TWINNING CONTRACT

JO/13/ENP/ST/23

Strengthening the capabilities of the Department of Statistics in Jordan

MISSION REPORT

on

Activity: 4.4 Plan for database structure - III

Mission carried out by
Poul Valeur, Statistics Denmark
Bo Guldager, Statistics Denmark

1-5 June 2014

Version: Final

STATISTICS DENMARK

Istat
Istituto Nazionale di Statistica

DOS 1949

Expert contact information

Povl Valeur
Statistics Denmark
Sejrøgade 11
DK-2100 Copenhagen Ø
Denmark
Tel: +45 39 17 35 89
Email: pov@dst.dk

Bo Gudager
Statistics Denmark
Sejrøgade 11
DK-2100 Copenhagen Ø
Denmark
Tel: +45 39 17 38 15
Email: bgc@dst.dk

Table of contents

List of Abbreviations

DoS	Department of Statistics of Jordan
DSt	Statistics Denmark
GIS	Geographic Information System
QoS	Quality of Service
SGN	Secure Governmental Network
ToR	Terms of Reference
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1. General comments

This mission report was prepared within the Twinning Project ”Strengthening the capabilities of the Department of Statistics in Jordan”. It was the third mission within Component IT and online dissemination of the project.

The purpose of the mission was primarily to assess the current status of IT systems and to look into IT Security.

The consultants would like to express their thanks to all officials and individuals met for the kind support and valuable information which they received during the stay in Jordan and which highly facilitated the work of the consultants.

This views and observations stated in this report are those of the consultants and do not necessarily correspond to the views of EU, DoS or Statistics Denmark

2. Assessment and results

2.1 Activities during the mission:

Sunday June 1

- Startup meeting with Thomas Olsen discussing the mission.
- Introduction to IT infrastructure at DoS.
- Introduction to IT infrastructure at Statistics Denmark.
- Compare IT infrastructure at DoS and Statistics Denmark.
- Report writing

Monday June 2

- Preparation.
- Continue comparing IT infrastructure at Dos and Statistics Denmark.
- Discussions on storage technologies.
- Inspection of datacentre.
- Discussions on technical aspect of IT security like network segmentation, firewall, IPS, Denial of Service.

Tuesday June 3

- Preparation.
- Presentation of ISO27001 standard
- Discussions of the ISO27001 standard related to DoS.

Wednesday June 4

- Report writing
- Discussions of tender specification for tablets to be used in the Census.
- Cultural exchange
- Meeting with representatives from Microsoft, Dell and Intel regarding choice of supplier for tablets.
- Discussions of tender specification for census website.

Thursday June 5

- Report writing

2.2 Assessment of the current IT infrastructure

The IT infrastructure is mostly supported by the IT department who is responsible for implementation, configuration, maintenance and support of all IT operations in the organization. In addition, the IT department is also responsible for data entry, application development and processing in databases.

Part of the IT infrastructure is outsourced to Secure Governmental Network (SGN). SGN operates a number of services for most govermantal institutions in Jordan:

- Common Active Directory where SGN is hosting the top level domain, and DoS has implemented a local chield domain.
- Mail services (Exchange 2010) including antivirus and antispam.
- Ingoing internet access to DoS's external services as webpages.
- Outgoing internet access for the employees of DoS. The traffic is being scanned for unwanted behaviour by a Blue Coat proxy.

DoS's web services are exposed via a DMZ on a local ASA firewall maintained by SGN. There is as limitation on 5 Mbit on the connection to the SGN network. 1 Mbit of this connection is dedicated to the GIS team.

Regional offices are connected to a single computer at DoS via ADSL connections secured by VPN. The connection is used for transferring data and nothing else.

The network administrators at DoS can do the daily administration of users, mailboxes and local network, without support from SGN.

The LAN is implemented with a Cisco 3750 switch stack as core switch, while workstations are connected to Cisco 2960 switches. There are implemented separate VLAN's for each floor in every building related to business roles, and the VLAN's are routed by the core switch.

