Report from a short-term Mission on ICT upgrading, maintenance and verification

26 August – 6 September, 2013

within the frame work of the

**AGREEMENT ON CONSULTING ON
INSTITUTIONAL CAPACITY BUILDING,
ECONOMIC STATISTICS AND RELATED AREAS**

between

INE and Scanstat

Bo Guldager Clausen

INSTITUTO NACIONAL DE ESTATÍSTICA

Bo Guldager Clausen
Statisitcs Denmark
Sejrøgade 11, 2100 Copenhagen Oe, Denmark
bgc@dst.dk
+ 45 39 17 39 17

Table of contents

List of abbreviations

DBA	Database Administrator
INE	Instituto Nacional de Estatística, Mozambique
IIS	Internet Information Server (A Microsoft product)
MZM	Mozambique Meticais
PX	Family of Software produced by Statistics Sweden
Scanstat	Consortium between Statistics Denmark, Statistics Norway and Statistics Sweden
SDMX	Statistical Data and Meta data exchange
SQL	Structured Query Language
XML	Extendable Mark-up Language

1   EXECUTIVE SUMMARY

Scope of the mission

The main focus of the mission was to follow up on the implementation of virtualization, network and storage made by DATASERV.

The implementation is not completed, but some of the outstanding tasks were implemented during the mission done in collaboration with DATASERV. Other outstanding issues that were not related to DATASERV were also implemented in collaboration between the IT Staff and the consultant. A number of old Windows servers can be shut down when data is migrated to the new fileserver or database server.

The new infrastructure enables INE to operate a stable IT environment with the possibility of expansion with additional resources whenever the need arises.

The virtual Hyper-V installation is based on an older version of Windows Server, and not the latest version. INE does not have the necessary licenses for the latest version of Windows Server, but negotiations with Microsoft about upgrading licenses are in progress. It is not known what the economic consequences will be for INE.

The IT staff now has a new system without having received all the necessary training. DATASERV has done some training as part of the implementation process, but there is a significant need for training of IT staff, to make employees able to manage the most important systems in the new IT infrastructure.

The lack of skills among staff makes it questionable whether INE has the ability to operate its own IT environment in a stable and secure manner. In case of minor or major crashes there will be a great dependence on DATASERV. This can of cause be an informed decision by senior management, but otherwise training the IT staff should have high priority.

It becomes very difficult to take advantage of the many new opportunities that the new technology makes available. If the IT staff does not have insight and skills to exploit the technology, then INE will not get the full benefit of the investment.

Implementation of documented procedures for daily tasks can help to improve the professional skills for the IT staff seen as a group. Sharing of knowledge will help to balance the workload individual that IT staff members are exposed to.

During review of the Cyberoam firewall, it was found that TDM does not deliver the agreed 4 Mbit bandwidth internet connection, as INE is paying for. The effective download is between 2 and 2.5 Mbps.

1 SUMÁRIO EXECUTIVO

Âmbito da missão

O foco principal da missão era de acompanhar a implementação da virtualização, da rede e do armazenamento feita por DATASERV.

A implementação não está concluída, mas algumas das tarefas pendentes foram implementadas durante a missão em colaboração com o DATASERV. Outras questões pendentes que não foram relacionados com o DATASERV também foram implementados em colaboração entre a equipe de TI e consultor. Uma série de antigos servidores Windows podem ser desligados quando os dados são migrados para o novo servidor de arquivos ou servidor de banco de dados.

A nova infra-estrutura permite INE para operar um ambiente de TI estável, com possibilidade de expansão com recursos adicionais sempre que necessário.

A instalação virtual do Hyper-V é baseado numa versão mais antiga do Windows Server, e não na versão mais recente. INE não tem as licenças necessárias para a versão mais recente do Windows Server, mas as negociações com a Microsoft sobre a actualização de licenças estão em andamento. Não se sabe quais as consequências económicas será para o INE .

A equipe de TI tem agora um novo sistema sem ter recebido todo o treinamento necessário. DATASERV fez algum treinamento como parte do processo de implementação, mas há uma necessidade significativa para a formação da equipe de TI, para fazer os funcionários capaz de gerir os sistemas mais importantes na nova infra-estrutura de TI.

A falta de habilidades entre os funcionários torna questionável se INE tem a capacidade para operar o seu próprio ambiente de TI de uma forma estável e seguro. Em caso de acidentes maiores ou menores, haverá uma grande dependência DATASERV. Isso pode ser causa de uma decisão informada pela gerência, mas se não a formação do pessoal de TI deve ter alta prioridade.

Torna-se muito difícil de tirar vantagem das muitas novas oportunidades que a nova tecnologia disponibiliza. Se a equipe de TI não tem conhecimento e habilidades para explorar a tecnologia, então INE não vai obter o pleno benefício do investimento.

Implementação de procedimentos documentados para as tarefas diárias podem ajudar a melhorar as competências profissionais para a equipe de TI visto como um grupo. Compartilhamento de conhecimento vai ajudar a equilibrar a carga de trabalho que os membros da equipe de TI estão expostos como indivíduos.

Durante a revisão do firewall Cyberoam, constatou-se que a TDM não de-fígado a 4 Mbit conexão de internet banda acordada, como INE está pagando. O download efectivo é entre 2 e 2.5 Mbps.

2 INTRODUTION

The mission was carried out 26 August – 6 September 2013.

Review of ICT
infrastructure

The installation of the new ICT infrastructure was done by a local company located in Maputo. The company is named DATASERV and further information can be found on their website www.dataserv-mz.com.

Installation and configuration of network, storage, Hyper-V and other Microsoft services has been carried out by Mr Fernando Lopes, Mr Paulo Saningo and Mr Cassamo Nurmahomed. All three consultants from DATASERV are competent in their work. There seems to be good working relations between the IT staff of INE and the consultants from DATASERVER. This is very important for successful results.

