WELFARE
OF THE REPUBLIC OF LATVIA

ISSMF

Gesellschaft für
Versicherungswissenschaft
und -gestaltung e.V.

GVG

Analysis

- IT process - The Information Technology Infrastructure Library rules (ITIL)
- IT security - ISO 17799:2005 standards

ITIL

NR	PROCESS	STATEMENT
1.	Incident management	Incident management is performed and incident records are kept by the outsourced service provider, who is also providing incident solving solutions.
2.	Problem management	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 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.

…

NR	PROCESS	STATEMENT
4.	Version control	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 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	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 defined. IT services are not defined in the Service-level agreements (SLAs)

...

NR	PROCESS	STATEMENT
7.	Financial Management	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 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: 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	Availability management is performed by the outsourced service provider, who is interested in the availability of the system to be close to 100%.

ISO/IEC 17799:2005

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.

...

NR.	PROCESS	STATEMENT
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.

...

NR.	PROCESS	STATEMENT
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.

...

NR.	PROCESS	STATEMENT
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.

Recommendations - ITIL

- IT architecture - develop information systems maintenance and development plan
- IT process description - document incident and problem-solving management
- Help desk
- Develop serviss level agreement Develop configuration and release management plans

IS Security Management

- Perform risk analysis
- IS security policy:
  - IS user security instructions
  - Information classification regulations
  - Resource classification rules
  - Physical Security Regulations
  - User Rights Assignment procedure
- Implement IS security policy
- User training
- IS service continuity plans

Information

- **ITIL** https://en.wikibooks.org/wiki/Category:ITIL_v3_(Information_Technology_Infrastructure_Library)
- **IS Security Management**

Standarts

Best practice

Information Security Policies Made Easy

- Access Control
- Acceptable Use
- Application Development
- Biometrics
- Computer emergency response teams
- Computer viruses
- Contingency planning
- Corporate Governance
- Data Classification and Labeling
- Data Destruction
- Digital signatures
- Economic Espionage
- Electronic commerce
- Electronic mail

- IEmployee surveillance
- Encryption
- Firewalls
- FAX communications
- Incident Response
- Identity Theft
- Information Ownership
- Information Security Related Terrorism
- Internet
- Local area networks
- Intranets
- Logging controls
- Microcomputers
- Mobile Devices
- Network Security
- Outsourcing security functions
- Password Management

- Password Management
- Personnel Screening and Security
- Portable computers (PDA, Laptops)
- Physical Security
- Privacy issues
- Security Roles and Responsibilities
- Social Engineering (including "phishing")
- SPAM Prevention
- Telecommuting
- Telephone systems
- Third Party Access
- User security training
- Web Site Security
- Wireless Security
- Voice Over IP (VOIP)
- *And many more!*

Question