Oracle is the application for statistical databases for both internal production and for dissemination. Oracle is running on the Solaris operating system. This choice has been done from both security and economic aspects. Oracle has a less strict license policy on Solaris servers compared to fx. Microsoft Windows.

The website is running Apatche on a Solaris server and the Oracle database for dissemination is stored on the same server. Dissemination data are replicated from the internal Oracle production database to the local database on the webserver.

The datacentre seems to be old and there are problems with physical environment. Part of the floor is missing, and it is risky for the IT staff to go around. 4-5 racks are placed in the room, but there is a lot of free space in most of the racks. There is a lot of stuff in the room not related to IT.

Most of the workstations are running Windows 7, but approximately 100 computers can't be upgraded because of outdated hardware. There are also problems with an application form from Oracle named Oracle Discover, where connection form the application to the Oracle database can't be initiated on Windows 7 computers.

Programmers and other special users have administrative privileges on workstations. They can do configuration and installation of software if needed. The IT staff is doing manual installations of software for the rest for the employees

2.3 IT Security

ISO 27001 - the international standard for IT Security was discussed in detail
With the following headlines corresponding to the similar named clauses in the standard:

Context of the organization

- Understanding the organization and its context
- Understanding the needs and expectations of interested parties
- Determining the scope of the information security management system
- Information security management system

Leadership

- Leadership and commitment
- Policy
- Organizational roles, responsibilities and authorities

Planning

- Actions to address risks and opportunities
    - General
    - Information security risk assessment
    - Information security risk treatment
    - Information security objectives and planning to achieve them

Support

- Resources
- Competence
- Awareness
- Communication
- Documented information
    - Create, Update, Control

Operation

- Operational planning and control
- Information security risk assessment
- Information security risk treatment

Performance evaluation

- Monitoring, measurement, analysis and evaluation
- Internal audit
- Management review

Improvement

- Nonconformity and corrective action
- Continual improvement

The concepts of CIA (Confidentiality, Integrity and Availability) in IT Security was discussed with the participants and it was emphasized that this concept is the red tread through the process of compliance

Technically DoS is in a good position since the needed skills, procedures and systems are already present to a large extent in the opinion of the experts, but there is clearly a need for more focus from top management on the subject of IT Security.

3. Conclusions and recommendations

3.1.1 External network connection

The services supported by SGN seem to be a good solution for DoS. A number of security issues are handled by the support team at SGN, and DoS does not have to implement solutions on their own.

There are some subjects where the solution causes problems. DoS have a 5 Mbit connection to the SGN network, and this limitation often causes problem for external users when browsing the website of DoS. The same is true for internal users when browsing other web sites on the internet. In the period where census data is reported from the field, there will be an increased need of capacity on the internet connection. After publishing the result of the census DoS can expect many visitors to the census website.

It is recommended to consider the following:

- Upgrade the bandwidth on the connection to SGN network/internet, especially during the census.
- Connect the regional offices directly to the SGN network to avoid the use of extra ADSL connection.
- Verify with the SGN support team if QoS is possible to ensure bandwidth for external users to the web site.
- It was not clear to the MS experts if the internet connection from the SGN network is protected against Denial of Service attacks or an Intrusion Prevention System is setup to protect the traffic. Verify with the SGN support team if the connection is protected.
- Testing security by third part provider.

3.1.2 Internal network

The internal network has been upgraded and standardized a year ago, and there seems to be a robust design behind the technical implementation. All VLAN are routed witch without any restrictions between workstations, servers and other equipment. It is recommended to consider a more restricted internal network infrastructure, with limitations on access to central services like databases, by implementing internal firewall or access control lists in the routing equipment.