The installation process was started in the end of February 2013. A new core switch was installed and the access networks are partially segmented into smaller units. Hyper-V with and disk system is installed, and 8 virtual servers are running on the system. It appears to be an unnecessarily long period of time for implementation, but the consultant is not sure what exactly is agreed between INE and DATASERV, or what is the background for the long implementation period.

2.1 Network

DATASERV has redesigned the network infrastructure from a flat design with only one VLAN into a segmented network with multiple VLANs.

Each of the access switch stacks will have a separate VLAN and ip address range. The VLANs are connected to the layer 3 core switch, where the traffic is routed between the different VLANs. There has been configured a DHCP relay in the core switch to facilitate the workstations clients with ip addresses from the central DHCP server. Only the switch stacks on 2th and 5th floor are configured as described in the new network design. The rest are still configured as a flat network. The consultant does not know if this is part of the contract. There is a problem with 2 missing GBIC modules to the core switch. The GBIC modules are necessary to implement the mission parts of the new network design.

There was a problem with the ip-phones in the new network design. The workstations are connected to an ip-phone witch is connected to an access switch. The ip-phones did not work when they were placed outside the default VLAN (1). During the mission a solution to this problem was implemented on the access switches with the new VLAN segmentation on 2th and 5th floor. The same solution can be used when the rest of the access switches are connected to the core switch. The procedure for configuration of IP phones and switches is attached to the mission report.

The physical Hyper-V servers are each connected to the core switch with two connections, configured with redundancy for both performance and failover. There is installed as separate 10 Gb switch for interconnecting the Hyper-V

servers to the backend storage. It is important to have at fast and redundancy connection, because a lot of virtual servers are depending on the connection to the storage.

The overall impression of network design is positive, but the task can't be completed due to the missing GBIC modules for the core switch. The best solution might be if the outstanding tasks of configuration are done by DATASERV together with the IT staff. DATASERV have the skills to do the job and IT staff will have hands-on training.

2.2 Hyper-V

DATASERV has installed a Hyper-V failover cluster with two physical HP DL380G8 servers. Hyper-V is part of the Windows Server 2008 and Windows Server 2012 operating systems.

At first the Hyper-V failover cluster was installed with Windows Server 2012, but due to missing licenses the installation was "downgraded" to Windows Server 2008 R2. There is a lot of new functionality in the Windows Server 2012 version of Hyper-V where the following among others can be mentioned:

- Live Migration of virtual servers between physical nodes. Windows Server 2012 Hyper-V provides the ability to migrate virtual machines, with support for simultaneous live migrations. That is, users can move several virtual machines at the same time. Live migrations are not limited to a cluster. Virtual machines can be migrated across cluster boundaries, and between stand-alone servers that are not part of a cluster.
- Live storage migration of virtual servers between disks. Live storage migration allows users to move virtual hard disks that are attached to a running virtual machine. Users can transfer virtual hard disks to a new location for upgrading or migrating storage, performing backend storage maintenance, or redistributing the storage load.

A list of new functionality in Hyper-V on Windows Server 2012 can be found in the document "Feature Comparison Windows Server 2008 R2 Hyper-V and Windows Server 2012 Hyper-V" from Microsoft. This document is attached to the mission report.

Since the Hyper-V installation probably is going to be in production for 5 to 10 years, it must as updated to the newest version at the time of installation, even though it is possible to upgrade later. DISI should examine whether it is possible to purchase 2 Windows Server 2012 Datacenter Edition licenses. This will cover the licenses for the Hyper-V 2012 failover cluster, and all virtual servers running Windows standard editions. By upgrading to Windows Server 2012 the lifetime of the entire system will be extended.

DATASERV has installed 8 virtual servers on the Hype-V cluster. This is servers for mail, antivirus, backup domain controller, MS SQL Server 2008 and a file server. 9 physical servers are still in production in the server room. The IT staff and the consultant made plans for migration of each server.

It may turn out that there are not sufficient resources in the physical Hyper-V server to run all 9 remaining physical server. If this is the case, it will most likely to be insufficient memory resources. This can be solved by adding additional memory in the physical servers. Extra memory will not affect Windows licenses. Another option is to add an existing server with 128 GB to the Hyper-V failover cluster, but this option will cost two extra 10 Gb connections to the SAN, and a Microsoft Windows Server 2012 Datacenter Edition license.

There are no performance issues at the moment.

2.3 Active Directory

A Windows 2008 Active Directory is implemented and the users, computer etc. from the old Windows 2003 are migrated. There is a physical and a virtual domain controller.

A number of Group Policies are configured to implement various settings on the client computers. Intelligent use of Group Policies is a good method to implement standard settings for the IT environment.

2.4 Windows Server Update Service

DATASERV had implemented Windows Server Update Service, but in connection with a power failure, the configuration was corrupted and the service was not able to start. During the mission there were several attempts to restore the configuration, but in the end DATASERV did a new installation on another server.

Client computers download updates from the local Windows Server Update Service at INI if this is possible. Otherwise the client computers will connect directly to the Microsoft service on the internet. All computers have downloaded updates from the internet instead of the local network. This has made an additional load on the heavily loaded internet connection. It is expected that the load on the Internet connection decreases after windows update again function as intended. The less loading is not expected to solve the general performance problems on the internet connection

2.5 File server

In the old IT environment there was a number of Windows file servers, where data and documents were stored. To replace these servers a new virtual Windows file server has been implemented. The process of migrating files from the old file servers is not yet complete, but there are plans for how to do the migration.

File Screening policies are not implemented to avoid the users from storing not relevant files on the network shares. It is ex. possible to store music and movies on the file shares. File screening must have been enabled earlier, as shown in the documentation from DATASERV. The functionality must be activated again.

Quota functionality has been enabled and configured, to set a limit for the disk usage for each user or group.

2.6 Exchange 2010

The Exchange 2010 system has been installed on four virtual servers with different Exchange server roles. A mail server for client access, two servers for mailboxes and a server for the Hub transport role. This distribution of Exchange roles on different servers is an acceptable solution.

