Final Project Report

LAN upgrade and improvement of intra/inter departmental communication at the MRD head office 1343/OC-SU

Prepared by: Manodj Gopalrai
Date: February 16, 2009

Executive Summary

This project is part of the Decentralization and Local Government Strengthening Program (DLGP), currently being implemented by the Ministry of Regional Development (MRD). Although significant investment has been made in acquiring new computers for the MRD head office, local staff have not been trained in the use of their PCs and the local area network (LAN) is not configured to facilitate intra/inter departmental communication and collaboration.

This project sought to upgrade the network at the MRD head office and to provide basic pc skills to personnel in order to utilize the facilities of this upgraded network. Benefits of this upgrade include:

- central storage of documents and permissions
- central management of users and computers
- a secure network with a firewall blocking and filtering unwanted traffic
- a backup and recovery plan for business continuity
- cost savings (obsolete internet connections, increased availability of IT services)
- a network configuration that will allow for implementation of enterprise applications and network expansion
- decreased exposure of internal documents to the internet (by allowing e-mail communications internally rather than via third party e-mail providers)

Seen the previous state of the network, this project has been successful in upgrading the network in complying with current IT security and operational standards.

Table of Contents

Introduction

The local area network (LAN) consisted of newly purchased PCs which were being used as standalone workstations although interconnected in a workgroup environment thru small switches. A workstation present was installed with Microsoft Windows 2003 server, however this server was not configured as a domain controller. All PCs were connected to the internet via one of the three TeleSur ADSL routers in the office, with each router forming a separate network. So in essence, three separate networks had been created in the office, two of them serving only one user.

Due to construction and renovation at the site, departments were being moved to different locations in the building and the IT department had not yet been assigned a server room. The server (workstation being utilized as a server) was placed at a desk of an ODAD department worker and physical access to it had not been restricted. Switches had been placed throughout the building where connectivity was required.

The local IT department consists of a senior IT technician and a junior technician. The junior technician is currently undergoing training in skills required to support the LAN. Neither technician is certified as network or system administrators.

Given these facts, several network aspects needed to be addressed by this project:

- Security: users logging in locally, many workstations not even requiring passwords for access
- Backup: documents stored on several PCs scattered on the network
- Threat Prevention: the absence of a consistent anti-malware program on the network
- Traffic Control: monitoring and restricting access to external networks (internet)
- Training: basic PC use for general users and network/system administration by IT staff

Objective

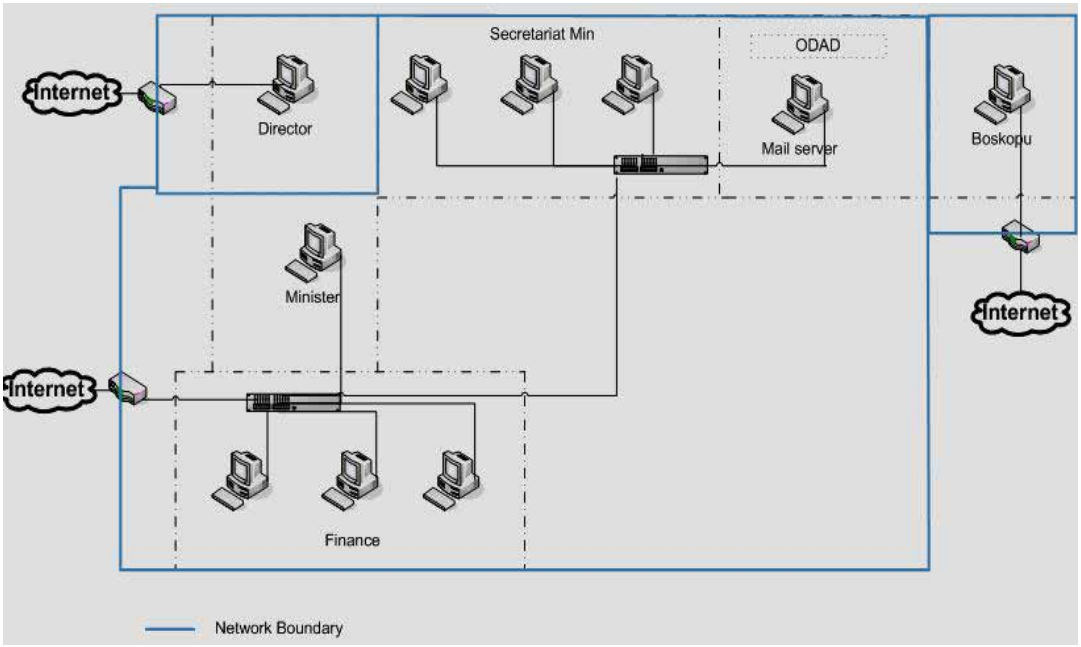
The objective of this project was to enhance intra/inter departmental communication at the MRD head office within six weeks by upgrading the local area network and training of local staff in effective use of the digital network. Training of general staff will focus on basic use of their PCs and applications. IT personnel will be trained in the policies and procedures of IT Operations.

Scope

This project focused entirely on the MRD head office, with the following work packages defined:

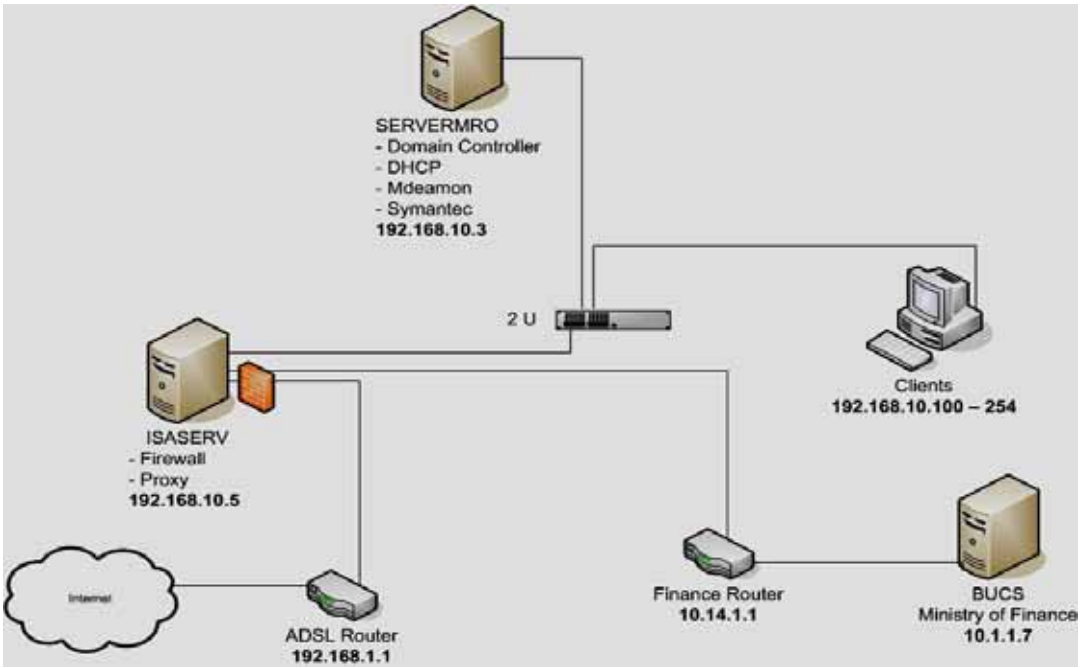
- Configuration of a file server as to facilitate document sharing as well as central management and backup of data
- Upgrade of the workstation currently used as a mail server to a domain controller for authentication of network clients
- The installation of a firewall to monitor and restrict traffic to external networks
- The installation of an enterprise antivirus program to prevent threats from viruses and other malware
- Training of personnel in basic use of their PCs and specific training to IT staff
- Developing and implementing policies and procedures for the IT department

