

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

**Jordan e-Government Project
Joining the SGN and Email Initiative
Project Initiation Document**

Final Report

**Deliverable for ICTI Component, Workplan Activity No. 433.2
Consultancy Agreement No. 278-C-00-02-00210-00**

July 2003

This report was prepared by EDS in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan.

List of Contents

LIST OF CONTENTS.....	1
0.1 DOCUMENT HISTORY.....	4
0.2 CHANGES FROM LAST ISSUE.....	4
0.3 ACKNOWLEDGEMENTS.....	4
0.4 DISTRIBUTION LIST.....	4
0.5 REFERENCED DOCUMENTS.....	4
0.6 ABBREVIATIONS.....	4
0.7 GLOSSARY.....	4
1. INTRODUCTION.....	6
2. PROJECT BRIEF.....	7
2.1 BUSINESS PRODUCT DEFINITION AND SCOPE.....	7
2.2 SCOPE OF THE PROJECT.....	7
2.3 OBJECTIVES.....	7
2.4 PROJECT-SPECIFIC QUALITY PROCEDURES.....	8
3. ANALYSIS.....	9
3.1 PROJECT START.....	9
3.2 INFORMATION GATHERING.....	9
3.3 DEFINING THE PROJECT SCOPE.....	9
3.4 RFP.....	9
3.5 IMPLEMENTATION.....	10
3.5.1 <i>Start-up and Engagement</i>	10
3.5.2 <i>Project Plan</i>	10
3.5.3 <i>Inventory</i>	10
3.5.4 <i>Documentation</i>	10
3.5.5 <i>Ordering and Receipt of hardware and services</i>	11
3.5.6 <i>User Training</i>	11
3.5.7 <i>Administrative Training</i>	11
3.5.8 <i>Staging of Network equipment</i>	11
3.5.9 <i>Client Rollout</i>	11
3.5.10 <i>Child domain installation</i>	12
3.5.11 <i>SGN Infrastructure Implementation</i>	12
3.5.12 <i>Internet Traffic</i>	13
3.6 PROJECT ROLL-OUT AND APPROACH.....	13
3.6.1 <i>Management of the project</i>	13
3.6.2 <i>Meetings</i>	13
3.6.3 <i>JTC Links</i>	13
3.6.4 <i>SGN Installations</i>	14
3.6.5 <i>Desktop & User Inventory</i>	14
3.6.6 <i>Approach to ensure institution's Desktops meet requirements</i>	14
3.6.7 <i>Desktop AntiVirus Software</i>	14
3.6.8 <i>Users accounts Creation</i>	14
3.6.9 <i>Password migration</i>	14
3.6.10 <i>Data migration (where email migration is required)</i>	14
3.6.11 <i>Rollout of eMail for Institution with existing eMail service</i>	15
3.6.12 <i>Internet access and ISP</i>	15
3.6.13 <i>IP Network</i>	15
3.6.14 <i>Network monitoring</i>	15
3.6.15 <i>Support and Maintenance</i>	15
3.6.16 <i>User Training for Outlook</i>	15
3.6.17 <i>eMail migration order within government institution</i>	16
3.6.18 <i>Microsoft Licensing</i>	16
3.7 ASSUMPTIONS.....	16
4. DETAILED DESIGN.....	17
4.1 SGN.....	17

4.1.1	<i>e-Gov Operation Centre configuration</i>	17
4.1.2	<i>SGN</i>	18
4.1.3	<i>Connecting to the SGN</i>	18
4.2	IP ADDRESSES	19
4.3	CLIENT PC'S	20
4.4	ENTERPRISE DIRECTORY	20
4.4.1	<i>Child Domains</i>	20
4.4.2	<i>Domain Dependencies</i>	21
4.5	USERS	21
4.6	EMAIL SERVICE	21
4.6.1	<i>Functional Requirements</i>	22
4.6.2	<i>Exchange Server Technical Design</i>	24
4.6.3	<i>Technical design implemented</i>	29
4.7	TRAINING.....	29
4.7.1	<i>User Training</i>	29
4.7.2	<i>Administrative Training</i>	30
5.	DEFINITION OF ORGANISATION & RESPONSIBILITIES	31
5.1	COMMUNICATIONS AND ESCALATION	31
5.1.1	<i>Technical Weekly Meeting</i>	31
5.1.2	<i>Steering Group Bi-Weekly meeting</i>	32
5.1.3	<i>Monthly Operations Meeting</i>	32
5.2	STEERING COMMITTEE INDIVIDUAL RESPONSIBILITIES	33
5.2.1	<i>MoICT PMO Head</i>	33
5.2.2	<i>MoICT PMO Junior Project Manager</i>	33
5.2.3	<i>MoICT PMO Project Manager</i>	33
5.2.4	<i>Ops Centre Manager</i>	34
5.2.5	<i>Government Institution Manager</i>	34
5.2.6	<i>Implementation Manager</i>	35
5.2.7	<i>Training manager</i>	35
5.2.8	<i>Quality Manager</i>	35
6.	PROJECT PLAN.....	35
6.1	PROJECT PLAN DESCRIPTION	35
6.2	PROJECT QUALITY STRATEGY	36
6.3	PROJECT ESCALATION	36
6.4	PROJECT PREREQUISITES	36
6.5	PROJECT EXTERNAL DEPENDENCIES	36
6.6	PROJECT PLANNING ASSUMPTIONS	37
6.7	GANTT CHART.....	37
7.	MILESTONES AND DELIVERABLES.....	38
7.1	MILESTONES	38
7.2	DELIVERABLE DESCRIPTIONS	38
	APPENDIX A – ANALYSIS REPORT	39
	APPENDIX B – INVENTORY & QUESTIONNAIRE SIGNOFF (IMPLEMENTATION).....	40
	APPENDIX C - SIGNOFF OF COMPLETION OF CLIENT WORK IN INSTITUTION.....	41
	APPENDIX D – SIGNOFF TEMPLATES FOR INSTITUTION REQUIRING EMAIL MIGRATION ..	42
	CRITERIA FOR EMAIL MIGRATION SIGNOFF (IMPLEMENTATION).....	42
	SIGNOFF OF COMPLETION OF EMAIL MIGRATION IN INSTITUTION	43
	APPENDIX E – SIGNOFF TEMPLATES FOR SGN.....	44
	SIGNOFF OF NEW INSTITUTION LINK TO OPERATIONS CENTRE (IMPLEMENTATION).....	44
	SIGNOFF OF NEW INSTITUTION ISP TRAFFIC VIA SGN (IMPLEMENTATION).....	45
	INSTITUTION'S SGN SIGN OFF / HANDOVER TO OPERATIONS CENTRE (PRODUCTION)	46
	APPENDIX F – IP SCENARIOS	47

APPENDIX G – LETTER OF COMMITMENT FOR USER TRAINING..... 48

APPENDIX H – NAMING CONVENTIONS 49

FUNCTION & DESCRIPTION LISTINGS 49

DOMAIN CONTROLLERS..... 49

MEMBER SERVERS 49

WORKSTATIONS..... 50

ACTIVE DIRECTORY..... 50

PORTAL NAME..... 50

USERS..... 51

NETWORK EQUIPMENT NAMING CONVENTION 52

APPENDIX I – DRAFT PROJECT PLAN 53

0.1 Document History

Version	Status	Reviewed/Approved by	Date
0.1	Draft	Abed & Shatha	16 th April
1.0	Issue		26 th July 2003

0.2 Changes From Last Issue

Version	Date Updated	Revision Author	Summary of Major Changes Made	Reviewed By	Review Date

0.3 Acknowledgements

N/A

0.4 Distribution List

Allan Gormley	EDS
Kendall Lott	EDS
Shatha Ahmad	MoICT
Abdelmajeed Shamlawi	AMIR

0.5 Referenced Documents

Reference Number	Title	Note
1.	SGN Statement of Needs reference JOG-CONS-ANLS-042-1.0	
2.	E-mail Statement of Needsreference GOJ.CON.S.ANLS.028.1.0	
3.	Joining SGN & eMail Initiative.mpp	
4.	SGN & eMail joing requiremenst.doc	
5.	RFP for phase in SGN & eMail Initiative.doc	

0.6 Abbreviations

DMZ	Demilitarized Zone
DNS	Domain Name Service
GOJ	Government of Jordan
LAN	Local Area Network
MoICT	Ministry of Information & Communications Technology
NIC	National Information Center
PC	Personal Computer
SGN	Secure Government Network
URL	Uniform Resource Locator – the official term for a web address such as www.nic.gov.jo

0.7 Glossary

This section defines the following terms that are used in this report:

CAT-5	Category 5 describes network cabling that consists of four twisted pairs of copper wire terminated by RJ-45 connectors. Cat-5 cabling supports frequencies up to 100 MHz and speeds up to 1000 Mbps. It can be used for ATM, token ring, 1000Base-T, 100Base-T, and 10Base-T networking.
DMZ	A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially <i>intranets</i> . All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Internet - also known as the World Wide	A worldwide network of linked PCs. Information is published to the public in graphical format on Internet Web sites for anyone to view. Many national governments now have one portal site to which users are initially directed, before being redirected (often by a search engine built into the

Web (www)	portal) to the Web site of the government department that they are seeking. (For an example, see www.ukonline-Gov.uk)
LAN	A network restricted to government users, which links PCs within a ministry. It uses protocols such as Token-Ring to share electronic files around the LAN. The format of these files is generally limited and will not usually include the graphical and enhanced formats that are available on an intranet.
Portal	A front-end software component that is provided on the Internet and on intranets (such as the SGN) to make it easier for users to find information and services. There are many components of a portal but the most important ones include a content management system (to ensure that the information content is of high quality), a search engine (to help the user find the information content that is of interest to them), and a directory of users.
Secure Government Network	An intranet that is provided by a government for the exclusive use of its civil servants. It will be provided with high levels of security to prevent any non-government users from gaining access to it. This type of network is also known as a Government Secure Intranet (GSI). Each Ministry will probably have its own intranet Web site that will provide information to intranet users.

1. Introduction

This Project Initiation Document continues with the initiative to establish an integrated Secure Government Network (SGN) and electronic mail system for secure Government-to-Government (G2G) communication. This document has been established to set out the requirements gathering, criteria to join the project and the implementation framework and has been prepared by EDS and in conjunction with representatives from Chemonics and MoICT as part of the AMIR 2.0 Program.

The document includes the following:

- Requirements Gathering
- Defining the project scope
- Objectives
- Approach
- Assumptions
- User Training Course
- Administrator Training Course
- Roles and Responsibilities

2. Project Brief

2.1 Business Product Definition and Scope

The expansion of the SGN and eMail initiative will be completed in stages. Each stage will be a phase in the SGN and eMail initiative and will be defined as a separate project using the same standard templates. The difference in the phases will be the government institutions involved. The size of each phase will be determined in the analysis stage but the business scope and the objectives will be the same.

2.2 Scope of the project

Each scope, Phase, is part of a wider initiative to introduce G2G communication to about 102 institutions numbering about 60,000 employees throughout Jordan. We believe that this will take about 3 to 4 years to fully rollout and will require heavy investment from the Government of Jordan.

Each phase will expand the membership of the SGN and includes the following

- Complete inventory of the existing hardware and network design within the joining institution.
- A readiness assessment that determines whether the institution will be included in this phase.
- The scope of the project will be determined, which will include details of the numbers of the following
 - ❖ RAM upgrades required in all the institutions
 - ❖ Replacement desktops in all the institutions
 - ❖ OS upgrades required in all the institutions
 - ❖ Users who will receive eMail (details of existing eMail accounts if relevant)
 - ❖ Functional eMail accounts and distribution lists to be migrated if relevant
- Implement the changes required to ensure that the institution's network is secured. This includes routing all Internet traffic via the SGN
- All users trained in Outlook functionality
- Two administrators trained within each institution to MCSA
- Anti Virus software installed on all user desktops and updated via the Operations Center
- Connecting the institution to the SGN via a 2MB leased line with ISDN backup.
- Installation of two servers within the institution as a child domain, which administratively belong to the local institution IT team.
- Handover of call logging to the Call Centre and operational support to the Operations Centre.
- Updating monitoring systems and maintain contracts for new hardware.
- Updating the existing documentation that exists within the Operations Centre with the details of the new institutions. Any relevant additional documentation will also be added.

To join the Secure Government Network, a point of presence is required within the institution. A generic set of networking equipment will be installed which includes firewall, router and switches. This equipment will be secured in a dedicated cabinet with an Ethernet port that will be connected to an existing firewall within the institution or to the Institution's own Local Area Network. This equipment will be supplied as part of the SGN and will be maintained and administrated as part of the SGN and not locally in the institution. The provision of the Internet via the SGN may make obsolete existing firewalls and routers; networking equipment within the institution is not within the scope of this project, however it must meet the joining requirements.

2.3 Objectives

The objectives of the initiative are:

- Increase the institutions using the government network for secure government to government communications;
- Increase the institutions connected to the secure electronic mail environment through which G2G communications can take place.
- Increase the overall security of government institution's networks by providing a secure link to the Internet for all external traffic.

Whilst this is a first step in enabling e-Government for Jordan, it is also fundamental to the wider goal of having on-line services and information available through a common portal to both citizens and businesses within Jordan as well as a more global audience.

During the initial phase the following have been setup, new institutions joining will join the existing structures.

- Operations center to manage the hardware – servers, routers and desktops – and associated software. The Operation Center is located at the NIC;
- Call center to provide first line support to the government employees using the SGN and electronic mail systems.
- SLA's which describe the agreed levels of service between the Operations Center and the member institutions.
- Procedures manual to cover operation of the Operations Center. This also details some of the standard functions within the institutions, example adding new users;
- Network Management – software which will manage the network loading and tolerances to failure;
- Hardware maintenance strategy and contract(s) for maintaining servers and routers. Contracts and SLA's will need to be established with Cisco, Dell and STS for the maintenance of this equipment.
- Connectivity – contracts and SLA's will need to be established with JTC for the connectivity on the SGN.
- Software – contracts and SLA's for the software including bug fixes, upgrades etc. are maintained by the Operations Centre. All licensing for the services offered within the Operations Center will be maintained by the Operations center.
- Monitoring software that alerts as soon as a failure occurs, either hardware or software. In most instances there is a backup that will be immediately implemented and the end user will not notice the failure.
- SLA to cover the service offering of the call center
- Management of client anti virus licensing for the desktops within the joined institutions will be maintained by the Operation Center.
- Monthly Reporting is being produced by the Call Center and the Operations Center on all aspects of their service.

2.4 Project-Specific Quality Procedures

The PMO Project Management team will maintain the Quality within the project and the PMO standards will be applied.

3. Analysis

3.1 Project Start

A new phase in the SGN and eMail initiative commences with a kick off meeting and presentation by MoICT with the proposed government institutions to be included in the new phase.