INE had many problems with the old Exchange 2003 mail system. One of the main reasons for failures was because the mail database became corrupted when it was full. This should not be a problem in Exchange 2010, but to limit the amount of mails, a quota restriction is implemented for most users. This will ensure that the solution remains fast and reliable.

2.7 Cyberoam security system

There has not been a detailed review of the configuration in the Cyberoam system. The overall impression of the system is positive and the consultant from DATASERV is competent in working with Cyberoam.

A number counters indicators show a proportioned system without any performance issues. The reason for the slow access to the Internet form INE is entirely due to high load on the Internet connection from TDM. Measurements show that TDM does not delivers the 4 Mbit INE pay for, but only about 2,5 Mbit.

2.8 SQL Server

DATASERV has implemented a Microsoft SQL Server R2, with the purpose of consolidate existing database on a one single server. This is a good approach to simplify and streamline the management of INE's databases. During the mission a number of databases were migrated, and procedure for automatic backup was implemented in a workshop with the IT staff.

The professional skills in handling databases are at a very low level. As INE in the future will be more dependent on databases this is worrying and training in the Database Administrator Role (DBA) should be prioritized.

2.9 Backup

The backup solution in the new environment is problematic because of problems with licenses, and uncertainty about which product to be used in the future.

The first plan was to use HP Dataprotector Express, but HP does not support the product any longer. Now there is installed Yosemite ServerBACKUP from Barracudaware, who has have taken over the previous solution from HP. INE has 4 client licenses to HP Dataprotector Express and they can be migrated to Yosemite ServerBACKUP.

INE has to decide if Yosemite ServerBACKUP will be the software to use in the future. If this is the case, then a number of additional backup client licenses must be bought. Another solution would be to purchase a product where the cost is on the backup server, but the backup clients are for free. With this type of license, INE has the possibility to install additional servers without having to pay for additional backup licenses. INE has asked DATA SERVICE for a quote on both solutions.

It would be advisable to buy online backup clients for Microsoft Exchange and Microsoft SQL Server. With this type of backup clients, it is possible to backup running systems in a safe and reliable manner. The different vendors of back-up software have online clients for Microsoft products.

A problem with the Exchange backup was identified. The daily incremental backup fails, and the only backup during the week is the full backup done in the weekend.

The remaining physical servers are not being managed automatically but only manually from time to time.

The backup solution does not run reliably and the problems should be solved urgently.

2.10 Storage

The storage system is an essential core component in any modern IT environment. All virtual servers are assigned to a virtual hard disk. The virtual hard disk makes use of the attached physical storage system. A crash on the disk system will cause all virtual servers to shut down as if the power was lost. Dependency on a reliable disk system is very high and can be compared to the dependency of the network infrastructure. This is a factor DISI has to be aware of.

If the storage system has poor performance, many vital services will become unstable with slow response. The storage system should be monitored to ensure that the necessary capacity in terms of performance and volume in TB. The capacity in performance and volume seems to be OK for the moment. If performance in the future will decrease, consideration should be given to mount faster discs types to parts of the virtual environment. This could by ex. SAS 15K or SSD hard drives for the virtual disks where OS's and databases for the virtual servers are located.

There should at least be made a daily check of hardware and the overall system status. A documented procedure for this operation is attached to the mission report. Procedures for automatic monitoring should be considered.

During the mission, the storage system was software upgraded to the latest version in collaboration with HP, DATASERV and the IT staff. There were known bugs in the older version of the software. The storage hardware was upgraded from 4 to 6 GB memory to support the HP recommended configuration.

To improve security, it is possible to mirror the contents of the disk system to an identical disk system. The mirror operation can be a synchronous or asynchronous. In an asynchronous configuration there will be at defined delay in

transferring data to the secondary disk system. In a synchronous configuration the mirroring are done continuously as data is written to the primary disk system.

2.11 Training needs for IT staff

Through the years there has been a need for training. The IT staff is still in need of getting training and skills in the areas of Microsoft products, general network and disk infrastructure.

There must be a common level of skills among the IT staff, to operate and support a stable operation of servers, storage and network. There is a strong desire among employees about learning new skills. This willingness to learn can be used to improve the skills essential.

Employees must be able to exploit each other's skills and thereby help to raise the common level of knowledge in the group. A method for efficient sharing of knowledge is to document how to do the daily procedures. Examples include managing users, assigning rights, implementation of the PC and backup / restore.

Relevant courses are listed in the recommendations.

The above text referring to lack of training is a direct copy of the text from a short term mission in December 2011. None in the IT staff has had any training for the past years. The last official Microsoft training was in 2005, but no one among the current IT staff has received official training. This is even more critical in the new server environment, where they also have to deal with management of new products like Hyper-V and storage.

DISI must now deal with the situation of having an outside contractor to perform implementation tasks. It is important as a customer to precisely understand the technical challenges, and also be able to set requirements to the supplier. IT Staff in the IT organization must have high level of skills in the applied technologies. Otherwise there will be a risk that the implementations not are the best solutions for the INE.

There has been no tradition of writing documentation for the various daily tasks done in DISI. A large number of procedures can be documented by using simple screen captures with a supplementary text.

During the mission, there were good discussions with many relevant and good questions. The IT staff is committed to their work and willing to perform new tasks. The problem is that they have little knowledge of systems, and therefore have difficulty in improve the professional level without the use of external training. There are major differences in the level of skills between different employees in DISI. This may indicate that resources are not being utilized optimally. It would mean a lot to introduce structured procedures for sharing of knowledge.

Smaller workshops have already been implemented, where an employee with skills in a specified area shared his/her knowledge with the other colleges.

DATASERV will provide documentation for a number of everyday tasks to systems, where they have been responsible for the installation.

A different approach to share knowledge is to implement a helpdesk system. This type of software is good to document the calls DISI receives from users, and continuously build up a knowledge base of problems and solutions. A GOOGLE search "free helpdesk software" found some helpdesk systems for free.