Previous Network Configuration (figA)



figA

Current Network Configuration (figB)



figB

Project Results

Server

Given the time constraints of this project a workstation with IDE drives has been upgraded to function as the domain controller (DC), however it is recommended that a server with RAID configuration (for disk fault tolerance) is used as a DC for the MRD network.
Microsoft Windows 2003 R2 Server is installed on the DC with active directory services and all users and computers on the network have been made part of the MRO domain. Each department is configured as a separate organizational unit (OU) in the MRO domain for deployment of department specific group policies and easy management. User groups have been created on department level and access given to department specific folders on the DC. These departmental folders are mapped on workstations thru login scripts to allow central storage of all documents.
The DC has also been configured as a local mail server with e-mail accounts created for all staff, allowing internal e-mail communication.
Backups are made daily on an external tape drive and tapes stored currently at the IT department, however an off-site storage location is recommended.

The following are the minimum requirements for the deployment of a reliable DC at the MRD:

Component	Requirement
Computer and processor	2GHz or faster processor
Memory	At least 2 GB of RAM
Hard disk	At least 100 GB
Drive	CD/DVD-ROM drive
RAID Configuration	At least RAID-5
Display	VGA or better
Backup Drive	Tape Drive with at least 100GB uncompressed capacity
Network Card	Gigabit Adapter

Server Room

Preferably servers must be placed in a dedicated server room which is air-conditioned and to which access is restricted to IT personnel only. The IT department has been assigned a server room currently and the domain controller has been moved to this location. Access to this room is still an issue with many employees who do not have access to internet using the computers at this location to check emails. It is recommended that access to this area is logged and access to this area is limited.
It is also preferred that all network cabling of the office converge in the server room on a numbered patch panel, so that each client in the office can be identified with its associated port on switches.

Firewall

The previous setup of the network did not allow for filtering of malicious traffic coming in and out of the LAN. The installation of a firewall has mitigated uncontrolled internet usage and now restricts traffic going thru the routers, minimizing the risk of security being compromised and saves bandwidth and costs for internet connectivity (current requirement for ADSL connections has been reduced to one).

ISA Server 2006 currently functions as the network firewall and routes traffic from internal clients to both the internet as well as to the network of the Ministry of Finance (MF). Previously clients using applications on the MF network needed to be configured with static IP addresses on the same subnet as the router connecting the MF network; however this is not the case now. The installation of the ISA server has made it possible to allow clients of the Finance department to be joined to the local MRO domain while maintaining access to applications on the MF network. The ISA server is physically located in the server room.

Antivirus

Previously infection by malware was quite common on the workstations at the MRD network. This was due to the lack of a consistent antivirus program on workstations as well as the absence of an enterprise application which allowed central threat prevention. Symantec Corporate edition has been installed on the DC and currently all clients on the network have been rolled out with antivirus software. Virus definition updates are controlled centrally on the DC, with updates and distribution of definition files occurring daily to clients. Scanning is scheduled daily on clients and the server. Any infection of a system is reported to the IT department thru the Alert Management System (AMS) by means of e-mail. This system will significantly reduce exposure of the internal network to malware.

Clients

All clients have the Microsoft Windows XP operating system installed are joined to the local domain MRO. This will facilitate group policy rollouts and central administration of all clients on the network.

It is recommended that PCs are labeled with their respective computer names for identification purposes and to facilitate remote helpdesk features.

Training

General Staff

Training has been conducted over a three day period and training topics included basic PC use, common Microsoft Office applications and the use of email. See ***Training Assessment Report*** for detailed report.

IT Staff

It staff has been trained in server maintenance, backup operations and user administration. They have been actively involved in the project and are aware of the changes on the network. Due to increased complexity of network and system administration of the upgraded network, it is recommended that at least one technician is certified in managing Microsoft Windows networks.

Policies and Procedures

Policies and procedures regarding IT Operations have been drafted in order to ensure that data and network integrity as well as security are guaranteed.

Policies and procedures have been formalized for the following operations:

- Creating Users or Groups in Active Directory
- Granting Users or Groups privileges on departmental folders
- Backup and restore tasks
- Disaster recovery tasks

Currently auditing has been enabled on the departmental folders on the DC, so that authorized access and unauthorized attempts for access can be logged. Full Access has only been granted to the Enterprise Admin group accounts so that backups can run under these accounts. The IT department is not a member of the Enterprise Admin group. It is recommended that new users are created and granted access to departmental folders only after a written request is submitted by the head of the department to IT.

For detailed backup and disaster recovery procedures, see ***Backup and Recovery Plan Ministry of Regional Development.***

Conclusions

This project has been successful in achieving its objectives of upgrading the local area network as well as facilitating inter/intra-departmental communication and collaboration. It is expected that users will utilize their e-mail to communicate within the ministry, which will lead to improved communications, delegation, scheduling and general organizing.
Central storage of documents on the server will lead to improved file sharing as well as business continuity in the event of a disaster (backups).
The current network setup is definitely more secure and reliable than its previous state where there was a lack of threat suppression, access control and traffic control.