At this meeting the government institutions should receive the presentation - Joining SGN & eMail Initiative.mpp and obtain a copy of the document - SGN & eMail joining requiremenst.doc.

This document will contain all the templates required and details for gathering the information required about the institution. At this meeting MoICT will also agree with the government institutions a date by when the information gathering should be completed and submitted back to a contact person within MoICT. MoICT will provide a single point of contact for all queries with respect to the information gathering; each government institution will also nominate a single point of contact through whom all communications should be completed.

Note: The individuals nominated by both MoICT and the government institution at this stage can change once the initial analysis is completed, the scope of the project defined, at the project implementation kick off.

3.2 Information Gathering

The proposed government institution for the project will complete the following inventories and present them to the MoICT project Management by the agreed date.

- User/Desktop
- eMail
- Personal Information
- Institution LAN/WAN/Server Hardware
- Network Diagram
- LAN diagram
- IP allocation details
- Questionnaire for Communications Room and Facilities
- Questionnaire for ISP Service
- Questionnaire for NT Domain

3.3 Defining the project Scope

Once all the information has been delivered to MoICT project Management by the agreed date. The Report in [Appendix A - Analysis Report](#) must be completed. This covers the details that must be added to the RFP for each institution with regard to users and desktops.

The remaining information needs to be overviewed for any unusual issues that may exist. Once reviewed by a networking engineer and confirmation is given that all is in order, these documents should be filed until the RFP is completed and vendor assigned, the vendor will then need these documents to fully plan the project. These are listed below:

- Institution LAN/WAN/Server Hardware;
- Network Diagram;
- LAN diagram;
- IP allocation details;
- Questionnaire for Communications Room and Facilities;
- Questionnaire for ISP Service;
- Questionnaire for NT Domain

At this stage the scope of the project is agreed, once all the documentation is completed and the network engineer has overviewed the documentation, a decision is take on the institution joining this phase.

3.4 RFP

Once the RFP has been updated with the analysis report from each government institution it is published and a vendor chosen.

3.5 Implementation

The implementation part of the project commences when the vendor has been appointed. The kick-off meeting for this stage of the project should be the introduction of the vendor to the government institution representatives.

The implementation can be broken down into a number of components. These components are discussed below under separate headings.

3.5.1 Start-up and Engagement

Within this phase the following will have sign off between MoICT and the Vendor:

- Letter of Intent
- Contract
- Statement of Work
- Work Order

3.5.2 Project Plan

The project Plan needs to be updated by the vendor in conjunction with MoICT, this will be dependant on the delivery time frames for the hardware and the software and the scope of work within each ministry. This Project Plan will be used as the initial baseline.

3.5.3 Inventory

The initial task of the vendor is to confirm all the information gathered by the institutions. This information dictates additional purchasing requirements and rollout timelines and it is important that the vendor ensures that no assumptions have been made and the institution's expectation are meet where possible.

The vendor will meet with each institution and review the inventories for completeness. Once both parties have agreed the inventories, this will define the final scope. There should be no changes made after this.

The following lists the inventories/questionnaires that need to be agreed and signed off by both parties, signoff sheet can be found in [Appendix B – Inventory and Questionnaire signoff](#).

- User/Desktop
- eMail
- Personal Information
- Institution LAN/WAN/Server Hardware
- Network Diagram
- LAN diagram
- IP allocation details
- Questionnaire for Communications Room and Facilities
- Questionnaire for ISP Service
- Questionnaire for NT Domain

3.5.4 Documentation

The Vendor will work with the institutions to complete the following

- IP Design
- New Network Design Documentation

The Vendor will work with the Operations center to ensure that the existing documentation is used and any documentation updates required are completed.

- Network implementation document (configurations required)
- Active Directory Build documents including server build.
- Staging /ATP document
- Post implementation documentation, updates required for monitoring and Operations Centre support.

3.5.5 Ordering and Receipt of hardware and services

The vendor is responsible for all aspects of purchasing as detailed:

- Purchase of all Hardware and Software as detailed in the RFP, with any changes required as a result of the review completed by the vendor.
- Ordering of the JTC links and ISDN lines.
- Testing JTC Links
- Customs duty exception documents for all Hardware and Software
- Receipt of equipment to the relevant sites

3.5.6 User Training

Within each government institution, there will be a training coordinator (it is advised that the training coordinator within the institution is from HR and deals with all the other IT training requirements within the institution). This training coordinator will work with the Vendor to ensure that all users are trained in the most efficient manner (for example as close to their client roll-out as possible), ensure that they are placed in the correct courses (advanced users and VIP's where appropriate), ensure that all students sign the commitment letter in advance and that the training schedule is completed in advance of training (at least a week).

The approach to be taken is as follows:

- Training Data Collection
- Training Schedule agreed and published with students assigned to each class.
- Outlook Training completed

3.5.7 Administrative Training

Two administrators will be trained from each Institution's local IT department to Microsoft MCSA with the following modules:

- ❖ Microsoft Windows 2000 Network and Operating System Essentials: (approximately 20 Hours)
- ❖ Supporting Microsoft Windows 2000 Professional & Server: (approximately 44 Hours)
- ❖ Managing MS Windows 2000 Network Environment: (approximately 52 Hours)
- ❖ Implementing and Managing Microsoft Exchange 2000: (approximately 44 Hours)

The approach to be taken is as follows:

- Gathering of Admin details who will complete the training.
- Training Schedule to be published and agreed between the Vendor and all the students.
- Training Completed

3.5.8 Staging of Network equipment

The Vendor is responsible for staging, the Operations Centre

- Detect out of Box failures and wrong shipments at an early stage during the Implementation
- Conduct all testing before the equipment is sent to the different sites, thus making sure the equipment will go live on the targeted dates
- Change control followed for all aspects of the installation.
- Minimal Downtime during installation.
- Accurate records of components that exist in each location
- Consistency in system configurations and guaranteed compatibility among multiple sites with the existing standards.
- Delivery to government institution
- Monitoring configured
- Handover to the Operations Centre with sign off by both institution and Operations Centre.

3.5.9 Client Rollout

- Vendor agrees with Government Institution the plan for upgrade and installation of equipment.

The client portion may be completed in sections, work that can be completed immediately and that work which required the new equipment arriving or the domain installed.

- Client OS upgrades (where RAM is not an issue).

- Installation of necessary software (Office & Outlook)

Once the new equipment has been delivered:

- RAM upgrades
- New Desktops rolled out to users
- Remaining OS Upgrades and software installations completed.

Once the child domain has been installed

- Add each Desktop as a member of the domain
- Install the Anti Virus on each desktop and configure as per standards

Depending on whether the institution has existing email or whether email is being implemented for the first time there are two main approaches. Before either the rollout or migration commences the “Jordan e-Government Institution Test Acceptance Document” must be completed and signed by both the Vendor and the Institution.

3.5.9.1 No existing eMail within Government Institution

If no existing email, then the email client can be configured as the desktop enters the child domain. This will save on the number of visits required to the users desktops. In this case there will only be one signoff required stating that all the work is complete, this signoff is found in [Appendix C – Signoff of Completion of Client work in Institution](#)

3.5.9.2 Existing eMail within Government Institution

Otherwise for email migration

- Obtain signoff per institution before moving on that all client upgrades are completed and all users have been notified. Sign off sheet in [Appendix D – Criteria for eMail Migration Signoff](#)
- eMail migration completed
- Signoff by the institution that migration has been completed. Sign off sheet in [Appendix D – Completion of eMail migration](#).

3.5.10 Child domain installation

- Operations Centre create child domain and setup single admin account that will administrative the child domain ensuring that this account has no access to the root or any other child domain.
- Vendor ensures that the admin access within the child domain adheres to the standards already implied, especially ensuring that no other administrator accounts outside the domain can see or administrative the new child domain.
- Servers installed to standard build documentation
- Users created to the defined standards
- Vendor ensures that the administration software is installed on administration workstations and that each administrator is given their unique account for administering the child domain.
- Vendor completes overview of administrative tasks that are completed by the institution staff
- Institution signoff on Domain installation and handover of administrative tasks with associated documentation, signoff sheets covered by Appendix C & D.

3.5.11 SGN Infrastructure Implementation

- Mounting of the equipment in the cabinet (CISCO)
- Power on diagnostics for Equipment.
- Connecting cables between equipment
- Connecting the JTC links to the equipment at the institution
- Obtaining Change control for completing the required cabling.
- Connecting JTC links within the data center.
- Testing the interfaces and the links
- Site ready for SGN connectivity
- Obtaining Change control for completing the required configuration
- Implementing the required configuration and testing the new link
- Adding the new leased lien to the monitoring station
- Configuring the monitoring on the new PIX Firewalls, Switches and Router.
- Testing of the monitoring

- Monitoring operational within Operations Centre
- Acceptance testing – Signoff sheet to be found in [Appendix E – Signoff for Institution joining SGN](#).

3.5.12 Internet Traffic

All Internet traffic will be routed via the SGN, either to the NIC or to another ISP provider.

- Obtain change control approval
- Configuration changes implemented on link and internet traffic routed via the SGN
- Redundant links disconnected from the institution's network
- Signoff received from government institution that network changes complete and all services working. Signoff sheet found in [Appendix E – Signoff on Migration of Internet traffic](#).
- Obtaining Acceptance testing
- Ensure full monitoring on place
- Call Center are ready to accept calls from the new institution
- All documentation within Ops Center has been updated to include the new institution
- SLA has been agreed and signed
- Ownership transferred, all accounts used by Vendor changed/disabled where appropriate.
- Signoff from Operations center that network configuration completed as agreed both in Operations Centre and in government institution. Network engineer from Operations center to complete initial security audit of joining network.
- Operations Centre takes full ownership for new configuration and support of links. Signoff sheet found in [Appendix E – Signoff on SGN Connectivity and Handover](#)

3.6 Project Roll-out and Approach

3.6.1 Management of the project

MoICT PMO will have the ultimate responsibility for the management of the project, however the Vendor Project Manager and the Project Manager from the government institution also have responsibility for large parts of the plan.

3.6.2 Meetings

There will be three meetings that are relevant to the project, these are:

3.6.2.1 Technical Meeting

This meeting is held weekly, chaired by the MoICT Junior project manager and includes the following:

- Technical issues including status of leased lines, purchasing, inventories.
- Training report on training completed
- Training plan for the coming week
- Plan of work for the coming week

3.6.2.2 Steering Group Meeting

This meeting is held bi-weekly, is chaired by the MoICT project manager and includes the following:

- Updating the project plan Project status report Local Change Management, example work within the government institution – DHCP configuration Quality control

3.6.2.3 Operations Meeting

This meeting is held monthly, is chaired by the Operations Manager and includes the following:

- Current status of Operations including details reports from the previous month A global Change Control - change that has the potential to affect one of more members of the SGN, for example router configuration updates. Operational issues Update on current projects being implemented

3.6.3 JTC Links

The installation of the JTC links will be the running of JTC cables up to the ministry buildings. The actual connection of these cables to the equipment and the testing thereafter will be the responsibility of the installation team (Vendor). JTC will need to be involved in the testing exercise should problems arise. The vendor project manager will carry out the co-ordination of these activities.

3.6.4 SGN Installations

The Vendor's installation team will complete the SGN installation, however the Operations Centre Manager is responsible for ensuring that all change control is completed and that the vendor has all the information required to ensure that the correct standards are implemented and ensuring that the security of the SGN is not compromised.

The Operations Centre is responsible for managing the administrative accounts that the vendor uses on existing devices and ensuring that these accounts are only valid within the change control periods.

3.6.5 Desktop & User Inventory

A user /machine inventory will be completed. This inventory will have two main purposes, namely:

- On completion of the inventory, the PCs requiring upgrade will be identified. Those PC's requiring replacement will be identified separately. Additional licensees need to be identified and purchased as appropriate. The intention of the project team is wherever possible to make full use of existing Servers and PC equipment and associated licensees. At the end of the project no desktop should remain connected to the network that does not meet the minimum standards.
- A user list will be completed for each institution connecting to the SGN and Microsoft Exchange 2000 Email system. This list will identify the users to migrate. The inventory may also be used to determine the level of training a user requires

3.6.6 Approach to ensure institution's Desktops meet requirements

Based on the user/machine inventory, machines with a processor of PIII (or higher) and 64 Megabytes of memory will be upgraded to the windows 2000 operating system and the Outlook 2000 email client. Any machine with Processor/Memory less than this should be replaced.

3.6.7 Desktop AntiVirus Software

The Vendor is responsible for ensuring that the Anti Virus is installed and configured on each desktop within the institution and relevant servers. The Operations Centre is responsible for ensuring that licensing is valid, by ensuring that the relevant details are included in the RFP. The Vendor is responsible for handing over the licenses purchased to the Operations Centre.

3.6.8 Users accounts Creation

The implementation team will manually create the users accounts using the new naming convention, this may create the problem of the user mailbox address changing (i.e. e-mail account will change). This will be fixed by adding a secondary e-mail address to the user properties in the active directory; this e-mail address will be exactly the same as the old one. This will ensure that each user can receive e-mails destined to the old or the new account

The implementation team is also responsible for ensuring that all the users details are entered as detailed in the personal information.

3.6.9 Password migration

There is no way to migrate the old passwords from the old e-mail system or NT system, so after creating the account in the AD, the implementation team will create initial password for each user. It could be his account name + his extension number for example, this will be defined as by the institution local IT group.

3.6.10 Data migration (where email migration is required)

If users have an existing email account, the implementation team will copy the contents of the existing email account to a personal folder on the users desktop when configuring the Outlook client to access the new email box.

3.6.11 Rollout of eMail for Institution with existing eMail service

- Addition of new MX record (institution.GOV.JO) pointing to the new exchange server. At this point all emails will go to the email server within the data centre.
- Rollout all email users, using the priority list drawn up by the institution IT Group.
- When all email users have been migrated then the old email server decommissioned (or at least the email service decommissioned)
- Signoff by the institution that all email users have been migrated. Signoff sheet is attached in [Appendix D – Signoff for eMail migration](#)

3.6.12 Internet access and ISP

Internet access and the ISP will be handled via the NIC and through the data center. Appropriate actions and discussions will need to take place to identify those institutions that currently have other ISP's. Conflicts will need to be addressed and resolved. Relevant information regarding proxy server, current Internet facing web servers will be collected via the network inventory to facilitate migration if necessary.

All devices that require publishing on the WWW will be provided a published IP address by the Operations Centre. The vendor is responsible for requesting and obtaining these IP addresses. The vendor is also responsible for ensuring that the relevant DNS changes are made at the appropriate time to ensure that there is minimal downtime.