In the report from the Canadian company C2D Services, they also express their concern about the technical skills of the employees at DISI and all of INE. To maintain stable it-services it is important to train the IT staff.

Another option is to outsource some IT functions to an external company. The need for inside information will diminish, but as previously mentioned, it still requires high technical skills to manage and control an IT supplier. By out-sourcing some of the IT tasks to external companies, a part of the IT budget will be spent and not be available to the INE.

3 RECOMMENDATIONS

3.1 Concluding remarks

Thanks to all at INE

Finally I would like to express my thanks to all officials and individuals meet during the mission. They all provided me with the necessary information in a kind and open atmosphere which greatly facilitated my work in Mozambique. But specially, I would like to thank Mr. Lars Carlsson for being an excellent host and for a very constructive sharing of his thoughts on the project and Mozambique.

My best personal professional opinion

It should be noted that this report contains my best personal professional opinions as consultant, and that they therefore do not necessarily correspond to the views of Statistics Denmark, Danida or INE.

3.2 Follow up on recommendations

3.2.1 Follow up on recommendations from January 2004

ID:	Description	Comments	Status
JAN-REC-03	Only store INE relevant data at INE equipment	The content of the fileservers are unknown. When Windows Server 2003 R2 is implemented, it will be possibility to control content by file extensions. The technique allows banning of etc. music and video files, and the users will not be able to store this kind of files. *Windows Server 2008R2 file server is installed and configuration of File Screening is implemented, but for some reason disabled again. The function must be*	On going

		re enabled.	
JAN-REC-06	Centralize software installation	The user still have local administrator on their workstations. Only IT staff should install software. It is also a security risk when the users have administrative rights on the workstations. Virus, worms and spyware have better conditions. When Windows Server 2003 is implemented, the use of group policy can install software on workstations. *Original Microsoft SCCM 2012 was planned to be installed, but was taken out of the scope for the installation don by DATASERV. Part of SCCM 2012 makes it possible to implement centralized software distribution.*	Not Implemented
JAN-REC-09	Add procedures for managing the user accounts.	Procedures for managing the user accounts when employees are hired, move from one part to another inside INI, or leave INE are not implemented. There should be procedures for these tasks. Human resources must provide the network administration with this information. The technical procedures for managing user accounts should be automated by use of scripts or templates. A yearly check for consistency between the user account database and lists of employees from human resources is recommended. *This recommendation can be implemented without any economic costs.*	Not Implemented
JAN-REC-10	Use personal normal and administrative accounts for daily work	The network administrators should have two accounts. One for daily work, and one for when administrative rights is needed.	Implemented
JAN-REC-16	Update operation manual and prepare maintenance documentation for all systems.	Fill out information in the documentation template will give a good basis in a disaster recovery situation. The information should be updates regularly, printed and places in a safe place. This can be the same place as the backup tapes. *As the infrastructure gets more and more complex, the need of documentation increases. INE will be less depending on skills by individuals. There are existing plans on having a changelog where changes are documented.* *The work done by DATASERV has been documented.*	Ongoing
JAN-REC-17	Store important data centrally	The network administration presumes that most data is stored on the file servers. As long as the users have administrative rights on the workstations, they can store data locally. *All users have a home folder on the new file server, where they must to store important data relevant to INE. There has to be done some awareness, to make sure all employees follow the procedure.*	Ongoing

3.2.2 Follow up on recommendations from December 2005

ID:	Description	Comments	Status
DEC09	FSMO roles	Place all Flexible Single Master Operation (FSMO) roles on a domain controller with a tape device. Windows Server 2003 has 5 FSMO roles: Schema master, Domain naming master, PDC emulator, RID master and Infrastructure master. As a general rule, the infrastructure master should be located on a non global catalog server, but in a single domain forest it is not an issue. Both domain controllers should be global catalog servers.	*Implemented*
DEC12	Assign permissions using group nesting	It is recommended to assign file permissions using group nesting. Domain local group are assigned rights on objects. Every user should have a global user group account. This group can be added to the domain local group when permissions are needed.	*Implemented*
DEC17	Knowledge of Linux and open source	It is recommended to get basic skills of Linux for testing purpose. It is possible that part of the environment in the future can run on Linux. It will be advisable to get experience on this platform already now. Also look at open source software. There are many open source application that runs on the Windows platform. For example the Open Office maybe an alternative to Microsoft Office for some users. *At the current situation with new members of the IT staff, this recommendation is not relevant.*	*Wating*

3.2.3 Follow up on recommendations from October 2007

ID:	Description	Comments	
OCT03	GOVNET network	As soon as the GOVNET can offer a faster connection it is recommended to move the traffic from TDM to GOVNET. By now the GOVNET connection is for free, but the bandwidth is too small. GOVNET will also cover the provinces and can be used to connect offices in the provinces to INE. *The plan is to move from TDM to GOVNET and remain TV-Cabo as a redundant internet connection. GOVNET has a 4 Mbit connection for free. GOVNET have been contacted to start implementation.*	*Ongoing*
OCT05	Mail quota	The Exchange has limited resources for storing mails in the database. This has cost INE a lot of problems in the past. The total size of the Exchange 2003 database can be 30 GB, it is recommended to implement mailbox limitations. It is possible to have different limits on different mailboxes. *Implemented in the new Microsoft Exchange 2012 implementation.*	Implemented