Recommendations

This project marks the first steps towards modernization of the network at the Ministry of Regional Development. As the network grows in size, requirements for the network will change. It is expected than the server will need to be able to handle more load than currently is the case, as network use will intensify. It is therefore recommended that:

- A server is procured as with a larger capacity in memory and storage as described by this document
- Network cabling is rewired with all cabling converging in the server room
- Use of small switches is discontinued on the network
- A UPS is installed in the server room which provides a minimum of one hour of battery runtime

Other recommendations include the following:

- A log is kept of problems on the network and user requests
- A log is kept of persons entering the server room
- Backup tapes are stored at an off-site location
- All authorizations are granted only after written requests from the specific department heads to IT (this can be in the form of email)

It is further recommended that at least one IT technician is trained in administration of a Microsoft Windows network.

Training Assessment Report

Basic Computer Skills Training

Ministry of Regional Development

Prepared by: Manodj Gopalrai
Date: 31 October 2008

Table of Contents

Introduction

As part of the LAN upgrade project a basic computer skills training was conducted for staff at the Ministry of Regional Development (See "LAN upgrade and improvement of intra/inter departmental communication at the MRD head office 1343/OC-SU"). The LAN upgrade project resulted in significant changes to the computer network which required users being trained in the new system.

Objective

The objectives of the basic computer skills training were:

- to make users aware of the changes on the computer network
- to provide users with the basic computer skills required to be able to utilize the computer network and communicate effectively

Training Topics

- General Computer Use
  - Logging into the domain
  - Storing documents
  - Document naming convention
  - Microsoft Windows shortcuts
- Microsoft Word
  - Formatting text
  - Templates
  - Indexes
  - Mail Merge
- Microsoft Excel
  - Using Formulas
  - Charts
  - Lists
  - Pivot Table
- Microsoft Outlook
  - Email
  - Using Calendars
  - Scheduling Meetings

Training Method and Materials

Training was conducted in the conference room at the Ministry by way of using a projector. It involved step by step demonstration of tasks in using Microsoft Office features. The total time for each training session was two hours. To encourage participants to use the computer network, all training material will be made available on a shared drive on the server.

Assessment Methods

At the start and end of the training participants were asked to fill out a questionnaire assessing their computer knowledge and skills in general use of computers and in Microsoft applications.

Limitations

Questionnaire results are based on subjective responses by individuals with varying degrees of computer proficiency. Further assessment is needed to determine actual employee skill levels.

Results

General Computer Skills

Of the total participants 34% identified themselves as having advanced general computer skills while 45% responded that their current computer skills are not sufficient according to their job requirements. After the training 83% responded that their general computer knowledge had increased, however only 34% were confident that their skills were sufficient.

MS Word

Of the total participants 40% identified themselves as having advanced MS Word skills while 39% responded that their current MS Word skills are not sufficient according to their job requirements. After the training 86% responded that their knowledge of MS Word had increased, however only 55% were confident that their skills were sufficient.

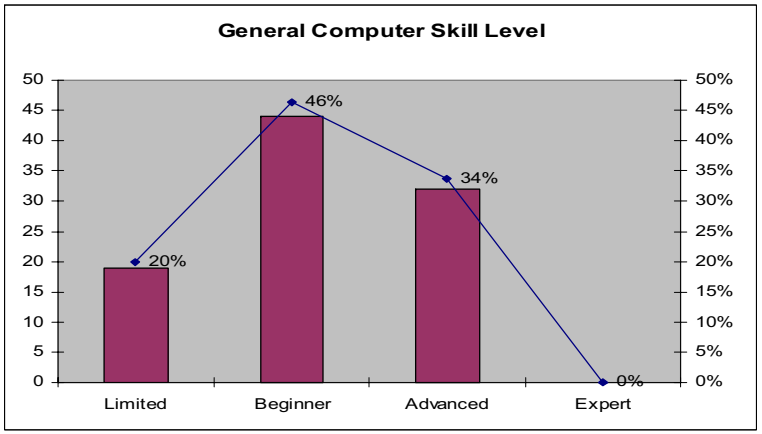
MS Excel

Of the total participants 19% identified themselves as having advanced MS Excel skills while 57% responded that their current MS Excel skills are not sufficient according to their job requirements. After the training 76% responded that their knowledge of MS Excel had increased, however only 32% were confident that their skills were sufficient.

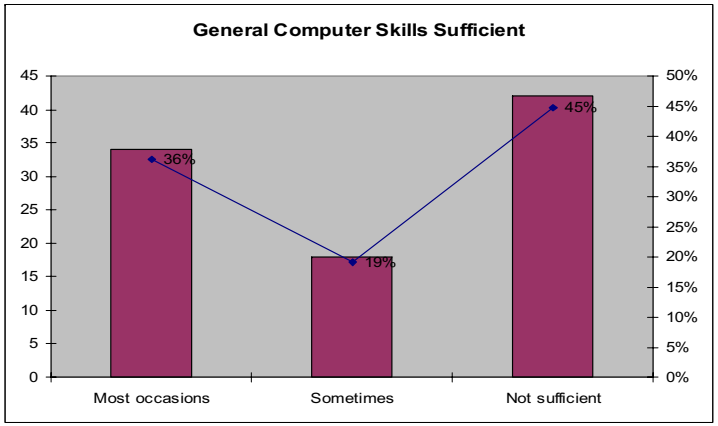
Survey Data

Before Training

How do you rate your general computer skills?

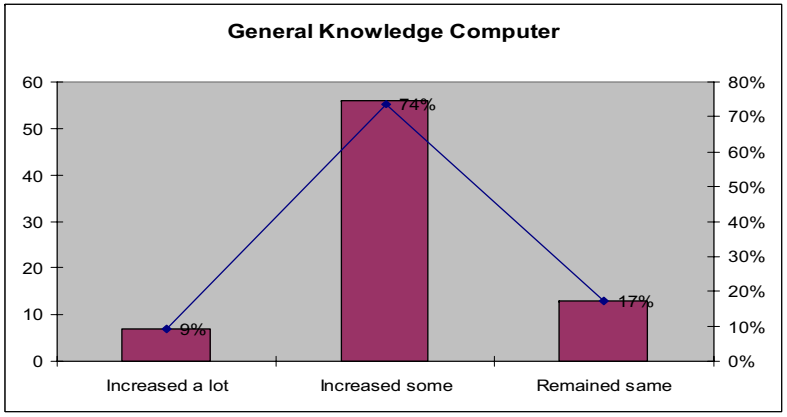


Is your current skill level sufficient?