In the event of the NIC not providing the ISP service for a particular institution based on different technical requirements, the relevant institution will still be required to route all traffic via the SGN and the alternative ISP will connect to the SGN also. Routing will be configured in such a way to ensure that only Internet traffic from that institution passes to that ISP and none of this traffic is passed via the NIC

3.6.13 IP Network

A detailed IP addressing solution for the Government network exists. The project will include changing the current addressing schemes within the institutions. Scenarios have already been documented and where possible these should be used for consistency, however should another scenario be required, this should be drawn up in line with the IP solution and documented by the implementation team. [Appendix F – IP Scenarios](#) contains details on these existing scenarios.

The vendor will work with the Institution to ensure that a new IP schema is drawn up and documented. Once the Operations Centre representative approves the schema, the changeover is planned and change control is drawn up. The Vendor then works with the institution to implement the new schema, this must be completed before the eMail rollout/migration can be completed.

3.6.14 Network monitoring

This is the responsibility of the Implementation team to implement with the co-operation of the Operations Centre. The Operations Centre are responsible for completing the change control and ensuring that security is not compromised by creating an admin account for the duration of this project that is only activated during the periods of change control. The network monitoring will monitor the E1 and ISDN links, also monitor all hardware devices for any hardware failures.

3.6.15 Support and Maintenance

The Operations Centre is responsible for ensuring that the definition within the RFP for support and maintenance is accurate and fits well with existing contracts. Where possible new contracts should fit directly with existing contracts to ease administration.

The Vendor is responsible for setting up the maintenance and support contracts in line with the definition within the RFP and handing these over to the operations center and obtaining signoff on this. The signoff for this is in [Appendix E - Institution's SGN sign off](#).

3.6.16 User Training for Outlook

All users should be trained in the use of Outlook 2000 and the OWA email clients. Training will be scheduled in a way for all users migrating to the new Microsoft Exchange 2000 system to attend training prior to receiving their new email mailbox. Training should occur, as close to the date of deployment as possible - within a three week period is the ideal.

Prior to training all students must sign a letter of commitment, see [Appendix G – letter of commitment](#) for letter to be signed. The local training coordinator within the government institution is responsible for ensuring that this is completed and handing over the signed letters prior to training to the MoICT Project Manager. The local training coordinator is also responsible for ensuring that students are allocated to the correct classes as early as possible.

When training starts, the Vendor will complete a roll call of all expected students and fax the results to the relevant government institutions within an hour of class commencing, this will allow the relevant training coordinator time to follow up and determine what happened in a timely manner. The attendance sheets will be completed at the end of every class and submitted to the MoICT project manager with details of any absentees.

Any students that fail to attend their initial training session, may be given a second chance to attend, this will be decided by the MoICT project manager if there is a valid reason for the initial non attendance, otherwise attendance will be at the cost of the individual or the relevant government institution.

3.6.17 eMail migration order within government institution.

For smaller ministries, with existing email service, the users should be migrated over a weekend. There should be at least 2 notifications to the user community notifying them of the email migration. When the user arrives on Sunday morning his machine will have been reconfigured and all email (internal and external) will be directed to the new Microsoft 2000 Exchange mailbox. There will be support people on hand to handle customer questions and troubleshooting.

For larger ministries, with existing email service, there may be some need to migrate users over a longer period of time. This may also require some migrations to occur during working hours. Because not all users can be migrated during the same time period this will cause a problem in directing inbound Internet mail to the ministry. The recommendation would be to continue directing all inbound Internet mail to the new mail server and the local IT group within the institution draw up a list of priority users that need to be completed within the first morning or first day.

The order of rollout for institutions within the scope should be decided on which institutions are complete with all other aspects of the project and ready to proceed first. Also may be determined by the volume of work required within each institution.

3.6.18 Microsoft Licensing

Licenses from the current agreement between the Government and Microsoft will be utilized by the project for the clients and servers.

3.7 Assumptions

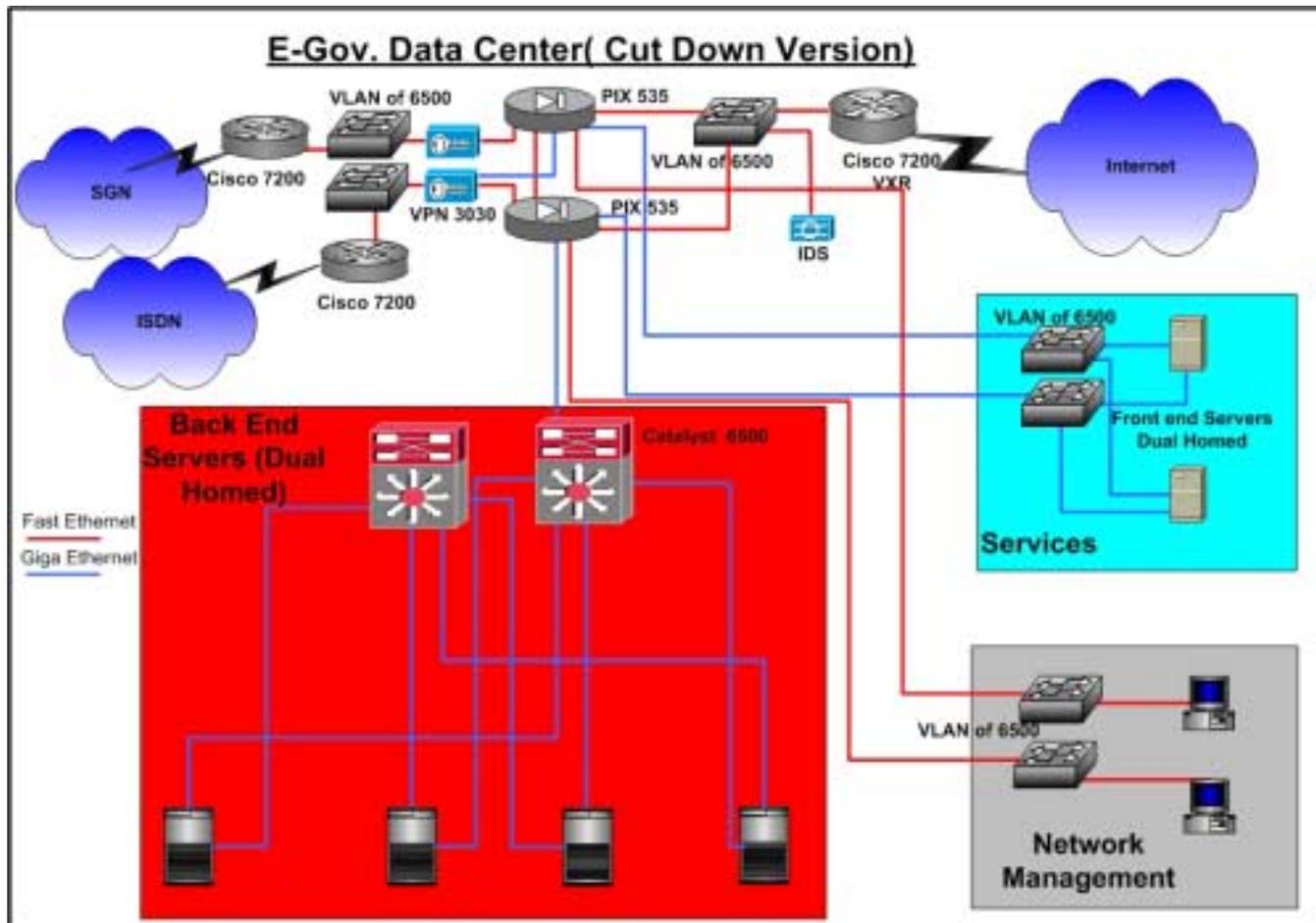
The following are the key assumptions, which we have made in determining the costs and implementation plan for this part of the project:

- All institutions will adhere to the existing standards.
- The Links will be E1 with ISDN backup.
- The NIC will be the ISP for all connected institutions
- The local IT team within each institution will be available at all stages to assist the implementation team where necessary.
- An Ethernet network exists within each institution.

4. Detailed Design

4.1 SGN

The e-Government data centre is currently sited at the NIC. The following diagram shows the initial installation currently installed. It is expected that there will be future expansion to support additional services example RAS, Web Services and Content management.



4.1.1 e-Gov Operation Centre configuration

Jordanian e-Government Operations Centre is to be divided into five different security zones, the zones are separated using the Cisco PIX firewalls 535 bundles with a fail over PIX to cater for the resiliency and fault tolerance.

The Outer Zone located at the interface between the Operations Centre and the IGR /Internet cloud. This zone is composed of Cisco 7200 VXR routers, which is mainly used to provide the required Internet access to e-Government applications and services as well as for the ministries & other involved departments users.

The IGR is connected to the PIX 535 outer interface and is given the lowest security value. There will also be an IDS probe at this segment as well to monitor all kinds of traffic and possible attacks on the Secure Government Network & services.

The second security Zone is the SGN Routers, which are connected to the PIX firewalls bundle (active & Failover) via VLANs on the two Cat 6500 switches, for fault tolerant and redundancy, we will have each router connected to one Cat switch, and each switch connected to one of the PIX firewalls, the Cat switches are interconnected via GBICs. The proposed Cisco 7200VXR routers at the Operations Centre used to interconnect the various ministries will be capable of handling the traffic generated to and from the other government ministries and/or departments. In order to maximize the resiliency at SGN gateway routers, Cisco HSRP (Hot

Standby Routing Protocol) will be running, this protocol will ensure the automatic route of all traffic from one router to the other if one of them should fail. This should maximize communication availability with other ministries. HSRP will provide redundancy on the links as well as load balancing. The e-Government's vision is to have two different links connected to the JT Cloud. Initially there is one main link on SGN-Router-1 and the Dial Backup on SGN-Router-2.

The other component of this security segment is a VPN concentrator, which is installed between the RAS and the PIX. This will cater for the VPN Access of mobile users into the Government intranet & Operations Centre with different security levels. The Cisco VPN 3030 can handle up to 1500 concurrent VPN sessions and support both pre-shared keys (username & Password) and digital certificates, once the PKI solution is in place.

The third security zone is the Front End Server Zone (Services). For server's aggregation all the servers are to be connected directly to the Catalyst 6500 switches. The Front-End Dual-Homed servers will be connected via Gigabit Ethernet to both Switches. On the other hand each Catalyst 6500 will be equipped with one 48-Port 10/100Mbps Fast Ethernet modules and an additional two 16-Port Gigabit Blades, connecting the Servers and the PIX Firewalls. VLANs implementation is considered at this stage for maximum security and manageability.

The fourth Zone resides on another DMZ Zone of the PIX 535, utilizing a fast Ethernet port of the PIX 535 firewall used for connecting the Management Stations Centre, the proposed management stations include Cisco Works 2000 and Cisco Secure Policy Manager, for Network and PIX management respectively.

The fifth and most secure Zone is the Back-End Server Zone connected to the inside of the PIX 535 firewall,

4.1.2 SGN

The Secure Government Network (SGN) is the heart of the e-Government project, so scalability, security, manageability are all among the important factors we considered when designing the WAN infrastructure.

At The Operation Center, two Cisco 7200 Routers are used as the main SGN gateway routers, each router is connected through a separate physical line to the JT Cloud, the main link speed was fixed to 2 MB (E1) while the dial backup link will change depending on the bandwidth requirement dictated by the applications (64 or 128Kbps), the two routers are running HSRP for maximum resiliency

For the two routers front-end Cisco PIX 535 firewall, high availability is supported at this level with the deployment of a redundant hot standby failover unit. This failover unit maintains concurrent connections through automatic stateful synchronization. This ensures that even in the event of a system failure, sessions are maintained and the transition is completely transparent to network users.

For the government institution's connectivity to the SGN, the Cisco 3660 is equipped with dual power. The router is connected to two Cat 2950 Switches stacked via a Giga Stack GBIC and the switches are connected to the PIX firewalls The inside of the PIX firewalls are also connected to Switch Stack, to eliminate single points of failure. An IDS probe is also recommended here to be connected in the inside network. Encryption for the traffic will be done on the PIX firewall.

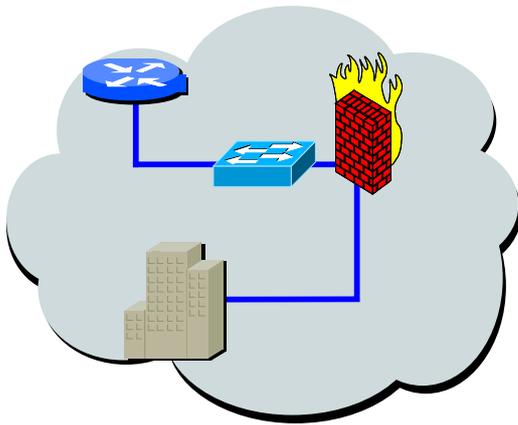
4.1.3 Connecting to the SGN

Each new institution requires an E1 and ISDN connection to the Data Centre. This work must be carried out by JTC and tested by the installation team.