3.2.4 Follow up on recommendations from January 2010

ID:	Description	Comments	Status
JAN01	Replacement of server hardware	The server farm at INE is keep getting older, and the wish to split up services from running on one server to run on more servers, can be helped by buying 2 new servers running VMWare. The 2 servers have to be configured with a lot of RAM and CPU cores, with Microsoft Windows Server 2008 R2. The 2 servers running VMware Server can host domain controllers, DNS- and DHCP-servers, Exchange server, file server, print server, MS Forefront server and BlackBerry server. One domain controller should still be physical as it can become difficult to start everything without having a domain controller running. After a power breakdown a domain controller should be started as the first one. The backup server should be physical as well and should be used for backup only. The server hardware should smoothly be replaced to keep the server hardware more up to date. *The Hype-V solution is installed by not all servers has been migrated. Most of the old physical can be shut down as soon as the migration is completed.*	*Ongoing*
JAN02	Administrator password	Both local administrator and domain administrator should have a strong password. The administrator passwords should be changed twice or at least once a year. If one who knows one of the administrator passwords is no longer at the IT staff, the administrator passwords should be changed. It is not a good idea to have people outside the IT staff knowing the administrator passwords. It has been noticed that some local administrators have no password. *This recommendation can be implemented without economic costs.*	*Not implemented*
JAN03	Change log	To share knowledge and to keep track of what changes have been made and why, a change log should be implemented especially for central systems like ISA firewall, DC's and Exchange. The change log should include date for change, who made the change, the change and why the change was made. It is of no cost to implement a change log but it is necessarily that everyone making changes put the change in the log. Otherwise the change log is of	*Not implemented*

		no use.	
		This recommendation can be implemented without economic costs.	
		During the mission there were good discussions on how implementation of a changelog can be done.	
JAN07	Requirements to new members of the IT staff at INE	To avoid any language barriers between members of the IT staff at INE and foreign consultants, using forums on the internet and reading manuals, it is important that members of the IT staff at INE talks and reads English.	*Implemented*
JAN11	VLAN	The network should be segmented into VLANs for security reasons. Now the net 172.16 and 192.168.3 are running on the same physical net and have different rules at the firewall. *DATASERV has designed a new design for the network at INE, and part of the design is implemented. When the 2 missing GBIC moduls for the core switch are purchased, then the implementation can be completed.*	*On going*
JAN12	Certificate	To avoid users of OWA to have the browser giving a certificate error, INE should buy a certificate from a trusted Certificate Authority like Verisign (expensive) or Thawte (less expensive). INE can also consider to buy a wild card certificate (*.ine.gov.mz) to be used on every SSL website from INE. A wild card certificate is more expensive than an ordinary certificate but is very flexible. *The president has on an earlier mission asked for a solution.*	*Not implemented*
JAN13	Workgroup	Members of the IT staff at INE should try to make some connections with members from IT staffs from other institutions in Mozambique to exchange knowledge and ideas. It is a cheap way to learn about new technology and to share knowledge across institutions which can be very helpful. *There have been meeting with the Ministry of education.*	*On going*
JAN14	IT policy	INE should create an IT policy. The IT policy should include rule about what is allowed browsing and downloading from the Internet, how often do users and administrators need to change password, what happens with a user account when an employee stops at INE and so on. *Long term advisor Mr. Mogens Grossen wrote an IT*	*Not implemented*

		Security Policy, but it has never been approved by president. *This is a management decision.*	

3.2.5 Follow up on recommendations concerning the infrastructure at INE's new building December 2011

ID:	Description	Comments	Status
JAN18	Backup	A separate physical server with tape drive and/or attached storage running a well-known and tested backup product like Backup Exec or EMC Networker. Backup needs to be taken often and automatically and can be both backup to tape and disk, and it is important to decide which systems and data need to be backed up. Daily check for success and take action on errors. *New backup solution is installed but there are problems with licenses. The situation is critical.*	*On going*

3.2.6 Follow up on recommendations from December 2011

ID:	Description	Comments	Status
Dec11-01	Training of employees	Recommended following training as a minimum: • Installing and Configuring Windows Server 2012 [20410] • General network understanding Server 2008 R2 course. • Maintaining a Microsoft SQL Server 2008 R2 Database [6231] Exchange 2010 course. • Configuring, Managing and Troubleshooting Microsoft Exchange Server 2010 [10135] Hyper-V is chosen to be the software used for • Implementing and Managing Microsoft Server Virtualization [10215] The Internet contains much documentation concerning almost anything. Remember GOOGLE is your friend. Those who are good to search and understand information on the Internet is a good employee. *There has been no training of IT staff. This recommendation has been updated.* *Do not necessarily send all the IT staff on training, but*	

		start by sending the IT staff members with the best qualifications.	
Dec11-02	Upgrade internal mailsystem to Exchange 2010	The internal mail system is based on Microsoft Exchange 2003 SP2. The latest version is Exchange 2010 has a significantly better performance than the previous version. The maximum recommended mailbox database size has increased to 2 TB in Exchange 2010. It is many times larger than the current database at INE Exchange 2003 server.	*Implemented*
Dec11-03	Virtualization of hardware.	Virtualization is an effective method of running the server infrastructure. In at virtual environment there will be a farm of physical servers from 2 to almost unlimited. The virtual servers can run on any server in the farm. If one of the physical servers breaks down, the virtual server can be moved to another server in the farm in no time. All of INE's present physical servers can be virtualized on two medium sized servers. VMWare, Microsoft and Citrix are three of the marked leaders when it comes to virtualization of hardware. INE should choose the vendor with the best support in Maputo. Microsoft Hyper-V is an integral part of Windows Server 2008 R2 Enterprise edition. It has been reported that INE already have licenses for Microsoft Hyper-V. When this occurs it will be obvious to use virtualization technology from Microsoft. *See comment to JAN01*	*On going*
Dec11-04	Centralized storage system	A central disk system is needed to implement virtualization as the physical hosts must run on a shared file system. This is necessary to move virtual servers from one physical host to another. The connection between the common disk system and physical servers can be done efficiently and cheaply by using iSCSI technology where standard switches are used to create the connection.	*Implemented*
Dec11-05	Testing of emergency power	At the new site UPS and power generator are implemented that can supply servers and workstations in the event of a power failure. The constructor company must prove that the system works by interrupting the injection of power to the building. The functionality should be tested by INE on a regular basis ex. once a month. The test will be to disconnect power to the building and then check that there still are power on the servers, network, storage and workstations. As part of the test, check that there is sufficient fuel in	*Not implemented*