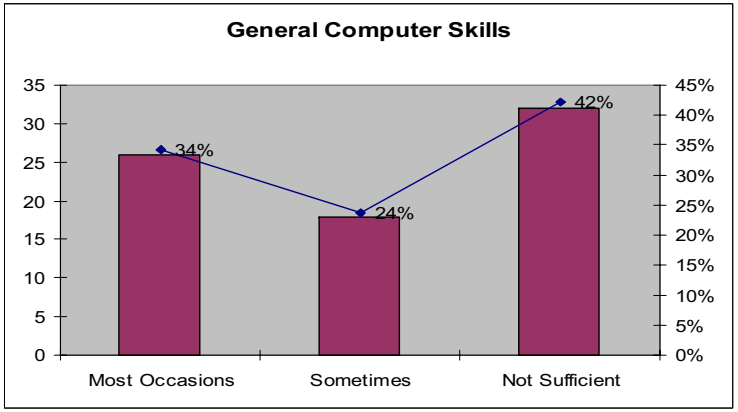


After Training

How did the training affect your general computer knowledge?

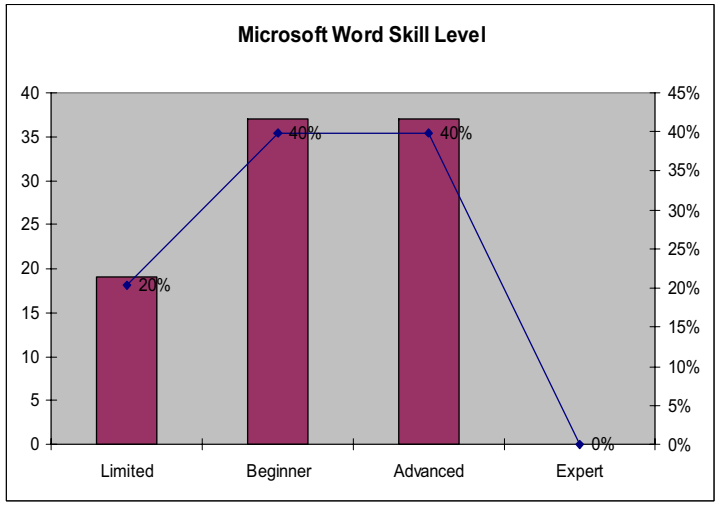


Is your skill level now sufficient?

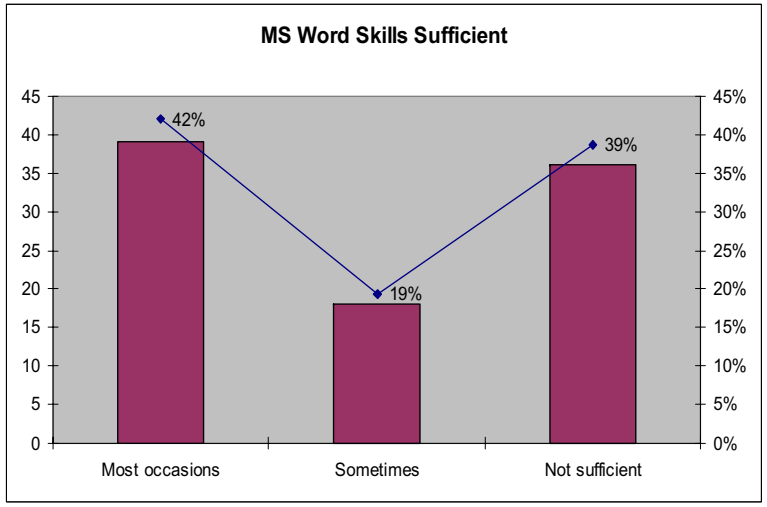


Before Training

How do you rate your MS Word skills?

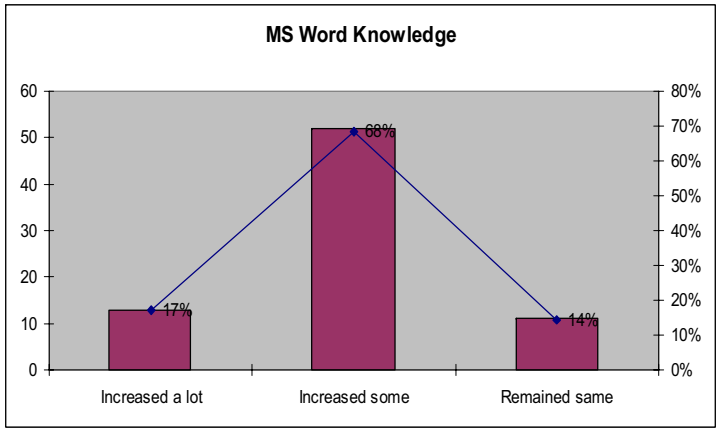


Is your current skill level sufficient?

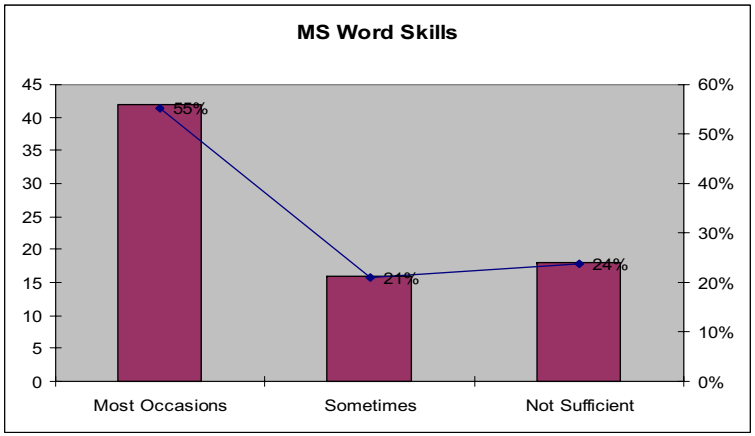


After Training

How did the training affect your knowledge of MS Word?

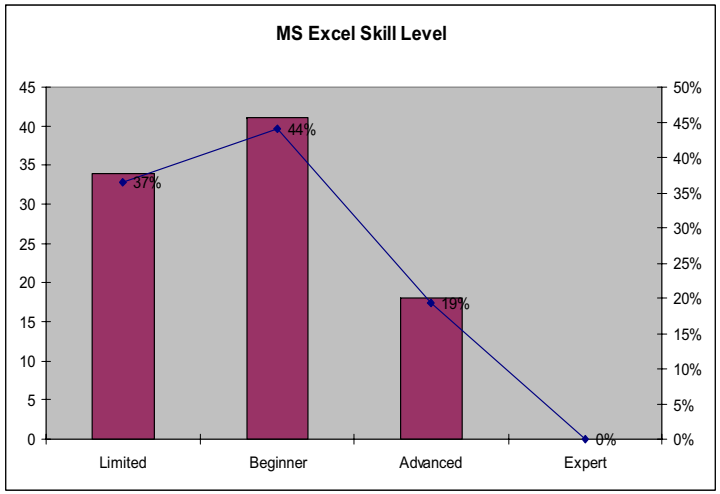


Is your skill level now sufficient?