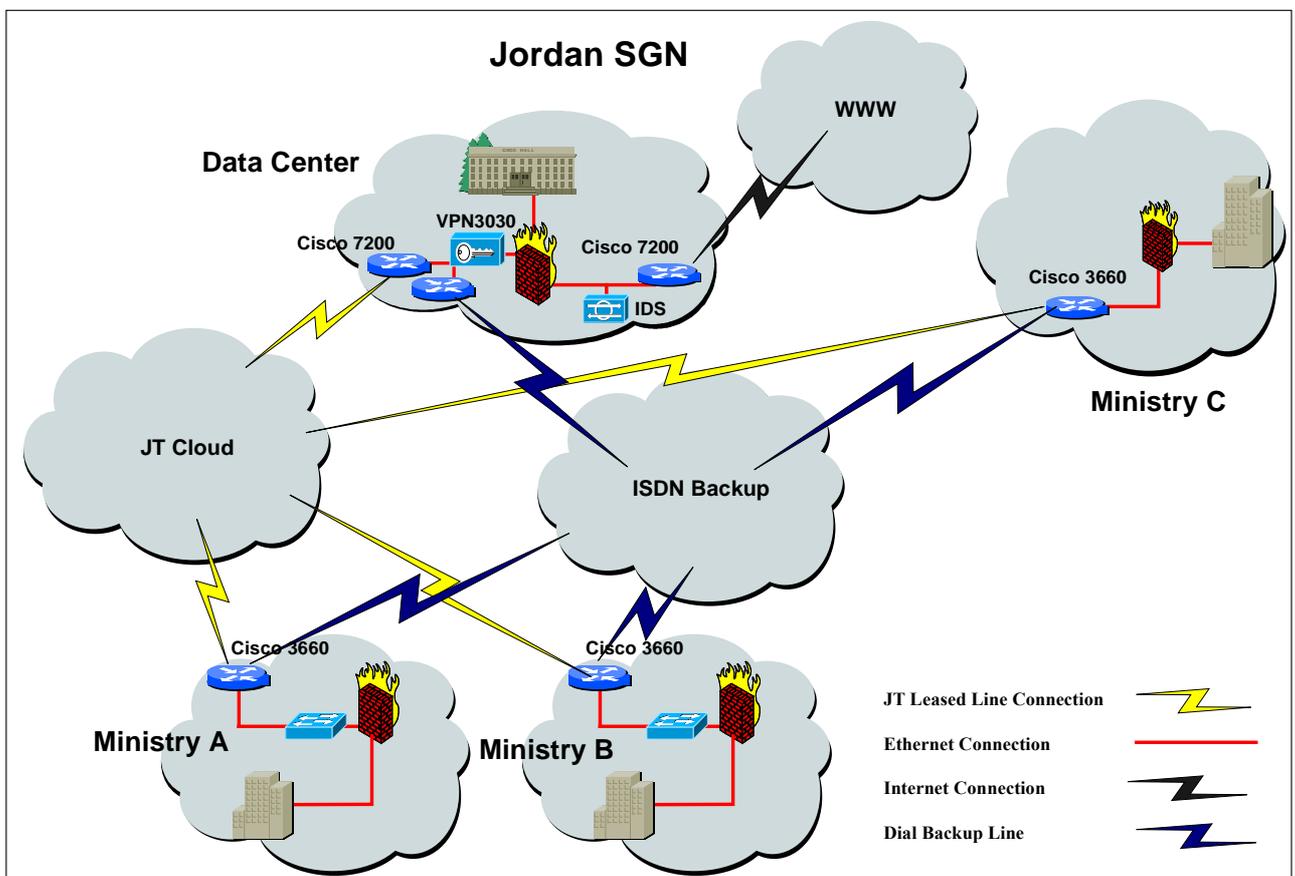
Each Institution will be required to have the following minimum configuration:

- A Cisco Router
- A Catalyst Switch
- A Firewall.

These will be connected as shown in the diagram below and will be housed in a separate cabinet within the government institution.



The design of the SGN will remain consistent and each institution will be connected in the same manner as existing connections. The overall configuration is shown in the diagram below.



4.2 IP Addresses

All new additions to the SGN will be given new IP addresses in line with the IP design strategy. Two scenarios have already been drawn up and used by the existing SGN institutions; these are detailed in [Appendix F – IP Scenarios](#). Additional scenarios may be drawn up if these are not applicable to the joining institution’s requirements, the only criteria are that these meet the IP standards already defined, this is documented within the Operations Centre.

- All Government institutions joined to the SGN will utilise these IP standards; this facilitates the following:
- Standard approach across all institutions to IP policy and security
- Allows ease of communications between institutions if requested

- Allows communications between institutions and Operations Centre without having to use IP translation and therefore facilities tracking of source if issues occur and facilities troubleshooting if problems exist.
- Prevents duplication of IP ranges within joined Institutions.
- Ease of Administration and support.

4.3 Client PC's

Each PC connected to the SGN must be of a minimum configuration. Existing PC's will be analysed for their upgrade capability. PC's that do not match the specification will need to be upgraded. Any Desktop with a processor of PIII can be upgraded if required to meet the minimum specifications for a Desktop to have Windows 2000 operating installed. This minimal configuration is:

- P4 1.7GHz
- 256 MB RAM
- 4GB of free space on the hard drive

Note: Generally only the RAM is upgraded.

The following is the specification of the minimum specification of new PC's purchased for connecting to the SGN. These specifications are based on Dell hardware; alternative hardware of similar specification will be accepted.

- P4 2 GHz.
- 256MB RAM
- 20GB Hard Drive
- 16MB AGP Graphics Card
- CD ROM Drive
- 1.44MB Floppy Drive
- Integrated NIC and Sound
- 15" Monitor (No Brand specific equipment)
- Windows XP Professional
- Microsoft Outlook

4.4 Enterprise Directory

The Government of Jordan will be deploying a Single AD forest / Single Exchange Organization infrastructure for the initial phase.

A root domain (GOJ.Local) will exist at the operations centre and will be named '.GOV'.

4.4.1 Child Domains

For the initial government institution, each institution will have its unique child domains. This will be created in the Operations Centre and administration will be configured so that only administrators created within the child domain will have any rights. By default the enterprise admin account will be removed from the administration group within the child domain but will always have the access to be able to rejoin this group if required. To maintain the highest level of security, this account will not be used unless specifically covered by change control and the passwords will be slit so that no individual will ever have it. In the future a more secure solution will be implemented.

This will enable the institution to full control over its domain and to remain operational if the line to the E-government Operation Center is down. All remaining institutions will be contained under a separate child domain. Example of Child domains:

Child Domain	Name
Government of Jordan – all other ministries	GOJ.GOV
Ministry of Information and Communication Technology	MOICT.GOV

The following is a pictorial example of the structure:

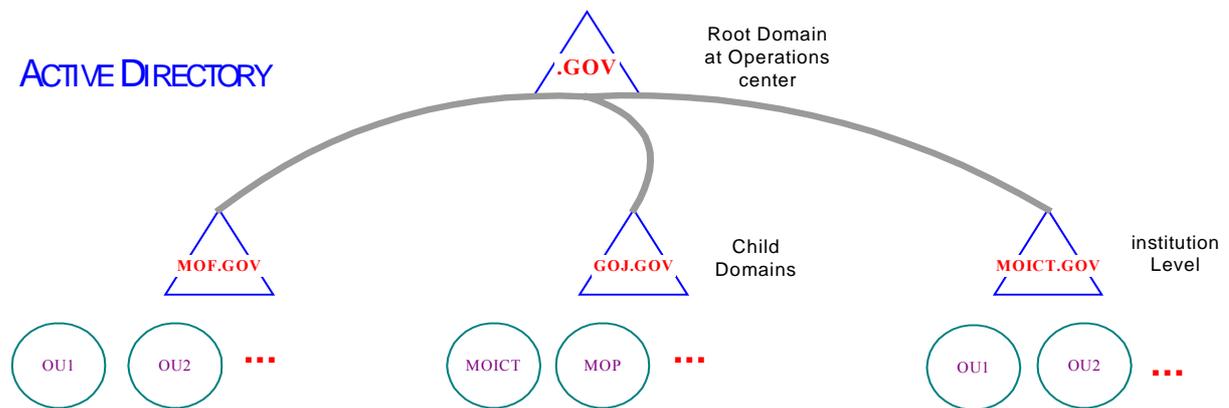


Figure - Additional Child Domains

This Single Forest / Multiple domain architecture supports the following functionality.

- **Supports a decentralized administration model:** GOJ will be utilizing a centralized support Model. This model is easily adapted to be a decentralized support model. Members of the Domain Administrators Group in each domain only have authority over the local domain. It still requires coordination among Domain admin groups.
- **Supports multiple domain security policy:** Security policy settings are only available at the Domain level. Although you can set different security policies, GOJ will enforce a global security policy. Each Ministry would have to show clear reasoning for a desire to create a different security policy and therefore a new Domain.
- **Supports domain and/or OU administrative delegation:** AD supports the capability to delegate authority for specific administrative functions. This can be done at either the Domain or OU level. In this model delegation can be set at either level.
- **Replication traffic isolation:** Replication is isolated between domain controllers within the same domain. Forest wide information such as schema, global catalogue, and configuration container are replicated between domains, but this is generally a small percentage of the domain replication.
- **User authentication:** Through Kerberos trusts, domain users can be authenticated through any domain in the tree.
- **Cannot “demote” a domain:** A child domain cannot be “demoted” to an OU if it is not necessary. But OU’s can be made into domains.

4.4.2 Domain Dependencies

The solution depends on the following points being implemented for its coherence and completion, they are:

- Each of the connected government institutions needs to have the correct hardware to be a child domain, which is two domain controllers.
- All Client workstations and servers in each of the joined institutions need to join their new domain.
- Each of the joined institutions will apply its account policy.
- Child Domain data and backup will be the responsibility of each joined institution.
- A single Global Address List is needed for all **GoJ** employees.
- Each of the joined institutions will have full Administrative control of itself.
- Security boundaries are needed between institutions.

4.5 Users

Users’ accounts will reside in the Active Directory. The users will need a “**Log on**” name to access the domain and resources on the Network. Users will also need a user name account for using the E-mail application on the Network. We unified both names so a user will need to remember and use only one name for the domain log on and e-mail account.

Details of the standard user name conventions are found in [Appendix H – Naming Conventions](#)

4.6 eMail Service

4.6.1 Functional Requirements

The following requirements have been implemented within the Exchange solution in production within the Operations Centre.

4.6.1.1 Messaging Service requirements

The Messaging service is made available to all registered Government employees and internal applications to provide a full messaging service (messaging, calendaring, scheduling, contact lists, etc). This service also provides a central point for the interconnection of department's email into a Government-wide network, including connectivity to the external Internet.

The messaging service improves existing communications while providing a better class of service. Through redundant technologies and security measures the environment is provides both ease of use and speed of communication as well as its fault tolerant design.

Although, a feature rich client will provide the primary access to the service, a variety of clients will be supported to accommodate users such as remote or mobile users.

The Messaging service implemented supports the following, not all of these may be fully available due to security decisions taken during the design and implementation:

- Support for a central environment that will act as the single point of communication with Institutions/Agencies and Internet mail.
- Support for the ability to handle multiple email domains.
- Support for MAPI, SMTP, POP3 and IMAP4
- The messaging solution needs to support full functionality with a web browser.
- Environment capable of scaling up to 100,000 + users.
- The scalability of the solution must include the requirement that not all 100,000 users will be supported day one and the solution, without loss of functionality, must be able to be deployed as the user population grows.
- Support for common portal technologies.
- Support for other clients/devices in the long term e.g. wireless or PDA's.
- Support for inter-connectivity between differing email services/products in a seamless manner (from the end user perspective), including Internet email services (SMTP), Exchange, MS mail, Lotus Domino, etc.
- Support for a "Global catalogue" of email users, including all users of departmental email services.
- Support for working with a corporate central directory (based on X.500) through standard X.500 supported protocols, including LDAPv3.
- Support for 'electronic forms'.
- Support for workflow.
- Support for remote management through the use of standard products and protocols e.g. SNMP, and/or through use of specific management/administration tools provided with the product.
- Support for the Arabic language.
- Spell checking capability at the client level.
- Support for Auditing and Reporting e.g. Mail File sizes, authentication failures, usage, etc.
- Support for Mailbox limitations.
- Support for Mailbox archiving.
- Support for Administration tools.
- Support for integration with leading Document Management technologies and products.
- Provide adequate levels of authorization and data content security, as well as third-party security capabilities through the utilization of industry supported APIs.
- Clear and manageable security mechanisms must be in place for the allocation and control of administrative rights and permissions with the service.
- Support for administration delegation of duties and access control to functions/tasks.
- The product supports the use of access control lists, along with secure management of those lists.
- The product supports encryption and digital signatures e.g. PKI.
- The product supports secure access over a public infrastructure e.g. Internet.
- The product supports the integration of market leading anti-virus products, both at the server and client level.

4.6.1.2 SMTP Relay Service

The solution ensures that all Inbound/Outbound Internet mail traffic will flow through the SMTP Relay service. The SMTP Relay service will provide the ability for departments to communicate with each other while maintaining a speed and class of service that will attract all departments. This centralized service provides the optimal ability for controlling viruses, content management and message tracking In and out of the Government wide network.

- The SMTP Relay service relays messages from both the Internet and other Ministries that are on the SGN but not yet connected to the Centralized Messaging system.
- The SMTP Relay service routes multiple email domains for both inbound/outbound email.
- The SMTP Relay service is isolated in a “DMZ” from the Internet and the internal production network.
- The SMTP Relay service supports anti-virus scanners and content management.

4.6.1.3 Directory Service

The Directory service is available to all registered Government employees on the SGN and internal applications to provide a single information repository for employee information. This Enterprise Directory will be synchronized with other application directories in order to keep information accurate. The initial phase only provides the user’s information within the Directory service.

The Enterprise Directory is intended to be leveraged, as much as possible, by users and applications as a central point for querying information. Other internal applications will leverage this directory for authentication and information queries. The Directory supports synchronization with an external directory if external applications are required to update this directory.

The Enterprise directory holds sensitive information so proper security methods are in place to protect the information from unauthorized use.

- The product supports X.500 based standards, including Lightweight Directory Access Protocol (LDAPv3).
- The product supports the ability to extend the schema by providing tools and interfaces to add/modify/delete object classes and attributes.
- The product supports methods of distributing the directory and segmenting the management of information.
- The implementation supports limiting the distribution of information (only a subset of information and/or attributes) to/from other directories during replication and synchronization.
- The implementation supports synchronization with other directories, either by use of third party tools or standard methods, must be ‘near instantaneous’.
- The directory supports additions/changes/deletes from multiple directories
- The directory addresses synchronization conflicts (e.g. through rules based resolution or administrative notifications) with limited effect on the end-users or applications ability to receive accurate information in a query.
- The product supports access from a range of clients and ‘platforms’ to the directory e.g. application, browser, third-party email client, PC, wireless, PDA, etc.
- Supports remote administration of the directory either through specific tools or integrated with the management toolset.
- Management of the directory is through an intuitive and easy to use interface.
- Supports Single Sign on functionality.
- Supports a wide variety of queries based on objects and values stored in the directory.

4.6.1.4 Email Resilience

The implementation has the ability to be available 24x7, the required supports are in place to ensure that the availability is maximized. Careful planning and an appropriate infrastructure achieve this. Messaging and Directory services are critical applications for the business of The Government of Jordan. The environment is available to users when they need it, which could be any time.

- The product and its operating system support failover architectures.
- The product utilizes a mass data storage solution that has a high availability back up and recovery. Within the mass data storage, extra storage is made ‘invisible’ to the service as seen by the end user.

- The product supports a dynamic back-up and recovery regime whereby data can be easily backed-up, without recourse to closing the system down, and restored, either completely or in part.

4.6.1.5 Deployment

Since the deployment of the eMail solution is being completed on a phased approach, the solution implemented supports this phased approach. The initial installation will not support the full scope of the initiative but expansion is possible without effecting the current deployment.

4.6.2 Exchange Server Technical Design

There are many aspects to the Exchange 2000 server design. The following details messaging server roles, database architecture, hardware configuration, disk configuration, Processor and Memory, the use of clustering technology and mailbox size limits.