ID:	Description	Comments	
		the tank. If it is not the case there must be a refill of the tank. *There has been a situation where the generator didn't start during an external power Failure. If this is because of a problem with the generator or missing fuel is not clear. Maintenance and test of the generator should be done on a regular basis, ex. once a year.*	
Dec11-06	Block window to the server room	In the server room is a window where the sun shines on much of the day, and generates some heat. The window should be covered to avoid the extra warming.	*Implemented*
Dec11-07	Fire protection of the server room	The door to the server room is an ordinary door like the other doors in the building. It is recommended to install a fireproof door that can resist a fire in the neighboring offices. There should be a pump on the door so that it automatically closes. A door to a server room must be closed by default. There are smoke detectors in the server room but no equipment for automatic fire fighting in case of fire. A facility for automatic fire fighting will be able to protect equipment in the server room efficiently in the event of a fire.	*Implemented*
Dec11-08	Keep order in the server room from the start.	Daily cleaning is more effective if all equipment is mounted in rack cabinets or at lease placed on a table. Dust and dirt can damage equipment in the server room	*Implemented*
Dec11-09	External Security test	An external Danish security company has conducted a security tests up against www.ine.gov.mz. The result is attached to the report. INE must quickly follow up on the recommendations listed in the safety report.	*Unknown*
Dec11-10	Management software to monitor the infrastructure	Monitoring the server and network infrastructure is an important to task. If a services or server break down a message can be sent automatically to the network administrators, who can take action to solve the problem.	*Not implemented*

3.2.7 New recommendations September 2013

ID:	Description	Comments
Sep13-01	Windows server 2012 Datacenter Edition licences	For now INE does not have licences for Windows Server 2012 Datacenter Edition but only for Windows Server 2008 R2 Datacenter Edition. There are many improvements in Windows Server 2012 especially on the Hyper-V part.

		There is governmental agreement with Microsoft, but it was not clear if this also contains server products.
Sep13-02	Temperature in the server room	The temperature is low in the server room. This is not necessary and it can be raised to at least 20-22 degrees without problems. In many datacenter's the temperature is up to 26 degrees
Sep13-03	Air-condition and server rack on the same UPS system	The Air-condition system is not connected to the same UPS system as the server rack. If power is lost to the air-condition system and the servers continues to run, it will cause the temperature to rise in the server room. To avoid this problem, the air-condition system in the server room should be on the same UPS system as the server rack.
Sep13-05	Shut down the servers as they are not in production	When servers are taken out of production, then shut down the server and remove it from the server room. This will reduce power consumption and save a little money

4   APPENDIX 1. List of persons met

INE
Mr. Salomão Muianga
Mr. Paulo Matusse, DDD
Mr. Momade Essumaila
Mr. Mauro Chumaio
Mr. Arlindo Nhaboma
Mr. Ilencia Martins
Mr. Alberto Muchanga
Mr. Euclides Abrao

DATASERV
Mr. Fernando Lopes, DATASERV
Mr. Paulo Saningo, DATASERV
Mr. Cassamo Nurmahomed, DATASERV

Scanstat Consortium, LTA:
Mr. Lars Carlsson, Team Leader

5   APPENDIX 2. List of Literature

All mission reports from the Scandinavian programme are available online on: *www.dst.dk/mozambique*

For this mission I would also like to refer to the reports:

Mission Report from a short-term mission on the ICT situation after move to new site 2 – 11 December 2011 by Bo Guldager Clausen. MZ:2011:09

Mission Report from a short-term mission on Stabilizing and extending the IT-Infrastructure 25 January – 5 February 2010 by Niels Poulin. MZ:2010:01a

Mission Report from a short-term mission on Windows 2003 Migration follow up and maintenance 15 – 26 October 2007 by Bo Guldager Clausen and Niels Poulin. MZ: 2007:11

Mission report from a short-term mission on Win03 and Migration 28 November – 9 December 2005 by Bo Guldager Clausen. MZ:2005:20

6 APPENDIX 3. Terms of Reference

TERMS OF REFERENCE

For a Short-term Mission on ICT upgrading, maintenance and verification

26 August – 6 September, 2013

within the

AGREEMENT ON CONSULTING IN INSTITUTIONAL CAPACITY BUILDING, ECONOMIC STATISTICS AND RELATED AREAS BETWEEN INE AND SCANSTAT.

Consultant*:* Bo Guldager Clausen
Counterparts*:* Salomão Muianga and other staff at DICRE/DISI

1. Background

INE has now moved to the new site and several changes to the ICT environment have been realized. The old and patched network is substituted by a new one with routers on every floor and the server room is gradually equipped with upgraded hardware, among other things with a new physical server capable of running several virtual servers. A local firm has now installed new equipment and updated several of the systems now running on, and around, the servers (see attachment in Portuguese).

2. Main Reasons for the Mission

This short-term mission is to; follow up and verify the work made by the local firm and should be seen as a continuation of the mission made in December 2011 as the proposed new server now has been bought and installed; see the report *MZ-2011-09: The ICT situation after move to new site - Bo Guldager Clausen* at www.dst.dk/mozambique .

3. Beneficiaries of the Mission

The mission will primarily benefit the staff at the IT-Department by providing knowledge of the software and hardware to be used. The beneficiaries in the long run will be the users of the INE network through improved functioning of network dependent processes.

4. Objectives of the Mission

Verify, secure and adapt the new server in co-operation with the DICRE/DISI staff. Propose and make necessary short and long term adjustments. Review and give opinion on the C2D report.

5. Expected Results

A system that gives a secure and stable environment for INE activities is the expected outcome.

6. Work to be carried out by the Consultants
The consultant will make a profound review of the system, including adjustments and proposals wherever necessary.