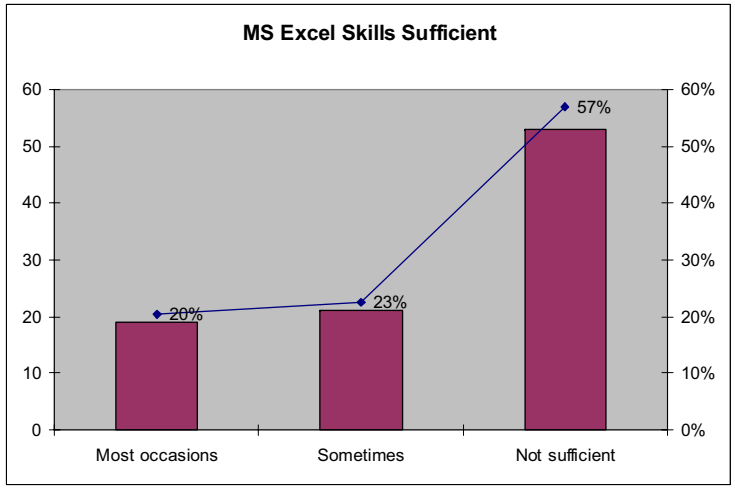


Before Training

How do you rate your MS Excel skills?

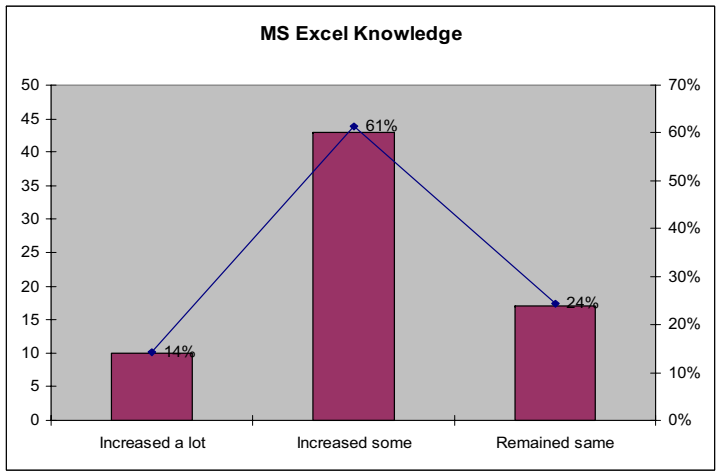


Is your current skill level sufficient?

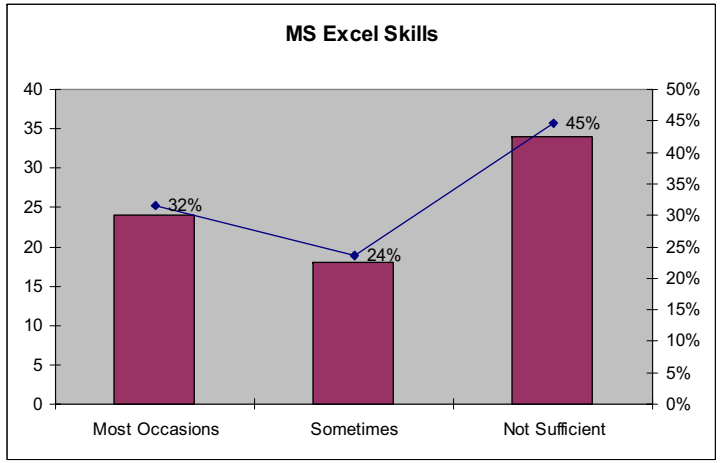


After Training

How did the training affect your knowledge of MS Excel?



Is your skill level now sufficient?



Recommendations

From the survey we can conclude that after the training more than half of the participants had an increased knowledge of general computer use and other topics covered in the training. The survey results also show that more training is required after this initial two hour training session. Particularly additional training is required in general computer use and MS Excel, where more than 40% of participants assessed themselves as lacking sufficient skills.
For future training it is recommended that:

- The LAN is fully functional before any other training sessions are conducted
- Participants are separated into groups according to skill level (advanced skill users need to be excluded from training)
- Specific training is provided to departments according to their daily tasks (eg targeted MS Excel training for the Finance Dept, MS Word for the Secretariat)
- Participants have access to a computer while the training is conducted

Backup and Recovery Plan
Ministry of Regional Development

Prepared by: Manodj Gopalrai
Date: February 17, 2009

Table of Contents

1. Backup Overview

This section describes the backup process, the backup schedule and recovery tasks (in the event of a system failure) at the Ministry of Regional Development (MRD).

As part of the LAN improvement project (1343/OC-SU) clients have been configured to authenticate with a Windows 2003 domain controller and it is therefore critical that proper backups are made of the server and recovery tasks are documented.

Key Business Functions

Key business functions are applications/services that are considered critical for continuing operations at the MRD.
The following are considered key business functions at the Ministry:

System	Function
SERVERMRO	Active Directory: Domain Controller: Authenticates clients on domain DNS: Provides Name Resolution to clients DHCP Server: enables dynamic IP configuration
SERVERMRO	Applications: MDaemon: Provides POP and SMTP service Symantec: Antivirus software

Backup Media

An LTO tape drive has been installed on the server which will run daily backups at 24:00hrs from Monday thru Friday.
Tapes are labeled according to the day of the week the backup was run and the exact backup date. Backup tasks run under the MRO\Administrator account and **ntbackup** is being used as the backup application.

The IT Department must ensure that backup logs are checked in the morning to verify that backups have run successfully. In case of backup failures, backup jobs must be re-run at the earliest possible time.

Retrieval and storage of backup media must be logged on a backup form which records the name of the person retrieving or storing the backup tapes, the date/time and the media label.

BACKUP OBJECTS	MEDIA LABEL	LOCATION
-Dept -System State -System Volume Information	Ma *DDMMYY* Di *DDMMYY* Wo *DDMMYY* Do *DDMMYY* Vr *DDMMYY*	

Recovery Strategy

The following are the steps to be followed (if applicable) in case a rebuild is required of a failed system:

1) Install or restore LAN/WAN connection at recovery location
2) Acquire hardware for system
3) Retrieve backups and media required to rebuild system
4) Rebuild system
5) Test system

LAN connectivity should always be first priority when a system rebuild is required.