3.1.3 Datacenter

It is recommended to implement a new datacentre. These are some standard guidelines for server room:

- Rack mounting of all equipment. No servers etc. should be placed on the floor or on tables.
- Cooling. The cooling system should be energy effective and use as little power as possible. Possible solutions:
    - Cool the entire server room (not recommended)
    - Inline cooling system directly in the racks.
    - Divide the server room into cold and warm zones. Cold air is coming up from the floor in front of the servers placed in a closed cold cube. The rest of the server room is warm (the solution at DSt)
    - Redundant cooling system.
- UPS for power protection in case of external power breakdown. A power generator can be considered if this makes sense, especially if there are many problems with power.
- Fire prevention
- Restricted access to the server room.
- Do not place server room under toilets or other room with water.
- Do not place server room on ground floor or lower.
- Do not place any unnecessary stuff in the server room.

3.1.4 Server hardware and virtualization

The hardware for the internal Oracle production database is 10 years old, and does not have the technical specification for a performance effective database server anno 2014. The memory is limited to 6 GB and it is not possible to expand the capacity of disk space according to the IT staff at DoS. The server should be replaced with new hardware because of poor performance.

There are a number of Windows servers that could be virtualized on a virtual cluster with 2 or 3 physical host servers. The virtualization software can be from VMWare, Oracle, Microsoft etc. Virtualization will make specifications for the server room less demanding.

Documents are stored directly on the local workstations and manually backed up to a common fileserver, but there is no procedure for the backup. Important documents can be places on workstations and never be part of a backup. It is recommended to place all documents on a centralized fileserver instead of storing documents on local workstations. The fileserver should be part of the daily backup.

Restrict non work related files on the fileserver.

3.1.5 Workstations

Around 100 of the workstations at DoS are running Windows Xp, because of old hardware or problems with Oracle Discover on Windows 7. Microsoft has stopped support of this operating system, and it is no longer possible to download security updates form Windows Update or WSUS server.

It is recommended to replace the outdated workstations with new workstations running Windows 7 like the rest of workstations.

It is recommended to contact Oracle get a solution to the problem with Oracle Discover.

3.1.6 IT Security

The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization.

It is important that the information security management system is part of and integrated with the processes of DoS and the overall management structure and that information security is considered in the design of processes, information systems, and controls.

In the opinion of the experts that for an organization of the size of DoS it will most likely be enough to have at least one person (Security Officer) dedicated to the task of IT-security.

It must however be observed that the need for resources is highly dependent on the level of ambition when implementing IT Security and that it **shall be backed up by the Top Management at all times in order to be successful.**

Annex 1. Terms of Reference

Terms of Reference

EU Twinning Project JO/13/ENP/ST/23

1-5 June 2014

Component 4: IT and Online Dissemination

Activity 4.4: Plan for database structure - III

0. Mandatory results and benchmarks for the component

- New database structure defined and online dissemination improved (Apr 2015)
- Assessment report on current situation (Jan 2014)
- Develop a plan for the database structure (July 2014)
- Improve the IT-security (Jan 2015)
- Improve the online dissemination (Apr 2015))

1. Purpose of the activity

- To review the current IT security measures taken in DoS
- To discuss technical aspects of IT security, e.g.:
  - Firewall
  - IPS (Intrusion Prevention System)
  - VPN, encryption of data over the Internet
  - Proxy
  - Antivirus
  - Updates of the operation system and software
  - Penetration test
  - Access via duplication
  - Back up / duplication
  - To discuss security issues especially related to Windows XP
- To discuss organisational aspects of IT security, e.g.:
  - IT security policy – the overall responsibility for the IT security is anchored in the top management
  - Organisation related to IT security
  - Administration of rights (procedures, periodic follow up etc.)
  - Awareness among staff

2. Expected output of the activity

- Recommendations prepared on how to improve the IT security in relation to the technical aspects
- Recommendations prepared on how to improve the IT security in relation to the organisational aspects
- To prepare a first draft (outline) of a DoS IT Security Policy meeting European Union standards
- Transfer of the Danish and in general the European Union, experience regarding IT security

3. Participants

DoS
Mr Tayseer Deeb, Director of Information Technology (*Component Leader*)