7. Agenda for the Mission
Working sessions with the staff.

8. Tasks to be done by INE to facilitate the Mission
- Elaborate the Terms of Reference for the mission
- Prepare and supply the consultant with necessary documents and information
- Supply good working conditions for the consultant

9. Timing of the mission
See above.

10. Source of Funding
Project: MPD-2008-0011 – Coordenação e Integração Estatística
PAAO13 – 3.2.1 Arquitectura e Gestão de Bases de Dados

11. Report
The consultant will prepare a draft Technical Report to be discussed with INE before leaving Maputo. A final draft will be submitted to INE for final comments within one week of the end of the mission.

Approved by Cirilo Tembe INE/DICRE

Day / / ....

Confirmed by Leia Macamo, Contract Manager for the INE – Scanstat Contract

Day / / ....

Annex to the Scanstat ToR

Termos de referência pela instalação do equipamento

Enquadrado nos esforços de melhoria da sua infra-estrutura tecnológica, o INE adquiriu por um concurso publico equipamento informático compreendendo o seguinte:
- 2 x HP Proliant DL380P G8 (2x 146 GB SAS HDD, 64 GB RAM);
- 1 x HP P4300 G2 8TB MDL SAS Storage System;
- 1 x HP StorageWorks LTO5 Ultrium 3U 3280 SAS Tape Drive

Pretende-se com o novo equipamento substituir os diversos servidores físicos ja obsoletos, implementando uma solução "High availability Smart Bundles", uma solução da HP e Microsoft.

Os serviços a implementar dentre outros, incluem os seguintes:
Servers:
a. Configuração do *Hyper-V Clustering* e virtualização de servidores;
b. Migração do Domínio para Windows Server 2008 (DFL/FFL);
c. Restruturação/Melhoramento da estrutura do Active Directory;
d. Criação de *Group Policies (GPO)* para automatização de várias tarefas do domínio (*Drive Mapping,My Documents Redirect,Windows Update,Software Deployment,etc..*);
e. Assegurar a replicação entre os *Domain Controllers* (DCs) de cada site (*Active Directory Sites and Services*);
f. Migração do File Server para o ambiente virtual;
g. Migração do Exchange Server 2003 para 2010 (*Client Access, Mailbox e Hub Transport*);
h. Configuração do *Microsoft Lync Server 2010/2013;*
i. Configuração do *System Center Configuration Manager* (SCCM) 2012 :
    - *Component Server (SMS Executive Server);*
    - *Site Database Server;*
    - *Site Server;*
    - *Management Point;*
    - *End Point Protection Point (****Forefront End Point Protection 2012** (**FEP)**);*
    - *Distribution Point* (DP);
    - *Fallback Status Point;*
    - *Report Services Point;*
j. Instalação do DataBase Server (SQL Server 2008/2012);
k. Configuração dos seguintes serviços de rede:
    - DNS (*Domain Name System*): *Forward e Reverse Lookup zones*;
    - DHCP (*Dynamic Host Configuration Protocol*): Configuração de um "*scope*" que abranga todos os hosts da rede da instituição e que seja escalável para o futuro;
    - WSUS (*Windows Server Update Service*) – Assegurar que todas os hosts façam *updates* localmente e que somente o *Update Server* tenha acesso aos servidores da Microsoft;
l. Configuração do Web Server (Apache 2) - Pretende-se que sejam criados virtual hosts para o alojamento de vários websites no servidor e também pretende-se que ele faça o redirect automatico de HTTP para HTTPS em alguns websites;

Storage
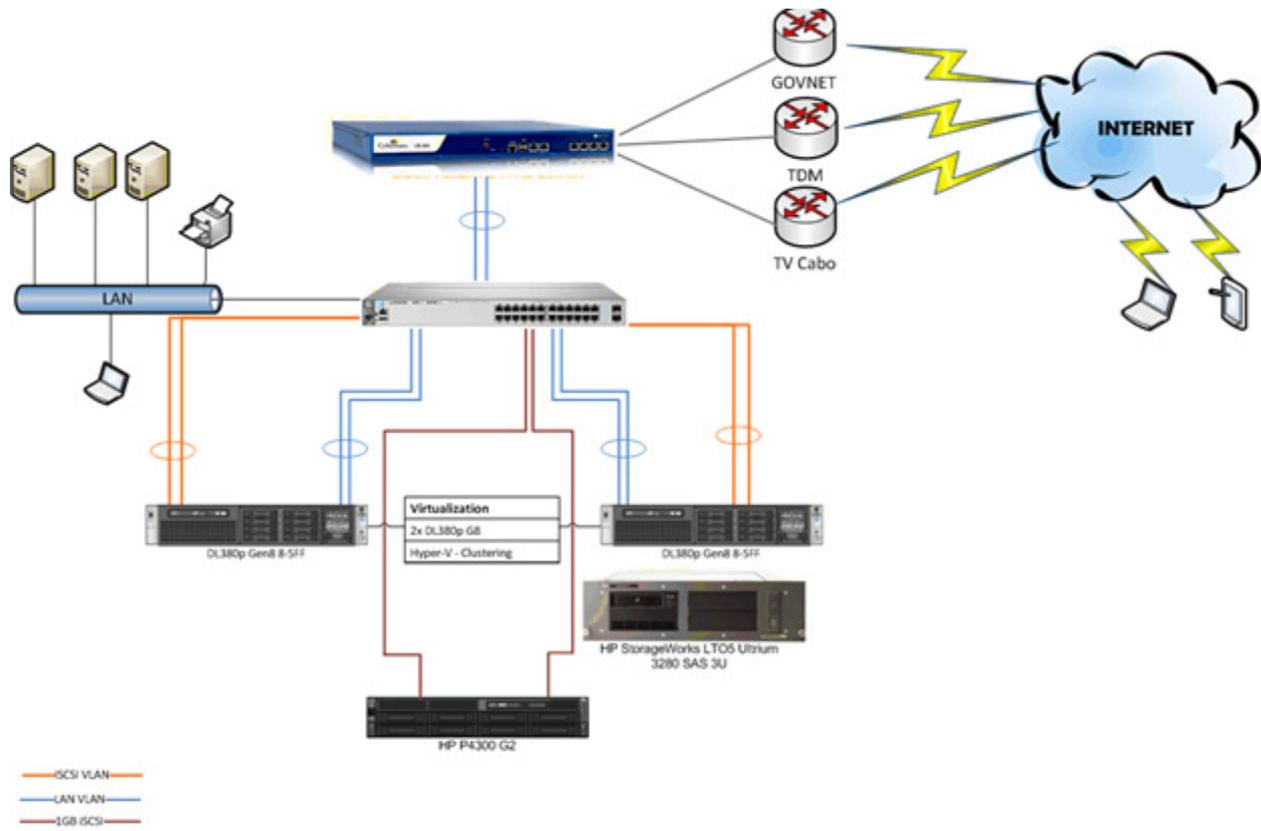   - Configuração do HP LeftHand P4000 Storage;