2. Recovery Tasks

This section will provide detailed steps on recovery of business critical applications/services as defined in this document.

Domain Controller (SERVERMRO)

Automated System Recovery (ASR) should be used to restore the domain controller server and will only work subject to the following conditions:

- The target system hardware (except for hard disks, video cards, and network adapters) is identical to that of the original system.
- There are enough disks to restore all the critical system disks.
- The number and storage capacity of the critical disks are at least as great as those of the corresponding original disks.

Recovery steps:

1. Insert Windows 2003 Server R2 CD in the server
2. Boot from CD when prompted
3. Press F2 for ASR
4. Insert the ASR floppy disk (asr.sif file). This will format the system hard drive and prepare for restoration of Windows 2003.
5. The system will reboot and prompt for backup media.
6. Confirm location of backup media.
7. The ASR process will restore all files on critical disks.

Note: ASR is used to restore critical disks only (disks with OS installed on them). User data needs to be restored from tape backup as described in this document.

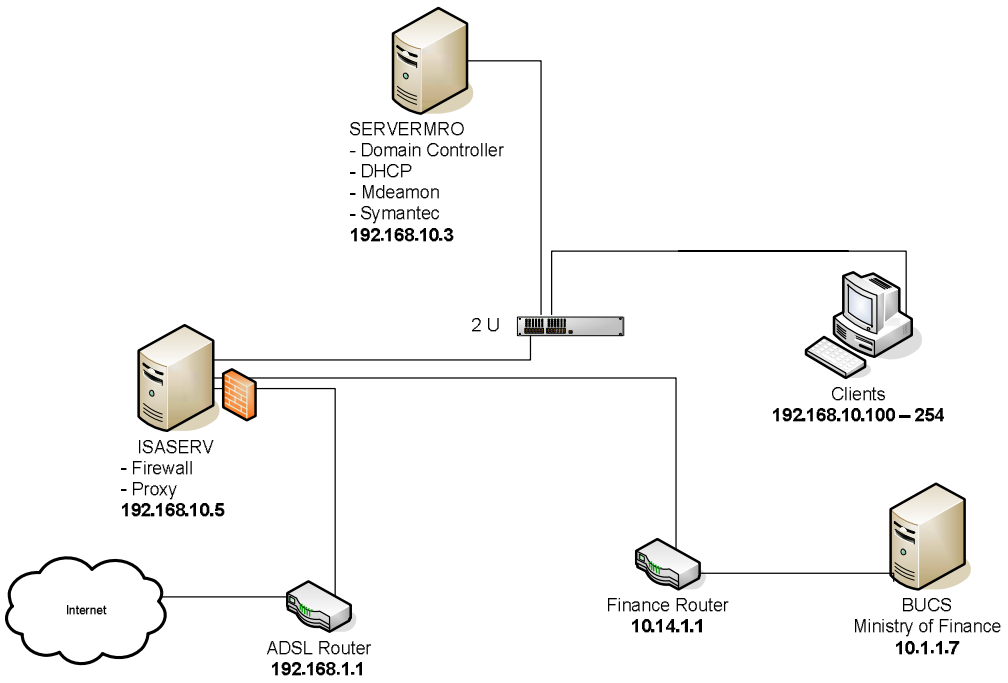
3.0 Network Configuration and Diagrams

This section provides information about the current network configuration and setup of LAN and WAN.

Subnets

Scope	Clients	Start IP Address	End IP Address
192.168.10.0	Workstations	192.168.10.100	192.168.10.254
192.168.10.0	Servers	192.168.10.1	192.168.10.20

Network Diagram



4. External Contact List

Service/ Systems	Company Name	Contact Name	Tel
Server Hardware			
Printers			
WAN (ADSL)	Telesur		400466
Switches			
Workstations			

5. Software List

Application Name
Microsoft Office 2003 Professional
Microsoft Windows 2003 R2 Server
Mdeamon
Symantec
Microsoft Windows XP Professional
ISA 2006

6. Equipment Listing

Count	Description
1	Server , 1GB RAM, 160 GB HDD, CDROM, SCSI drive
1	200 GB/400 GB LTO Tape drive
30	Workstations, 1 GB RAM, 60 GB HDD, CDROM

Implementation of

Microsoft Office Sharepoint Server at the MRD

Prepared by: Manodj Gopalrai
Version: 2.0
Date: October 30, 2008

Table of Contents

Introduction

The Ministry of Regional Development (MRD) has identified a need for the implementation of a Document Management System (DMS) at their head office. The purpose of this system is to facilitate document life cycle management as well as the setup of a repository for enterprise documents. The proposed system for this project is Microsoft Office Sharepoint Sever 2007 (MOSS) and this document describes the initial project plan to implement MOSS at the Ministry.

Recommendation for MOSS is not based on requirements analysis but rather on the ease of integration with Microsoft Office currently in use at the Ministry and the minimal training required for users. Process mapping of document workflows will determine system requirements but due to time constraints and the current upgrade of the LAN (See “LAN upgrade and improvement of intra/inter departmental communication at the MRD head office 1343/OC-SU “) workflows have not been documented. Selection of MOSS should be reevaluated after document workflows have been mapped and based on these requirements MOSS should be compared to other document management systems available on the market.

MOSS Features

MOSS features the following document management capabilities:

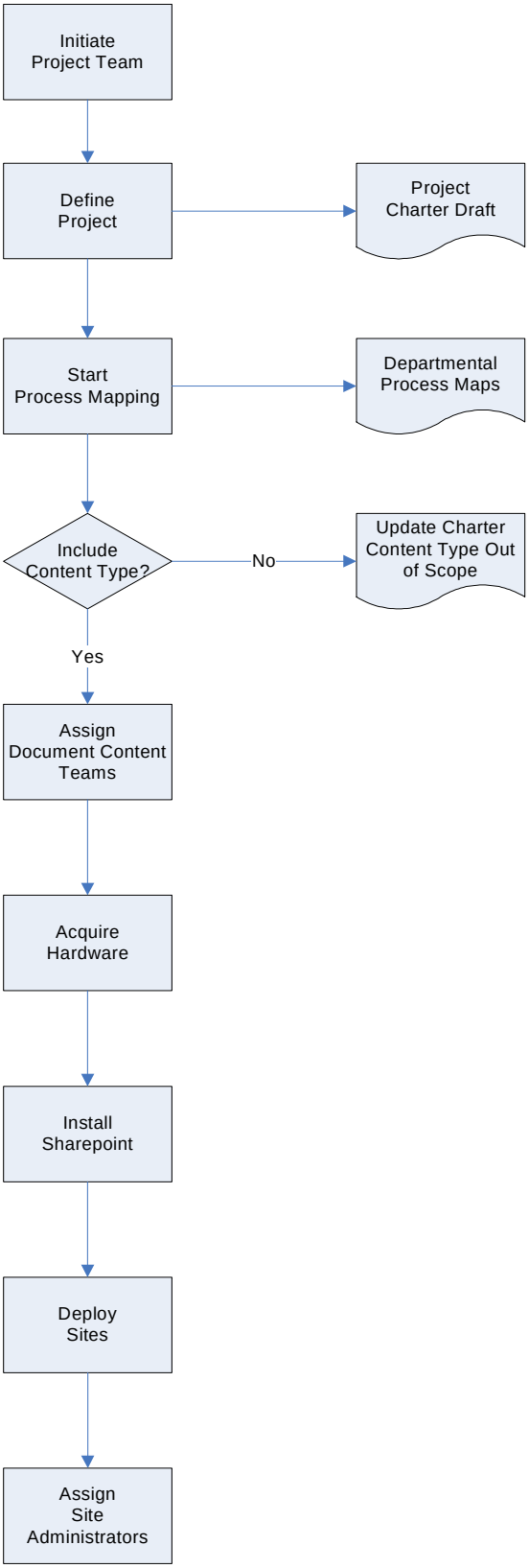
- document collaboration
- document versioning
- document control
- workflow: review and approval
- document publishing
- document indexing and search

Project Planning

Planning for the implementation of MOSS will include the following tasks:

1. Initiating a project team
2. Defining the project
3. Process mapping of processes at the respective departments
4. Narrowing the Scope
5. Assembling document management teams
6. Acquiring hardware for the server
7. Installation and configuration of MOSS
8. Deployment of sites
9. Assigning site administrators
10. Training of staff in use of MOSS

Project Overview



Initiating the Project Team

It is important that high level document management roles are identified in the organization. They will be the key stakeholders in this project and should be part of the initial project team. High level document management roles include document approvers and reviewers. These are usually department heads that request document creation and approve content distribution. In addition to these roles, library content managers should be involved in the setup of the document repository.

Defining the Project

Management of documents in an organization encompasses vast amounts of potential data that needs to be classified and stored in a content library. It is therefore important to restrict the scope of this project to documents that require a workflow, need version control and are made available for enterprise search.
All documents at the MRD should be cataloged and classified according to their content type. Examples of content types are: contracts, policy documents, forms, etc. Based on the analysis above, specific content types should be selected for MOSS deployment. Documents with content types that do not need collaboration and do not need to be disseminated in the organization should be excluded from the scope of this project.

Process Mapping

It is critical that the following stages of the document life cycle are mapped within each department:

1. Creation
2. Review
3. Approval
4. Dissemination
5. Retention
6. Disposal

Process mapping each stage of the document life cycle will provide the basis for creating workflows in MOSS. It will identify users that are involved in the document life cycle as well as information management policies that need to be applied to documents. Information management policies handle document retention or disposal.

Narrowing the Scope

Process mapping will allow the project team to select which document types are selected for the final scope of this project. Factors in deciding inclusion or exclusion from this project should be:

1. The total amount of data that will be generated by the document life cycle and the capacity of the server that will be procured for this project
2. The need to reduce document life cycle time
3. The need to make these documents available for enterprise search
4. The need for version control, access auditing, task scheduling, or any other document management features

Assembling Document Management Teams

Document Management Teams (DMTs) consist of members that perform document management roles on one or several document types. Document types that have the same DMT should be grouped together on the same site to reduce administration as well as the number of sites deployed. In other words if the DMT for different document types are the same, then a single site should be created for both document types.

DMTs will be working with the MOSS implementer on site design and workflow settings. DMTs are automatically assigned document management tasks each time a new document is uploaded to the site.

Acquiring Hardware

The hardware requirements for the installation of MOSS depend on the deployment architecture. Configurations where the Application server and Database server are hosted on separate machines will require multiple server hardware.

The following are requirements for a standalone server:

Component	Recommended
Processor	Dual processors that are each 3 GHz or faster
RAM	At least 2 GB
Disk	NTFS file system with at least 3 GB
Drive	DVD drive or the source copied to a local or network-accessible drive
Display	1024—768 or higher resolution monitor
Network	56 Kbps or faster connection between client computers and server

Installation and Configuration

MOSS requires Microsoft Windows 2003 or higher for installation. Internet Information Services and the Microsoft .Net framework should be installed and configured prior to MOSS installation.
Installation of MOSS involves the following steps:

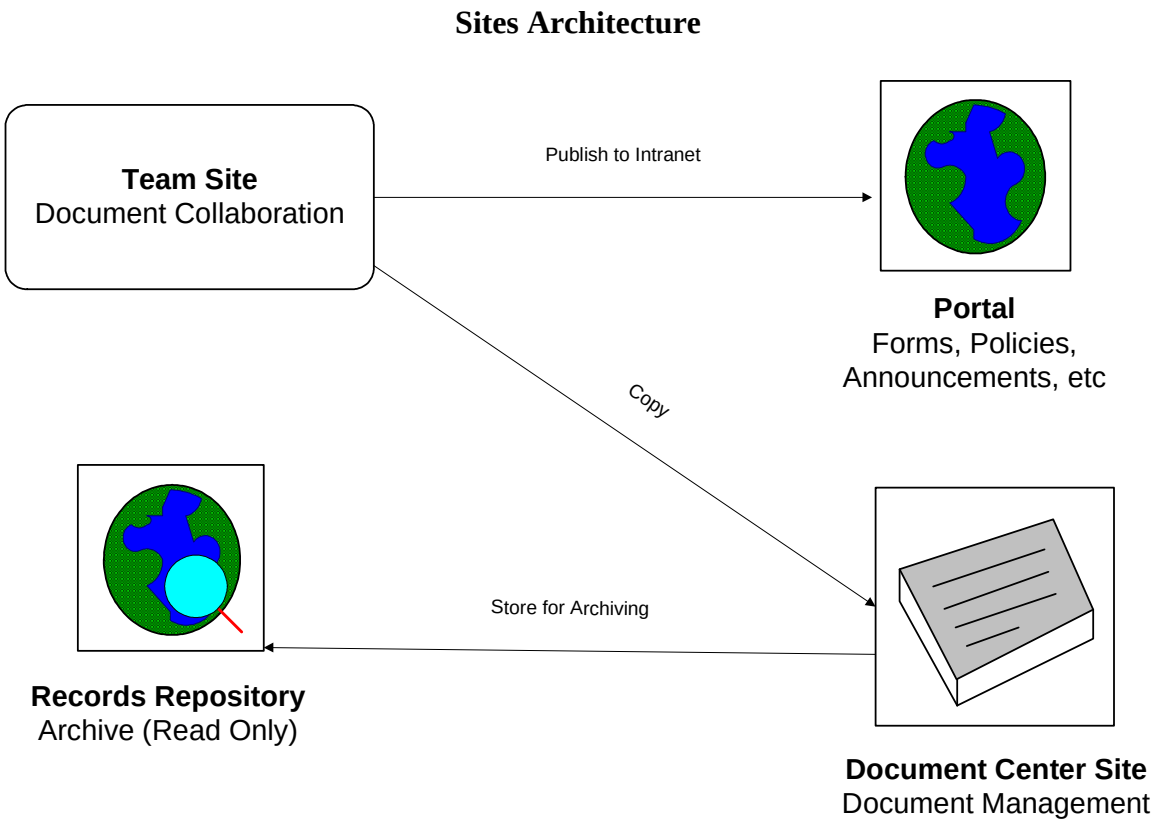
- installation of MOSS
- configuration of a Shared Services Provider (SSP)
- configuration of a web application which will host sites
- configuration of SMTP for incoming and outgoing messages (user alerts)
- configuration of workflow settings (web application level)
- configuration of search
- configuration of antivirus settings

SSP provides central management of services available to web applications, which includes search settings, usage reporting, etc. MOSS crawls all sites on Web applications using the SSP to create a single index of all content, data, and metadata. Crawls can also be configured for shared folders on the network.
Workflow settings allow scheduling and assignment of document management tasks to users.

Deployment of Sites

It is recommended that the following sites are deployed at the MRD:

1. A Team Site for each document content type, which will allow document authoring, review and approval.
2. A Document Center Site, to be used as a repository for documents
3. A Records Center Site which will be used for document archiving
4. A Publishing Portal which will host information intended for the entire MRD staff



Assigning Site Administrators

It is important to assign site administrators who will be responsible for site maintenance. Site maintenance tasks will include: granting user access, scheduling workflows on documents, publishing of documents, notifications to users, etc. As some sites will contain confidential documentation, it maybe necessary to enable auditing on these sites so that document access history is retained.

Training of Staff

The learning curve to use MOSS is very low due to its integration with Microsoft Office. Most tasks can be performed via a web browser so additional software installations on clients are not needed. Documents can be edited directly via web browser or on the client's computer via the check out feature available in Microsoft Office.

Operation:	**1343/OC-SU**
Project:	**SU0019-Decentralization and Local Government Strengthening Program**
Executor:	**Ministry of Regional Development**

TERMS OF REFERENCE
Experts for
Ministry of Regional Development
On as need basis in the field of ICT

Budget line: 3.1.13, 3.3.14, 3.1.15, 3.1.16
(Dossier 35)

I. BACKGROUND

The Government of Suriname (GOS) has requested support from the Inter-American Development Bank (IDB) to strengthen the institutional and financial capacity of local governments in the country, and reinforce the national legislative and regulatory framework within which local governments can operate. In view of the low level of financial authority and institutional capacity that currently exists at the local government, coupled with the GOS's limited experience in support of local governments, a first stage pilot program in Decentralization and Local Government Strengthening (DLGP) has been formulated for IDB financing. Limited to a group of five pilot Districts, the DLGP will focus on a set of core activities - fiscal policy reforms and the creation of local planning and financial management systems - that will enable the Districts to assume active roles in the delivery of public services.
This requires fundamental changes with respect to the organizational and operational structure of both central and local government in the long run more specific with respect to the political administrative culture and its level. This type of changes is very sensitive due to possible conflicts of interests and political primacy. For this reason an integrated approach with an interactive and iterative process is necessary.
Seen the major restrictions of the roles of government between the national and district levels, it is important to train the national level personnel in their new role. Some efforts resulted in restructuring the institutions of the Ministry of Regional Development (MRD). Technical assistance has been needed to support MRD during the implementation of the adjusted administration and the structure. Among others: to rehabilitate office space, to purchase office furniture and the establishment of telecommunication, media facilities and vehicle. The PIU will provide the required facilities to the relevant parts of the administration related to the Decentralization Program. Assumptions and expected constraints:

- The natural resistance to change within the national government will challenge this effort.
- Ongoing guidance of the personnel to stimulate a positive attitude for the project.
- The integrated functioning of the administrative systems based on two level governments instead of one central government administration will need to be addressed.
- The need to utilize qualified personnel at the right place and time is important to this effort.

II. OBJECTIVE

The general objective of this consultancy is to assist MRD on as need basis to make policy in providing skills needed for the new roles and in creation and implementation of a road map to transfer roles, responsibilities, personnel, to the local governments in the field of ICT.

III. CHARACTERISTICS OF THE CONSULTANT

- Type of consultancy: Individual.
- Duration: Maximum of 20 expert days.
- Place of work: Paramaribo and when necessary the other districts of Suriname.

Qualifications:

- At least 3 years of training experience and intensive project related experience;
- Holds a degree in ICT, preferable a Masters level;
- Fluency in written and oral Dutch and English;
- Has teaching and training skills;
- Has excellent computer skills.

IV. SCOPE OF ACTIVITIES

In collaboration with the PIU, the Ministry of Regional Development and other consultants and other possible key stakeholders, the consultant will advise the Permanent Secretary of the Ministry of Regional Development on as need basis in the field of ICT.

V. DELIVERABLES

The consultant will deliver:

- Reports and Notes on advice given related to the issues, tasks, and activities within the scope of this consultancy.

VI. SUPERVISION

The consultant will report to the Managing Director of DLGP and the Permanent Secretary of the Ministry of Regional Development. Supervising and monitoring will be through the Permanent Secretary of the Ministry of Regional Development.

VII. TIME & PAYMENT SCHEDULE

The total amount of the consultancy is 20 days. Declarations should be send to the PIU Managing Director. Payments will usually be made within 21 days after declaration. Declarations can be made in Surinamese Currency or United States Dollar. All payments will be in Surinamese Dollars at the buying exchange rate of the Central Bank of Suriname.