4.6.2.1 Server Roles

A single Exchange 2000 server can perform many roles or those roles can be delegated to dedicated servers for performance, management or security reasons. The assigned roles within the GOJ implementation are:

- **Back-end server.** System dedicated to housing mailboxes with an appropriately sized, highly available disk subsystem. Deployed on clustered servers.
- **Front-end server.** Server that handles the Internet protocols HTTP, IMAP4 (Internet Message Access Protocol version 4), POP3 (Post Office Protocol version 3), NNTP (Network News Transfer Protocol) and SMTP and passes them through to back-end mailbox and public folder servers. Front-end servers do not house any data and are commonly used in a perimeter network (also known as DMZ, demilitarized zone and screened subnet) for security purposes.
- **Public folder server.** In the initial implementation the Back-end servers support this. System with disk configuration dedicated to housing public folders. Can separate public folder load from mailbox; one public folder server can support several mailbox servers.
- **Connector server.** This function is available on Back-end servers.

4.6.2.2 Database Architecture

The data stored on the Exchange 2000 server is housed in one or more information store databases. Each database consists of two files, one optimised for messaging application programming interface (MAPI) data, the other for Internet protocols and streaming data. Up to five databases can be assembled into a storage group and a single server can support up to four storage groups. The Exchange information store uses transaction log architecture to improve performance and provide rollback in the event of failure. All the databases in a single storage group share the same set of log files.

Exchange 2000 supports online backups as an appropriately designed backup program is utilised. For efficiency all databases in a single storage group are backed up as a unit because otherwise the transaction logs will be backed up repeatedly, once with each database. It is possible to restore a single database while the others in the group remain online and active.

Should it be necessary to recover a database, the most recent full backup of the information store will be restored along with all the log files generated since that backup. If log files are available up to the moment of failure, then the system will recover right up to the last committed transaction. It is important to provide a reliable disk subsystem for Exchange 2000 because disk failure will force recovery procedures. It is critical to protect the log files because they contain data for recovery after the time of the previous backup.

The reasons for dividing data into multiple databases on a single server include:

- Keeping the size of each individual database down speeds up restore time for any one database.
- Keeping the size of each individual database down makes it faster to run database utilities should the need ever arise.
- When recovering from a complete server failure, users can be brought back online database-by-database rather than having to wait for one large database to restore. It may be possible to restore databases in parallel if the backup hardware supports it.

Reasons for not dividing data into multiple databases include:

- The benefits of single instance storage are more noticeable with one database. A message sent to several users in two databases will be stored twice.
- Additional databases require more memory, though not as much as an additional storage group.
- Adding a storage group has more performance overhead than adding a database to an existing storage group.

Reasons for adding storage groups include:

- There are already five databases in an existing storage group and another database is needed.
- Each storage group has different logging needs—for example, one houses mailboxes and requires that circular logging be off, while the other houses Internet newsgroups and requires circular logging to be on because it will not be backed up.
- Support of clustering; because whole storage groups are moved between cluster members rather than individual databases.

4.6.2.3 Disk Configuration

Disk input/output performance is a vital part of the total performance of the Exchange 2000 server. The desired disk characteristics of each type of server include the following elements:

- Placement of data
- Storage requirements
- (RAID) Redundant array of inexpensive disks technology

Exchange 2000 uses different storage areas for different purposes. The storage is always fault tolerant; that is RAID 5, RAID 1 technology. To improve fault tolerance, redundant RAID controllers in active-active mode are used and have one or more standby disks per disk enclosure.

Note: In the following discussion the term *volume* describes two or more physical disks grouped together using RAID 5, RAID 1 technology. Note that this is different from two or more partitions of the same physical disk.

Basic guidelines followed for configuring disk subsystems for Exchange 2000 were as follows:

- Create a RAID 1 volume for Windows and Exchange binaries.
- Place the page file on the system disk, unless paging indicates the need for an additional spindle.
- Create one dedicated fault-tolerant volume per storage group for the transaction logs using RAID 1. It is essential to split store and log files onto separate RAID volumes.
- Create at least one fault-tolerant volume for the databases using RAID 5. If there is one array, place all databases on this array. If there are multiple arrays (preferable), it is appropriate to have one array for the databases of each storage group. Larger volumes will provide for better handling of peak I/O request rates.
- Use hardware RAID controllers.

When determining the storage requirements the following were taken into consideration and the solution based on these criteria.

- When determining the number of disks needed for the information store, it is necessary to calculate how much storage will be required. For example, if each user can have 100 MB of storage, then a 5,000-user system requires approximately 500 GB of storage that can be provided by, for example, 14 18-GB disks or 27 9-GB disks. Also, single-instance storage ratio and deleted items retention factor into the storage calculation.
- The formula for disk sizing is (the number of mailboxes * average mailbox size)*(deleted items retention/single instance storage ratio). However at this stage, due to the lack of empirical evidence regarding single instance ratio, the basic formula of (the number of mailboxes * mailbox size limit) provides the simplest guidance with room for growth.
- Maintenance space, online spares, and space for snapshot technology should also be factored into the overall storage planning. Before selecting an appropriate disk size, ensure that both I/O and disk space requirements will be met.
- Exchange 2000 has the capability of providing a full text index of each database. About 25 to 30 percent of extra disk space should be reserved for indexing stores. For better performance, keep the indexes on separate volumes. In addition, move the server's Temp folder from the paging file disk.
- Volume capacity must accommodate future growth and potential problems. The transaction log files volume should have enough capacity to hold two to three times the normal number of daily transaction log files, in case of a massive increase in transactions due to of message loops, virus attacks, or failure

of the daily backup. Some utilities (such as ESEUTIL or ISINTEG in certain modes) require as much temporary disk space as the largest database because a copy of the database must be saved. Though it is possible to direct these utilities to use a network drive as their temporary work area, this greatly reduces performance.

- **Best practice** . For the disk array that will house databases, start by determining the maximum size of the databases that will be stored on the server. Add 30 percent for full-text indexing (or allocate a separate array). Add a minimum of 25 percent for free space when databases are populated to your expected maximum; if the largest database is bigger than this figure, then use that database size plus 50 percent. The result is the minimum size of the database array. If budget and server capacity permits raise the free-space allocation to 50 percent. It is important to monitor disk utilization on a regular basis to ensure that planned thresholds are not exceeded.

The Raid configurations on the Back-end and Front-end servers were determined based on the following industry standard practices:

- It is recommended that the system volume use RAID 1 technology and that it be reserved for the operating system and Exchange 2000 binary files.
- For ease of management and maximum reliability, each storage group should be placed on a separate volume. Assigning each individual database to a separate volume is an even better setup, if disk configuration allows for it. For optimal performance, disk striping should be used across as many drives as possible, and the volumes should be placed on different disk controllers and different data buses.
- Transaction log files must always be placed on a different volume than the corresponding storage group to increase performance and resilience.
- Exchange 2000 information stores are characterized by the random nature of disk read and write operations, while transaction log files are accessed sequentially, usually for write operations only. The recommended RAID technology for mailbox stores is either RAID 5.
- These settings are best for ordinary operation and not for backup, when data is read from the volumes. However, by using multiple databases and by backing up the databases in a parallel fashion, the backup time can be reduced.
- It is recommended for mailbox servers to have multiple paging files on multiple disks to increase performance, and to use the same settings for **Initial Size** and **Max Size** because it decreases the fragmentation of the paging file.

4.6.2.4 Processor Requirements

Based on the principle that the recommended CPU for Exchange should be the best possible at time of purchase, including at least a 2-MB L2 cache, the hardware was selected. The following standards were also taken into consideration.

For the **Back-end servers**, the requirement for processing power for the server depends on the number of users. Recommended guidelines follow the following

Number of mailboxes	Number of processors
Less than 500	1
Between 500 and 1,000	2
More than 1,000	4

The following were also taken into consideration:

- Note that when determining the number of mailboxes you can have on a server, the important factor is usually not the raw processor capacity. The most important factors are the storage limits and the defined service levels for the maximum time required to perform a backup, recover from a disaster, restore a single database, restore a single mailbox, and restore a single document. Based on this maximum time, you can calculate the maximum database size and the number of mailboxes.
- Service levels and response time are the primary factors to consider for public folder servers. Your requirements depend directly on how your Exchange organization uses public folders.
- Full-text indexing allows clients to search through large amounts of Exchange data and receive quick results. During periods when the search service is crawling and rebuilding, it will place a constant load (initial testing indicated consistent 20 to 40 percent load) on the processor. Because of this, fast or multiple processors are required when turning on full-text indexing. Indexing is not switched on by

default, so user need, processor impact, and off hours scheduling should be evaluated as part of the deployment process in order to determine how to best utilize this service.

For the **Front-end servers**, the recommendation for CPU's is One (1) CPU.

4.6.2.5 Memory Requirements

For **Back-end servers** the following were taken into consideration:

Back-end servers serve many active users at any given time, which places a high requirement for processing power on the server. Server load will vary depending on the activity of the user population. Testing has shown that to operate at peak efficiency, Microsoft Exchange 2000 requires 300 Kilobytes (KB) per user per storage system, plus an additional 128 MB of memory for the operating system environment. Additionally, each storage group requires an additional instance of the Exchange Storage Engine (ESE) and 150-MB virtual memory. This number should be used as a guideline for configuring systems. For example, a 2,000-user system with a single storage group would require 864MB of memory to operate at peak efficiency. If less memory is used, there will be an increase in disk I/O and response time. For memory configurations over 1 GB, you should enable the /3GB switch to the boot.ini file. It is critical that the Store.exe process does not run out of virtual address space (around 2.8 GB). When this happens, memory allocations will fail (even if there is plenty of RAM left), and the information store must be restarted.

The following table lists the recommended memory requirements for a given user population, giving a good margin for growth and high load. If full-text indexing is enabled then 256 MB of RAM should be added.

Number of Mailboxes	Memory Required with 1 storage group
Fewer than 500	512 MB
500 – 1,000	1 GB
1,000 – 4,000	2 GB
More than 4,000	3 GB

For **Front-end servers** the following were taken into consideration:

The recommended memory configuration for computers designated only as protocol front-end servers based on the number of back-end mailboxes that the front-end server is supporting is shown in the following table:

Number of back-end Mailboxes	Memory required
Fewer than 1,000	128 MB
1,000 to 3,000	256 MB
3,000 to 5,000	384 MB

4.6.2.6 Clustering

Note: A server cluster is a group of independent servers running Cluster service and working together as a single unit. Clusters provide high availability, scalability, and manageability for resources and applications by grouping multiple Microsoft Windows 2000 Advanced servers or Microsoft Windows 2000 Datacenter servers into a single administrative unit.

Clustering has been implemented and has many numerous benefits, including:

- **High availability.** With a server cluster, ownership of resources such as disks or IP addresses are automatically transferred from a failed server to the surviving server. The software is restarted on the surviving server, and users experience only a momentary pause in service.
- **Failback.** Windows clustering automatically rebalances the workload to an assigned node when a failed server comes back online.
- **Manageability.** Cluster Administrator can be used to manage a cluster as a single system and to manage applications as if they were running on a single server, even though they are running on separate servers.

4.6.2.7 Mailbox Size Limits

Mailbox limits are important when performing capacity planning to determine how many servers are required. The driving factor in capacity planning is server recovery time. Server recovery time is controlled by the speed with which data can be restored. Data restore times are affected by the hardware solution used and ultimately by the volume of data involved. Thus, in order to plan capacity needs, it is important to start first with service level agreements on how long an outage can last. From that time, deduct the time taken to build a replacement server and use the data restore speed to calculate how much data can be recovered in the time remaining. This calculation provides the total database size for a single server. Note that it is possible to prioritise which users are recovered first by allocating them to particular databases.

The only way to determine accurately how many users can be assigned to a server with a given data capacity is by limiting the maximum size of each mailbox. It is vital to have some kind of limit on mailbox size because storage capacity is a finite resource. Exchange 2000 provides three limits that can be set. These limits apply to a whole information store and can be overridden on a per-user basis.

The three limits are:

- **Warning.** The mailbox size at which users start to receive warning messages.
- **Prohibit send.** Once users hit this limit, they are prevented from sending new mail.
- **Prohibit receive.** Once this limit has been hit, the store will reject any new mail that arrives. It is advisable to set a high value on this to protect against situations where messages bouncing between Exchange 2000 and a foreign mail system cause runaway store growth.

4.6.2.8 Design Decisions

➤ Information Store Size

	Name	RAID	Size (GB)
SG1	EDB1	5	36
	EDB2	5	36
	Logs1	1	18
SG2	EDB3	5	36
	EDB4	5	36
	Logs2	1	18
SG3	PF1	5	72
	Logs	1	18

SG: Storage Group

EDB: E-mail box Store

PF: Personal Folder

➤ Clustering of Mailbox and Public Folder Servers

There are a two-node Active/Passive Cluster for the Back End servers, to host the government institution recipients' Mailboxes and public folders. There is a single Exchange Virtual Server EVS that hosts the Exchange cluster services and user data.

➤ Front-End Servers

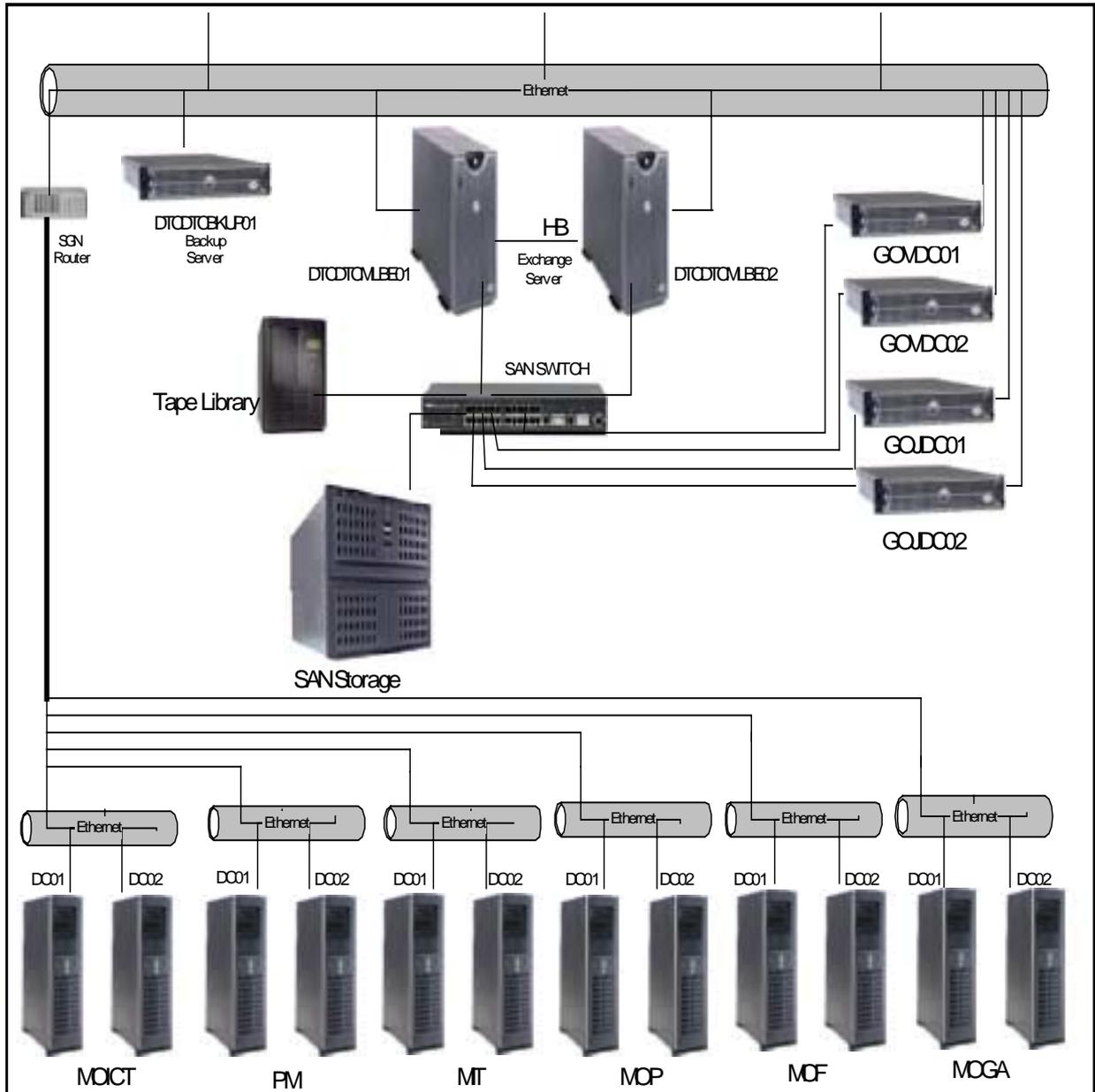
Two Front End servers are configured with Windows 2000 Network Load Balancing. They host the SMTP connector and OWA for the GOJ.