Component team members…

MS experts
Mr Povl Valeur, Head of IT, IT Department, Statistics Denmark
Mr Bo Guldager, Chief Adviser, IT Department, Statistics Denmark

Programme for the mission

Time		Place	Event	Purpose / detail
Sunday, morning	08.30 – 10.00	Hotel /DoS	Meeting with RTA	To discuss the programme of the week
Sunday, morning	10.00 – 12.00	DoS	Meeting with BC Component Leader and BC Experts	Discussions of the weeks programme Brief introduction to the Danish experience with IT-security
	12.00 – 01.00		Break / Preparations / Report writing	Break / Preparations / Report writing
Sunday, afternoon	01.00 – 03.30	DoS	Meeting with BC Component Leader and BC Experts	Discussions of technical aspects of IT security
	03.30 – 04.00		Preparations / Report writing	Preparations / Report writing
Monday, morning	08.30 – 09.30	DoS	Preparations / Report writing	Preparations / Report writing
	09.30 – 12.00		Meeting with BC Component Leader and BC Experts	Discussions of technical aspects of IT security
	12.00 – 01.00		Break / Preparations / Report writing	Break / Preparations / Report writing
Monday, afternoon	01.00 – 03.30	DoS	Meeting with BC Component Leader and BC Experts	Discussions of technical aspects of IT security
	03.30 – 04.00		Preparations / Report writing	Preparations / Report writing
Tuesday, morning	08.30 – 09.30	DoS	Preparations / Report writing	Preparations / Report writing
	09.30 – 12.00		Meeting with BC Component Leader and BC Experts	Discussions of organisational aspects of IT security
	12.00 – 01.00		Break / Preparations / Report writing	Break / Preparations / Report writing
Tuesday, afternoon	01.00 – 03.30	DoS	Meeting with BC Component Leader and BC Experts	Discussions of organisational aspects of IT security
	03.30 – 04.00		Preparations / Report writing	Preparations / Report writing
Wednesday, morning	08.30 – 09.30	DoS	Preparations / Report writing	Preparations / Report writing

	09.30 – 12.00		Meeting with BC Component Leader and BC Experts	Discussions on what should be included in a DoS IT-security policy
	12.00 – 01.00		Break / Preparations / Report writing	Break / Preparations / Report writing
Wednesday, afternoon	01.00 – 03.30	DoS	Meeting with BC Component Leader and BC Experts	Discussions on what should be included in a DoS IT-security policy
	03.30 – 04.00		Preparations / Report writing	Preparations / Report writing
Thursday, morning	08.30 – 09.30	DoS	Preparations / Report writing	Preparations / Report writing
			Meeting with BC Component Leader and BC Experts	Final discussions on what should be included in a DoS IT-security policy
	09.30 – 11.30		Ad-hoc meetings	Final clarifications with BC Experts, preparation of report and presentation for BC Project Leader
Thursday, morning	11.30 – 12.30	DoS	Meeting with BC Component Leader	Presentation for BC Project Leader
Thursday, noon	12.30 – 01.00	DoS	Debriefing with BC Project Leader	Conclusions and decisions and their consequences for the next activity and the implied work programme for BC Experts

Annex 2. Persons met

DoS:

Tayseer Deeb (Head of IT Department Twinning Team Member)
Yasir Nasrallah (Head of Technical Support Division)
Rana Swaidat (Head of Information Technology Development Division Twinning Team Member)
Rania Abu Dhaim (Head of Analysis and Programming Division Twinning Team Member)
Hussam Abu Shukur (Head of Web Dissemination Division & Twinning Team Member)
Eng. Mohammad Sakhrieh (Network Engineer & Twinning Team Member)
Mohammad Shatnawi (System Engineer)
Eng. Haneen Ananzeh (Technical Support Division)

External stakeholders:

RTA Team:

Thomas Olsen (RTA)
Amal Aliah (RTA assistant)