Tape Drive
- Configuração de backups HP StorageWorks LTO5 Ultrium 3U 3280 SAS Tape Drive;

Networking & Security:
- Segmentação da rede em VLANs (*Virtual LANs)*;
- Configuração de VTP (*VLAN Trunking Protocol*) e *Trunking;*
- Configuração do STP (*Spaning Tree Protocol*);
- Configurar Cyberoam CR 300ia UTM
  - Segmentação do tráfego entre as zonas LAN, WAN e DMZ;
  - Multi-Link c/ *Load Balancing* (Suporte Simultâneo de 3 ISPs – TDM (4MB), GovNet (2MB), TvCabo (10MB));
  - Identity (Autenticação de usuários no Cyberoam por SSO(Single Sign On));
  - Firewall (Controle de tráfego entre as várias zonas LAN,WAN,DMZ e VPN);
  - Anti-Spam;
  - Anti-Virus;
  - IPS;
  - Web Filter;
  - Application Filter (Bloqueio de *Torrents, Streaming*,etc..);
  - VPN (SSL VPN & L2TP);

De uma forma resumida, o cenário que se pretende é o seguinte:

GOVNET

TDM

TV Cabo

INTERNET

LAN

Virtualization

2x DL380p G8

Hyper-V - Clustering

DL380p Gen8 8-SFF

DL380p Gen8 8-SFF

HP StorageWorks LTO5 Ultrium
3280 SAS 3U

HP P4300 G2

iSCSI VLAN

LAN VLAN

1GB iSCSI

7 APPENDIX 4 Activities during the mission

The following activities where conduct during the mission:

Monday 26 August Kick off meeting

Reading of the technical installation documents on the installation done by DATASERV.

Reading the report written by C2D Services Inc. "Technical Assistance for the National Statistics Institute of Mozambique (SEL:2012-A-034271-1)"

Tuesday 27 August Review of network diagrams made by the vendor. The review was arranged as workshop with hands on training on the network infrastructure. There were good discussions about network infrastructure, where the employees showed great interest and understanding of the subject.

Mr Mr. Fernando Lopes and Mr. Paulo Saningo from Dataserv were present at INE, and presented the Hyper-V installation, including network and storage configuration for the consultant.

Wednesday 28 August Part of the day was spent on writing mission report because the employees attended a meeting for the entire organization.

It was investigated how the process of virtualizing physical server to virtual servers can be implemented by using the tool disk2vhd from Microsoft. The first tests of migrating a physical disk into a virtual disk was started I the afternoon. The migration process was finished during the night.

Thursday 29 August Meeting with Mr Paulo Matusse (Dissemination & Documentation Department) where the primary subject was migration of applications from the two physical servers STATBANK and ESDEM. A plan for the migration was made and after migration the two servers can be shut down if it is OK with Mr.

Review of Hyper-V and Storage documentation.

Hands on training using the disk2vhd tool.

Friday 30 August A physical server was virtualized from the output of the disk2vhd tool form the day before.

Held a meeting where the implementation done by DATASERV was discussed. A list of questions on outstanding tasks was prepared and sent to DATASERV.

Reconfiguring faulty Windows Server Update Service implementation started.

Monday 2 September Meeting with DATASERV where outstanding tasks where discussed. The following activities where planned with DATASERV for the week:

- Firmware upgrade of storage system.
- Firmware upgrade of core switch.
- DMZ VLAN implementation in core switch and Hyper-V
- Segmentation of net access switch stack.

Two databases where migrated to the new MS SQL Server 2008 server for testing the migration method.

The switch stack on 5th floor was connected directly to the new core switch, and configuration changed to reflect the segmented VLAN infrastructure. The switch stacks on 4th, 7th and 9th floor are waiting for the purchasing of the last 2 GBIC interfaces to the core switch.

Tuesday 3 September	The necessary configuration to have an IP phones and a computer on one switch port were tested with a positive result. The procedure to do changes in the IP phones and switch configuration were documented. The documentation was tested by part of the IT staff.
Wednesday 4 September	Migration of Microsoft SQL Server databases to the new DBS server.
	Implementation of database backup was done on the DBS server.
Tuesday 5 September	There was made a plan for the upgrade tasks on storage and core switch. The implementation was done on Friday 6th September.

Held a meeting where the topics among others were the following:

- Follow up on recommendations from previous missions.
- Discussion on how to implement the WAN connections to the DPINE's

After work there was good discussion on the Canadian C2D report.

Friday 6 September Further discussions on the Canadian C2D report.

Organizing workshop where monitoring of disk system was discussed.

Organizing workshop where Microsoft SQL Server backup was discussed.

After office hours the disk system was upgraded to newest version of software and the memory was expanded from 4 to 6 GB. The core switch was also upgraded with new software, and a DMZ VLAN was configured.

After office hours DMZ VLAN implemented on the Hyper-V servers.

Saturday 7 September Report writing