➤ Mailbox Size Limits

The following size limits are implemented:

Warning limit: 45 MB
 Prohibit send limit: 50 MB
 Prohibit receive limit: 100 MB

4.6.3 Technical design implemented



The initial implementation is shown above.

Within the Data Centre, there are two domains, the root domain of the enterprise domain (two servers Primary & Backup GOVDC01 & GOVDC02) this is named .gov. The child domain is goj.gov (two servers GOJDC01 & GOJDC02). Nothing is contained within the root domain, the backend exchange servers are installed within the child domain, also shown on the diagram. The Front exchange servers are not shown as they are installed on a different network separated by firewall, they run the OWA service only.

The actual user mailboxes are contained on the SAN storage, accessed via the backend exchange servers, therefore if one of the servers should fail all users can still access their eMail. Also on this network segment is the backup server and the tape library. Backups are performed daily.

The SGN router is to show the connectivity to all the ministries (note there are leased lines and firewalls not shown). In each ministry there are two servers installed as another child domain. Example mof.gov is the child domain in the Ministry of Finance, two servers one being the primary and the other the backup.

4.7 Training

4.7.1 User Training

The training course that will be provided by the Vendor will cover the following items. The breakdown of the training over a number of days is unknown at this stage.

Getting Started with Outlook 2000:

- Start Microsoft Outlook 2000.
- Navigate in the Outlook Bar.
- Review e-mail messages and attachments.
- Reply to and forward e-mail messages.
- Save e-mail messages and check sent messages.
- Format and print a copy of e-mail messages.
- Customize your Inbox.

Creating and Sending E-mail Messages:

- Compose and send messages.
- Use the address Book.
- Add attachments to messages.
- Mark messages confidential or urgent.
- Retrieve messages sent in error.

Organizing and Managing the Inbox:

- Organize e-mail messages for fast reviewing.
- Set up file folders for organizing e-mail messages.
- Flag e-mail messages for follow-up.
- Create Rules to handle e-mail messages automatically.

Using Internet Explorer for Outlook Web Access:

- Introducing Internet Explorer.
- Using Internet Explorer for Outlook Web Access.
- Handling messages.

Outlook Test.

Handing out Evaluation Sheets so that the students can give feedback on the training received.

Handing out Certificates.

4.7.2 Administrative Training

Two administrators will be trained from each Institution's local IT department to Microsoft MCSA with the following modules:

- Microsoft Windows 2000 Network and Operating System Essentials: (approximately 20 Hours)
- Supporting Microsoft Windows 2000 Professional & Server: (approximately 44 Hours)
- Managing MS Windows 2000 Network Environment: (approximately 52 Hours)
- Implementing and Managing Microsoft Exchange 2000: (approximately 44 Hours)

5. Definition of Organisation & Responsibilities

5.1 Communications and escalation

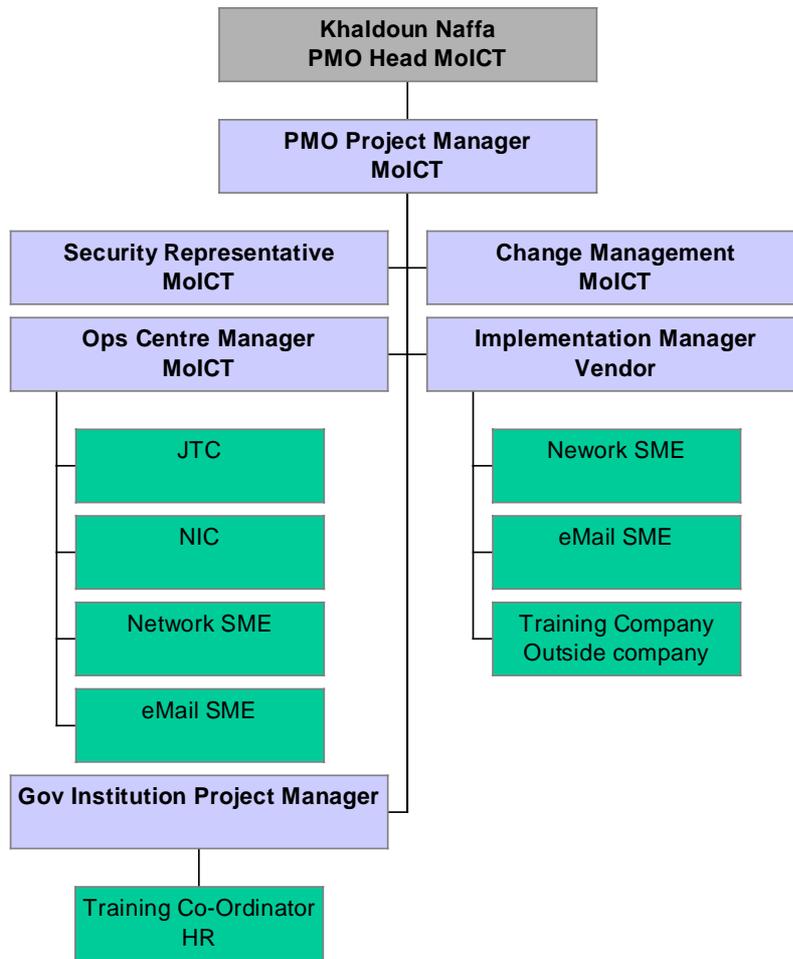


Diagram 5.1 – Communications & Escalations chart

The chart shows the communication paths that will be used. Example the Ops Center Manager will be the main point of contact with JTC, if any other member of the Steering Group contacts JTC; they need to ensure that the Ops Center Manager is fully aware of all communications and involved if possible.

Within the above chart the PMO project Manager represents two different roles. A junior Project manager that will chair the weekly technical meetings and the vendor and government representatives report to this individual. This individual will also attend the bi-weekly steering group meetings and the monthly Operations meeting. The second MoICT project Manager will chair the biweekly meeting. This individual will not attend the weekly meetings but will attend the monthly Operations Meeting.

5.1.1 Technical Weekly Meeting

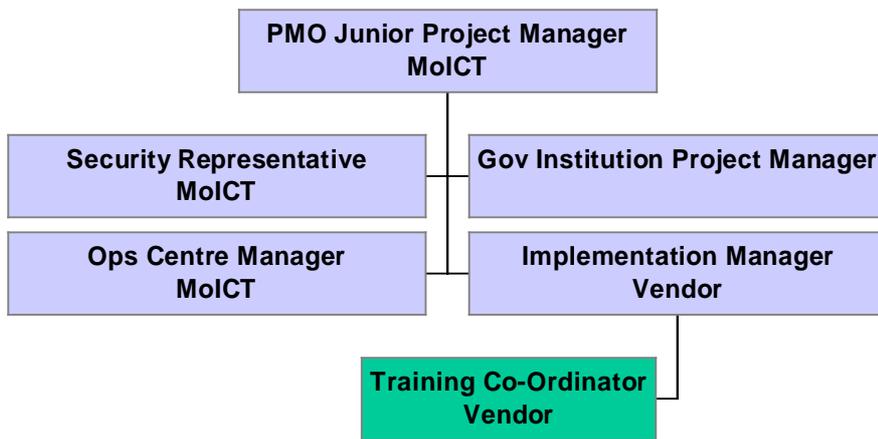


Diagram 5.2 – Technical Committee

The technical committee meets on a weekly basis. The MoICT Junior Project Manager chairs it. The focus of this meeting is to ensure that all parties are aware of what is happening and that the approach taken is as planned, example user communications completed before work commences. All issues are dealt with in this meeting unless escalated.

The following items are covered:

- Technical issues including status of leased lines, purchasing, inventories.
- Training report on training completed
- Training plan for the coming week
- Plan of work for the coming week

5.1.2 Steering Group Bi-Weekly meeting

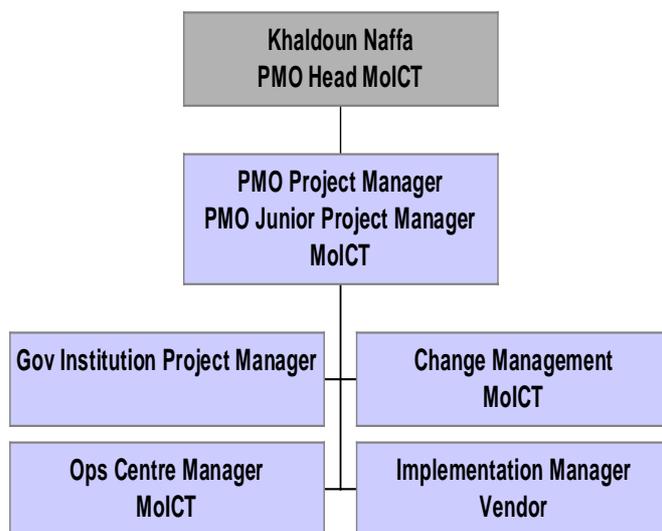


Diagram 5.3 – Steering Group

The Steering Group meeting happens on a bi-weekly basis and is chaired by the PMO Project Manager. This meeting focuses on the project tracking, quality and change control. Issues may be escalated from the weekly meeting here.

The items covered by this meeting will include:

- Updating the project plan
- Project status report
- Local Change Management, example work within the government institution – DHCP configuration
- Quality control

5.1.3 Monthly Operations Meeting

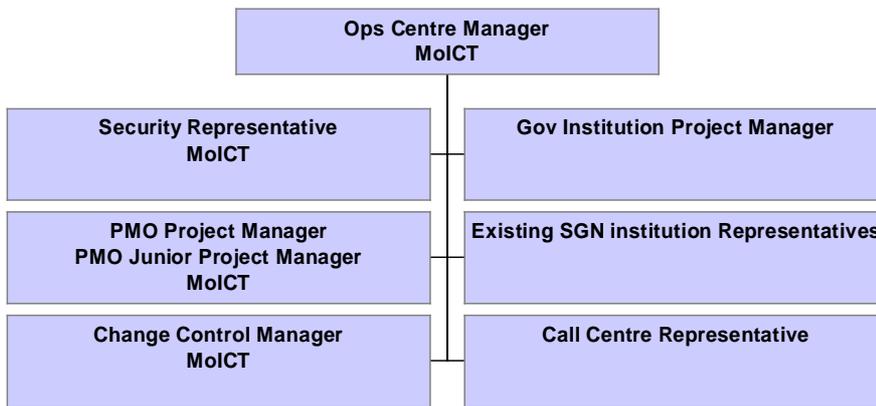


Diagram 5.4 – Operations Members

The monthly Operations meeting are ongoing and outside the project, however global change control must take place here. All changes that can potentially effect the current members of the SGN need to approve changes, for example connecting new institution, creating child domain etc This meeting is chaired by the Operations Centre Manager.

The following items are covered:

- Current status of Operations including details reports from the previous month
- A global Change Control - change that has the potential to affect one of more members of the SGN, for example router configuration updates.
- Operational issues
- Update on current projects being implemented

5.2 Steering Committee Individual Responsibilities

5.2.1 MoICT PMO Head

The MoICT head acts as the main escalation point. Responsible for assuring that the business products are in accordance with current and future business requirements. Responsibilities include:

- Monitors project costs versus business benefits.
- Provides advice on resolution of apparent conflicts.
- May attend steering committee meeting.

5.2.2 MoICT PMO Junior Project Manager

The MoICT Junior Project Manager will chair the weekly technical meetings and be the main point of contact for the vendor implementation manager and institution managers. This individual will deal with all issues initially and will escalate them to the steering committee if necessary and ensure a timely response.

The responsibilities include:

- Daily tracking of all issues
- Ensuring that technical issues are escalated to the relevant authorities and that they are resolved in a timely manner.
- Follows up on decisions made and ensures that they are implemented as agreed. For example actions items from meetings are completed as agreed.
- Maintains the issue log
- Tracking of Training on a weekly basis and associated action items
- Chairs steering technical committee meetings and attends bi weekly steering group meetings and Monthly operations meeting.

Responsible to the MoICT Project Manager

5.2.3 MoICT PMO Project Manager

This individual will be responsible for receiving all deliverables, invoices, and other correspondence produced by the project, and for delivering back all document review comments, variation correspondence, fault reports and other

correspondence. The MoICT Project Manager will have the authority to make decisions on project issues on behalf of E-Government to enable the progress of the project to continue unimpeded. Where a decision has to be made within the E-Government organization at a higher level, the MoICT Project Manager will have the responsibility to seek a timely decision and to convey the decision to the steering committee.

The responsibilities include:

- Ensuring that the focus and direction of the project is in support of current and future e-Government business requirements.
- Responsibility for the acceptance of the products of this project within the defined time scales
- Ensures that each part of the project is complete before the next stage is set in progress, i.e. local LAN in government institution has met all security standards before connecting to the SGN.
- Ensures progress visibility and maintains the project high profile.
- Consolidate reports from team leaders and update project plan on a bi-weekly basis and distribute to the steering group
- Responsible for all-commercial aspects, adherence to Budgets and Time scales, Contract negotiations and sign-off
- Chairs steering Committee Meetings and attends the monthly Operations meeting when necessary.
- Responsible to the PMO Head.

5.2.4 Ops Centre Manager

This individual will be responsible to ensure that the centre can provide all services to the new government institution, this will include all leased lines and ensuring that any hardware required within the Operations Centre for the project is added to the RFP, this would include additional router ports for leased line connectivity and exchange servers if required. The other area of responsibility will be the technical co-ordination of adding new entities to the SGN, ensuring that this is managed through a change control process and adheres to the standards already set and all documentation is updated. Similarly, the co-ordination of the new institution

The responsibilities include:

- Ensures that all additional spurious hardware & software required within the Operations Centre is added to the RFP.
- Responsible for all change control to ensure new institution joins the SGN in a managed fashion.
- Maintains security within the SGN at all times by ensuring that implementation team have limited access to the systems where possible and where full access is required that a separate account be created and that it is disabled when not required as defined within the global change control. Full supervision is also required when the implementation team is working within the Operations centre.
- Ensures that Implementation team has the latest operational documentation for the project, for example standard server build, naming conventions etc.
- Works with the installation team to ensure that the networking equipment is installed within the joining institution as per standards. Perform acceptance tests in association with the implementation team and ensures acceptance criteria are clearly understood.
- Creates the child domain for the new joining institution in a timely manner with the appropriate change control and ensures that the relevant administrator accounts have been created and have the correct access. Provides the details to the implementation team.
- Ensures that the Exchange environment has sufficient specifications for the new users and that the correct configuration is known by the implementation team, i.e. which container contains the mailboxes
- Ensures that all configuration changes are documented and all necessary documentation from the project has been completed and filed within the operations manuals.
- Participates in the bi-weekly Steering Committee Meetings and weekly technical meetings.
- Chairs the Monthly Operational Meeting

Responsible to the MoICT Project Manager

5.2.5 Government Institution Manager

The Institution Project Manager is in overall charge of ensuring that the Local LAN and Desktop environment is fully compliant with the joining requirements. This individual is also responsible for ensuring that all the users are trained in the new eMail functions. This individual needs to work closely with the HR individual in their institution to ensure that this is planned and complies with the project plan.

The responsibilities include

- Participates in Steering Committee Meetings, weekly technical meetings and monthly Operational meetings when required.
- Responsible for ensuring local environment meets joining requirements e.g. that the desktops are all of a minimal specification and have at least W2K installed.
- Ensures that the LAN is fully secured and that there are no external links without verification from the security manager.
- Ensures that all the criteria has been met before implementing the next stages in the project, sign off on completion within the ministry for each stage.
- Working closely with Implementation Manager to ensure that the implementation team always has access to the areas of the institution when required.
- Ensures that all users have been trained in the use and functionality of the new Outlook environment.
- Nominates the two people that will be trained as administrators as part of the project.

Responsible to the MoICT Junior Project Manager

5.2.6 Implementation Manager

The Implementation Manager is responsible for completion

- Day to day management of the SGN project, including supervision of other e-Government project staff.
- Responsibility in ensuring Security Requirements is met.
- Installation of two child domain servers and creating of users and adding all desktops to the domain within all the defined standards.
- Responsibility for liaising with the Email Implementation Manager as necessary to ensure that the project runs as planned.
- Hardware and Software Procurement
- Setting up of meetings to review project deliverables, leading to formal sign off.
- Ensuring that all deliverables conform to project standards with the Ops Centre Manager.
- Participates in Steering Committee Meetings.

Responsible to the MoICT Project Manager

5.2.7 Training manager

Responsible for all aspects of training, this includes email and MS administration. These managers are responsible for the organisation of training courses, attendees and suitability of course materials in conjunction with the government institution Manager.

- Participates in Steering Committee Meetings when required.

Responsible to the Government Institution Project Manager

5.2.8 Quality Manager

Responsible for identification of appropriate project standards, ensuring that they are observed, and to ensure that the standards identified in this Project Initiation documents are complied with. To liaise with Quality Services to establish project specific procedures where required. Holds a quality audit on a monthly basis and where necessary develops corrective action reports.

- Participates in Steering Committee Meetings.

Responsible to the MoICT Project Manager

6. Project Plan

6.1 Project Plan Description

The project plan has been assembled using knowledge gained from previous Network projects, and experience of similar projects. The plan described here is a template that needs to be updated with the relevant information by the vendor Project Manager and the MoICT project manager.

The project plan will be monitored using a PC-based project management tool: Microsoft Project. Progress will be regularly monitored against the project plan and appropriate corrective action taken as described in the PMO Quality Plan. Each month the updated project plan will be included in the monthly progress report by the MoICT.

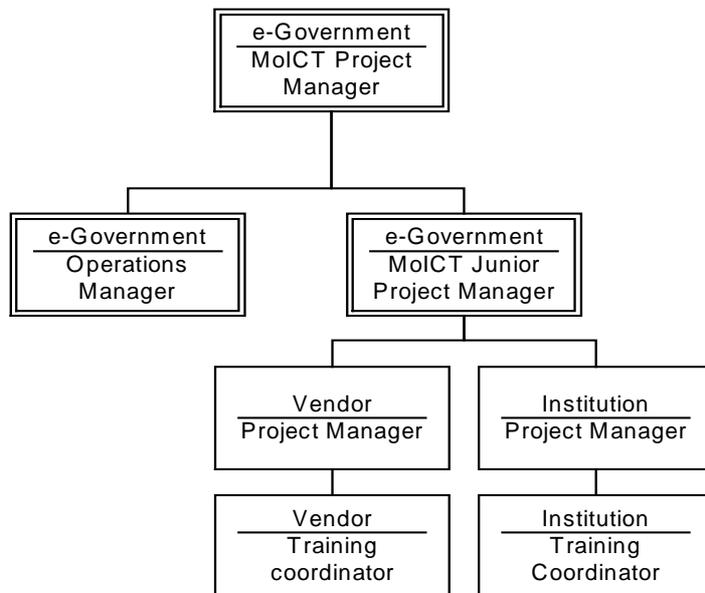
6.2 Project Quality Strategy

The project will follow the appropriate sections of the PMO Quality Plan, with reference to quality control, assurance, planning, document layout and reviewing. Documents will be produced using Microsoft Word for Windows, with tables generated using Microsoft Excel, where appropriate. Regular progress meetings will be held, bi-weekly, as indicated in the previous section.

6.3 Project Escalation

All issues will be escalated to the MoICT Project Manager; the escalation paths are shown below.

Escalation Strategy



6.4 Project Prerequisites

The project takes its starting point from the following:

6.5 Project External Dependencies

The plan and activities described in this document are dependent on the following:

- The provision of the necessary facilities, services, and access to appropriate e-Government staff and vendor for the duration of the project.
- System Support.
- PC and network support.
- Electronic access, and reasonable physical access to the Network where necessary as requested via change control.

- Physical accesses to buildings out of standard office hours for those project team members that require this access.
- Availability of required personal with notice to ensure decisions are made in a timely manner, these include the local institution's IT team and Operations center personnel.

6.6 Project Planning Assumptions

The following assumptions have been made:

- Use of e-Government's system or an equivalent for testing, implementation and demonstrating tasks. Responsive management and control of these resources to expedite the project development.
- e-Government will arrange for structure changes to be reviewed.

6.7 GANTT Chart

The initial version of the project Gantt chart is presented in [Appendix I – Draft Project Plan](#).

Note: The project plan presented here is in draft form, the following list is the outline level 2. Within Institution Project Start and Institution Implementation. All tasks need to be duplicated per Institution. This amendment to the project plan needs to be completed by the MoICT Project Manager initially and then by the Vendor Project Manager

Project Plan-Egov-Draft for Gov institution Joining

- SGN / Email Project
- MoICT Project start
- Institution Project start
- RFP Tender
- Project definition
- Purchasing
- Institution Implementation
- Project Closedown

7. Milestones and Deliverables

7.1 Milestones

The following are the major project milestones:

- MoICT Project Manager assigned
- Project Plan Published
- Project Manager Assigned
- Readiness Assessment completed
- Decision on whether this institution is within the Scope
- Vendor Chosen
- Contract Signoff
- SGN connected via E1
- Network & IP Complete
- Server configuration complete
- Email rollout complete
- User Training complete
- Administrator Training complete
- Call Centre activation date
- Entity accepted by Operations Centre

Note: Some of these milestones will be duplicated, for example SGN Connected via E1, this will need to be duplicated for each government institution joining the SGN

7.2 Deliverable Descriptions

The Project will provide a fully functional secure government network, connecting a number of government institutions to the existing SGN; ensure that full monitoring and maintenance agreements are in place for the new devices and links. Also implement a minimum standard desktop configuration with all users having access to a centralized managed email system. All users should receive appropriate training for the new email environment. Full handover of the new institutions SGN to the Operations Centre and Call Centre with appropriate documentation completed.

Appendix A – Analysis Report

Government Institution _____

From the **User/Desktop Inventory** complete the following:

	Details	Number	Other Comments
A	Total User Desktops		
B	Desktops that meet Hardware Criteria		
C	Desktops that meet Hardware Criteria with working NIC		
D	Desktops to have RAM Upgrade		More details attached
E	Desktops to have RAM Upgrade with working NIC		
F	Desktops that require replacing		
G	Excluding F, Desktops that need an OS upgrade		
H	Existing eMail users		

Note: Items B + D + F must equal A

Note: For the Ram Upgrades, the data regarding those desktops must be extracted from the full inventory and attached. The details are required so that a correct costing can be completed as RAM for different makes and models vary. The required fields are shown below:

Name	Type L/D	Manufacturer / Model	LAN Y/N	Memory	Processor & Speed	HD size	HD Free	Operating System
------	----------	----------------------	---------	--------	-------------------	---------	---------	------------------

From the **eMail Inventory**

I	Number of functional eMail accounts		
J	Number of distributions lists		

From the **Personnel Directory Information** complete the following:

K	Total Number of Users to be created		
----------	-------------------------------------	--	--

Note: It is assumed that this number is the same as the number of eMail users required and students for the outlook training. Please note if this is not the case.

Is there an NT domain to be migrated within the government Institution? _____

Appendix B – Inventory & Questionnaire Signoff (Implementation)



Inventory & Questionnaire Signoff (Vendor & Government Institution)

Signing this document is a statement by both the Vendor and the government Institution that they have agreed that the Inventories and Questionnaires attached are complete and have been validated by the Vendor.

The Inventories and Questionnaires that are attached are:

- User/Desktop
- eMail
- Personal Information
- Institution LAN/WAN/Server Hardware
- Network Diagram
- LAN diagram
- IP allocation details
- Questionnaire for Communications Room and Facilities
- Questionnaire for ISP Service
- Questionnaire for NT Domain

Signoff by Institution and Vendor

Institution's Name: _____

Date: _____

I have read and agree that all documents attached as listed above are accurate and conclusive.

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Appendix C - Signoff of Completion of Client work in Institution



Criteria for client work completed in Institution and handover to local IT

- Anti Virus installed on all Desktop with updates happening on a regular basis
- LAN connected to SGN
- Child Domain servers installed in the ministry (if applicable)
- New Desktops, RAM installations and OS upgrades are completed as detailed in scope.
- All user accounts created with associated mailboxes and personal information updated in user properties.
- All Workstations added to the domain
- Users created and Workstations added to domain are same as scope
- All Workstations checked for correct version of Outlook
- eMail rollout to all users and all users have received Outlook training, details same as scope.
- Administrative accounts have been set-up for all local administrators within Institution and administrative client installed on all relevant administrative workstations.
- 'Jordan e-Government Institution Test Acceptance' has been completed and signoff obtained
- Administrators have received documentation on local administration tasks. These include:
 - ❖ User creation, modify and deletion
 - ❖ eMail account creation, modification and deletion
 - ❖ Locking and unlocking user account
 - ❖ Functional eMail account creation, modification and deletion
 - ❖ Distribution list creation, modification and deletion.
 - ❖ Adding desktop to domain
 - ❖ Installing and configuring client Outlook

Institution's Name: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive.

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Appendix D – Signoff Templates for Institution requiring eMail Migration Criteria for eMail Migration Signoff (Implementation)



Acceptance Criteria for eMail Migration

- Anti Virus installed on all Desktop with updates happening on a regular basis
- LAN connected to SGN
- Child Domain servers installed in the institution (if applicable)
- New Desktops, RAM installations and OS upgrades are completed as detailed in scope.
- All user accounts created with associated mailboxes and personal information updated in user properties.
- All Workstations added to the domain
- Users created and Workstations added to domain are same as scope
- All Workstations checked for correct version of Outlook
- Users notified about the migration
- Critical users list completed and received
- 'Jordan e-Government Institution Test Acceptance' has been completed and signoff obtained
- Plan of action for Migration/Rollout, i.e. no of users/dept per day, ministry has arranged access to the relevant areas completed, agreed between Vendor and Institution and attached to this acceptance.

Institution's Name: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive.

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Signoff of Completion of eMail migration in Institution



Signoff on Completion of eMail migration and Handover to Local IT

- All pre existing eMail users can receive eMail to their old address and have their old eMail messages stored locally on their desktop in a personal folder.
- All Distribution lists have been created as existed with old environment.
- All functional eMail accounts have been created as existed in the old environment and the relevant users have access.
- The old eMail server (or service if server is multi functional) has been decommissioned.
- eMail rollout to all users and all users have received Outlook training, details same as scope.
- Administrative accounts have been set-up for all local administrators within Institution and administrative client installed on all relevant administrative workstations.
- Administrators have received documentation on local administration tasks. These include:
 - ❖ User creation, modify and deletion
 - ❖ eMail account creation, modification and deletion
 - ❖ Locking and unlocking user account
 - ❖ Functional eMail account creation, modification and deletion
 - ❖ Distribution list creation, modification and deletion.
 - ❖ Adding desktop to domain
 - ❖ Installing and configuring client Outlook

Institution's Name: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive.

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Appendix E – Signoff Templates for SGN

Signoff of new Institution link to Operations Centre (Implementation)



Acceptance Criteria for new Institution on SGN

- All network hardware installed in Cabinet in Government institution, with correct cabling and racking completed.
- E1 Link and ISDN line correctly connected to Cisco cabinet within Government institution, example under floor cabling and termination points completed.
- Links have been tested
- Hardware installed in Operations Centre if applicable (this is only necessary if additional card or Router is needed for capacity) to Operations Centre standards, example Router has two power supplies one for each power source, all cabling is completed in a managed fashion.
- New E1 connection cabled through to Router as per acceptable standards example cable management, termination points, labelling.
- Initial configuring required allowing traffic from government institution to Operations Centre and vice versa as per standards, ensuring that Internet traffic disallowed if Internet link exists in institution.
- Backups have been completed for new configurations
- Testing of configuration has been completed
- Documentation has been updated to reflect new link and devices
- Monitoring has been configured and tested for the new links and devices

Institution's Name: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive: From this point the Operations Centre will monitor the new links and devices.

Operations Centre Representative's Name: _____

Operations Centre Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Signoff of new Institution ISP traffic via SGN (Implementation)

Signoff on Migration of Internet traffic via SGN

- Configuration changes made on link for Internet traffic.
- Internet connectivity checked, separate test for each service, services allowed via SGN detailed under
- Any pre-existing security measures are still in place.
- All external ISP links have been removed from the government institution
- All relevant devices moved to DMZ of SGN firewall within institution, example institution's web server
- Institution has contract with NIC (or other ISP provider) for level of service configured via SGN
- Institution's web services are reconfigured with Operations Centre range of published addresses and all functionality has been fully tested via the SGN.
- Institution's DNS service is reconfigured with Operations Centre range of published addresses and all functionality has been fully tested via the SGN.
- All Document changes required are completed
- Backups have been made of new configurations

Institution's Name: _____

ISP Provider: _____

Services Allowed: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive: From this point all Internet Traffic will be router via the SGN. All services allowed via the SGN are listed above.

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Institution's SGN sign off / handover to Operations Centre (Production)
Signoff off on work within Government Institution's Network

- All changes made to Institution's network as per agreed final network diagram
- Institution change over to new IP schema as documented
- Internet traffic router via SGN
- Documentation completed within Operations Centre, Call Centre and Government Institution.
- Operations Centre network engineer approved new network design as being secure and fully implemented
- All External links removed from institutions network
- Acceptance testing completed.
- Call Centre online to receive all cases about new institution's link
- All Administrative accounts used have been deleted or disabled
- The Vendor has completed all network related work within this government institution
- Maintenance contracts within the Operations centre have been updated to cover the new devices and links.
- SLA has been signed between the Government Institution and the Operations Centre

Institution's Name: _____

Date: _____

Government Institution's Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive. The Vendor has completed all project tasks relating to the network within this government institution.

Operations Centre Representative's Name: _____

Operations Centre Representative's Signature: _____

Institution Representative's Name: _____

Institution Representative's Signature: _____

Vendor Representative's Name: _____

Vendor Representative's Signature: _____

Appendix F – IP Scenarios

Assumption we used in this design

In the design we will have two main scenarios, in which all the members of the Jordan e-government ministries and agency will fall under

The format of the Jordan E-Government IP addressing is **10.AAAO0000.SSSSNNN.HHHHHHHH**.

Where, AAA represents the area ID, 8 areas are available

O0000 represents the organization ID (each area will have 32 organizations)

SSSSSS represents the sub organization ID (each organization will have up to 32 sub organizations connected to it)

NNN represents the subnet in each sub organization (each sub organization will have 8 subnets)

HHHHHHHH represents the host within each subnet (up to 254 host per subnet).

First Scenario

The first scenario covers all the members with only on class C network in the network side, and this scenario is the recommended scenario

The format of this scenario IP addressing is **10.AAAO0000.SSSSNNN.HHHHHHHH**.

It is going to be divided as follows:

10.AAAO0000.0.0 -->10.AAAO0000.7.0	Netmask 255.255.248.0	Reserved
10.AAAO0000.8.0 -->10.AAAO0000.15.0	Netmask 255.255.248.0	Main site
10.AAAO0000.16.0 -->10.AAAO0000.23.0	Netmask 255.255.248.0	Reserved for main site
10.AAAO0000.24.0 -->10.AAAO0000.31.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAO0000.32.0 -->10.AAAO0000.39.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAO0000.40.0 -->10.AAAO0000.47.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAO0000.48.0 -->10.AAAO0000.55.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAO0000.56.0 -->10.AAAO0000.63.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAO0000.64.0 --> 10.AAAO0000.127.0	Netmask 255.255.252.0	Reserved for medium sites (16 networks)
10.AAAO0000.128.0 --> 10.AAAO0000.2557.0	Netmask 255.255.254.0	Reserved for small sites (64 networks)

Second Scenario

This scenario covers only the exceptional networks, where the number of users within a LAN is more than one CLASS C. However, it should be highlighted at this stage that such a solution would have issue with scalability and performance, and it should be replaced with a structured setup where L3 switching would play a major role

The format of this scenario IP addressing is **10.AAAO0000.SSSNNHH.HHHHHHHH**. **Only for the main site**

10.AAAO0000.0.0 -->10.AAAO0000.31.0	Netmask 255.255.224.0	Reserved
10.AAAO0000.32.0 -->10.AAAO0000.63.0	Netmask 255.255.224.0	Main site
10.AAAO0000.64.0 --> 10.AAAO0000.127.0	Netmask 255.255.252.0	reserved for Large to medium site (16 networks)
10.AAAO0000.128.0 --> 10.AAAO0000.2557.0	Netmask 255.255.254.0	reserved for small sites (64 networks)

For consistency of the design, all the Organizations will have the same IP scheme, but with a different mask depending on the adopted scenario

Appendix G – Letter of Commitment for User training

يـطـخ رارـقـا

خـيرـاتـلـا: / / مـسـقـلـا/قـرئـادـلـا: مـسـسـؤـمـلـا /قـرـاـزـولـا

قـرـودـب قـول عـتـمـلـا و رارـقـا اذـه يـف قـرـاولا طـورـشـلـاب مـازـتـلـالـا عـلـع _____ انـأ قـفا و ا
يـف _____ عـلـا _____ نـم قـرـتـفـلـا يـف دق عـتـس يـتـلـا _____

طـورـشـلـا:

1. لـو بـقـم رذـعـب الـا بـيـغـتـي الـأ و يـف قـنـق عـنـمـلـا و قـرودلـاب قـول عـتـمـلـا تـارـضـا حـمـلـا قـفـاك روضـحـب بـرـدـتـمـلـا مـزـتـلـي
2. قـيـلـا تـاـءـارـجـالـا ذـا خـتـا مـتـي ؁ اـمـب حـومـسـمـلـا بـا يـغـلـا قـبـسـن زـوا جـت و ا رـر بـم رـي غـلـا بـي غـتـلـا لـا ح يـف
 ■ قـهـجـلـا عـلـا بـا يـغـلـا و روضـحـلـا فـشـك هـب ا قـفـرـم بـرـدـتـمـلـا نـع ا رـيـر قـت بـيـر دـتـلـا زـكـرم لـسـرـي
 بـرـدـتـمـلـا نـع قـلـو يـسـمـلـا
 ■ قـرودلـا روضـح قـدـاشـن نـم بـرـدـتـمـلـا مـر حـي
 ■ قـرـا زـو عـلـا ا مـب قـول عـتـم يـر خـأ مـوسـر و ا فـيـلـا كـت قـيـلـا قـمـك قـرودلـا فـيـلـا كـت عـقـد بـ بـرـدـتـمـلـا مـزـتـلـي
 قـيـن عـمـلـا قـسـسـؤـمـلـا و ا قـرـا زـولـا ر بـع تـا مـول عـمـلـا ا يـجـولـون كـتـو تـالـا صـتـالـا

مـسـالـا: _____

عـيـقـوتـلـا: _____

Appendix H – Naming conventions

Function & Description Listings

Function & Description Listings	Function and Number Abbreviation
Domain Controller	DCO
Front End Exchange Server	FEX
Back End Exchange Server	BEX
Load Balancing Exchange Server	LBX
Cluster Exchange Server	CLX
DHCP Server	DHC
WINS Server	WIN
Web Server	WEB
File and Print Server	FPR
Application Server	APP
Workstation	WS
Router	RTR
Switch	SWT
Firewall	FWL
Site	ST
First server in as many	01
Second server in as many	02
First Workstation in as many	001
Second Workstation in as many	002

Domain Controllers

The naming convention will be based on the domain association and a function with a two (2) digit serial number.

(Domain Name – Function –Serial Number)

So: GOV – DCO - 01 will appear as GOVDCO01.
This would be the first Domain Controller for the root domain in the Operation Centre.

Examples:

Root Domain - First Domain Controller	GOVDCO01
Root Domain - Second Domain Controller	GOVDCO02
Ministry of Finance – First Domain Controller	MOFDCO01
Ministry of Finance – Second Domain Controller	MOFDCO02

Member Servers

The naming convention will be based on the Domain Association and a function Description (3 letters) and a two (2) digit serial number.

(Domain Association - Function –Serial Number)

So: GOJ - FEX - 01 will appear as GOJFEX01
This would be the first Front End Exchange Mail Server under the GOJ domain in the Operation Centre.

Examples:

Operation Centre Exchange Back End Virtual Server	GOJVEX01
Operation Centre Exchange Back End Cluster Server 1 ST Pair	GOJCLX01
Operation Centre Backup Server	GOJBCK01
Any Ministry (e.g. MOICT) First File and Print Server	MOICTFPR01
Any Ministry (e.g. AMM) Third Application Server	AMMAPL03

Workstations

The naming convention will be based on the Domain Association and a function Description (2 letters) and a three (3) digit serial number.

(Domain Association - Function –Serial Number)

Example: MOF - WS - 009 will appear as MOFWS009
This would be the ninth workstation under the MOF domain in the Ministry of Finance.

Active Directory

Logical components

Root Domain Name

This Root domain is to be placed in the Operation Centre.

Root Domain GOV.

Child Domains Names

The Child domain names will reflect the name of the Institution it represents:

Government of Jordan	GOJ.GOV
Prime Ministry	PM.GOV
Ministry of Finance	MOF.GOV

Sites (ST)

Naming convention for the Sites will be based on Location followed by and Underscore and a function (ST) for site, followed by a two (2) digit serial number.

Physical Location _ ST - Serial Number

Operation Centre Site (GOV & GOJ domains)	NIC_ST01
Prime Ministry Site	PM_ST01
Ministry of Finance	MOF_ST01

Site links

Naming convention for the Site Links will be addressed as follows:

Link source point _ Link destination point

Example: A Prime Ministry Link to the Operation Centre appears as: RM_NIC

Organization Units

Organization Units (OU) will be the primary object of representation for Internal Departments within each ministry. The OU names will be reflective of the department they represent. Please refer to the Data collection documents provided by the ministries themselves for further info.

Portal Name

The e-Government Project will be represented on the World Wide Web and thru other Internet services with the Portal Name of:

www.gov.jo

Web Access

Users of the World Wide Web can access it by typing the address: www.gov.jo

Users

Users' accounts will reside in the Active Directory. The users will need a "**Log on**" name to access the domain and resources on the Network. Users will also need a user name account for using the E-mail application on the Network. We unified both names so a user will need to remember and use only one name for the domain log on and e-mail account.

Users Naming Convention

The naming convention will be used in the UPN form; (Universal Principal Names).

User's first name.1st initial of last name @domain.gov.jo

For example, a city of Amman employee with a name of:

Mohammad Abdel-rahman Ibrahim AL-Majali

Would have the following UPN: [mohammad.m @amm.gov.jo](mailto:mohammad.m@amm.gov.jo)

Name rules that apply:

- A person's first name is always used.
- A dot following the first name is always used to separate the first name from the last name letter and not allow for indicating a female name for a male person. For an example, Samir.a without the dot becomes Samira, which is a female name.
- A letter representing the 1st initial of the person's last name is always used.

Duplicate Name recommendations that can be used:

- If multiple identical first name and a last name initial combinations occur, then a second letter is used and then may be as many letters as ministries see appropriate can be used after the dot (.).
- The second and subsequent letters used after the dot are the choice of the administrator in each ministry and don't have to follow a certain rule as long as they differentiate the identical users.
- Any prefix to the last name is always dropped before that last name initial letter is considered. AL-Majali is considered only Majali, so is Al-Khasawneh as Khasawneh and so forth.
- (Abu) is not considered a prefix.
- Any long compound first name will be reduced to the first part of the name. A first name of Mohammad-Ameen will be reduced to Mohammad or Ameen according to the user's request. A first name of Abdel-rahman is not considered compound, however we should drop the dash (-).

Users Log on Name

User Log on name is the same as the User UPN, universal principle name.

Users E-mail Address

User E-mail Account is the same as the User UPN, universal principle name followed by the .JO.
For the same example above:

Mohammad Abdel-rahman Ibrahim AL-Majali

Would have the following e-mail address: [mohammad.m @amm.gov.jo](mailto:mohammad.m@amm.gov.jo)

Special Cases

Some Standard Positions or titles will be allowed for a standard E-mail account. These names will be reserved for these special cases, some of which are:

For the each Ministry :	<i>min @ min.gov.jo</i>
For the “ Minister ”:	<i>minister @ min.gov.jo</i>
For the “ Secretary General ”:	<i>sg@ min.gov.jo</i>
For the “ Mayor ” at Amman City:	<i>mayor @ amm.gov.jo</i>
For the “ Deputy Mayor ” at Amman City:	<i>dmayor @amm.gov.jo</i>
For the “ Under Secretary ” at Amman City:	<i>wakeel @amm.gov.jo</i>

Network Equipment Naming Convention

The following format is used to name the data center network equipment:

Location-Segment Name-equipment-Interface type and number

Where, Location: DC = Data Center

Segment Name:	INT = Internet FE = Front End BE = Back End FO = Fail over SGN = Secure Government segment SS = Service segment
Equipments:	R = Router VPN = VPN 3030 PIX = PIX firewalls IDS = Intrusion detection system SCA = Secure Content Accelerator CON = Content Modules or content switches 650X=613 LAN switch.
Interface:	L0 = Loopback0 FE n=Fast Ethernet Number n GE = Gigabit Ethernet

Appendix I – Draft Project Plan

ID	Milestone	Task_Name	Predecessors	Successors
0	No	Project Plan-Egov-Draft for Gov institution Joining		
1	No	SGN / Email Project		
2	No	MoICT Project start		
3	Yes	MoICT Project Manager assigned		
4	No	Draft Scope completed		5
5	No	Introduction Meeting for all institutions in Draft Scope	4	
6	No	Scope finalised	21	23
7	Yes	Project Plan Published		
8	No	Institution Project start		
9	Yes	Project Manager Assigned		
10	No	Project Plan updated		
11	No	Readiness assesment		
12	No	Client/Desktop Inventory		19
13	No	Personal information Inventory		19
14	No	LAN/WAN/Server Inventory		19
15	No	Network Diagram		19
16	No	IP Inventory		19
17	No	ISP Questionaire		19
18	No	NT Domains		19
19	No	Analysis complete	12,13,14,15,16,17,18	20
20	Yes	Readiness Assesment completed	19	21
21	Yes	Decision on whether this institution is within the Scope	20	6,68,116,69,71,70,73,106,111
22	No	RFP Tender		
23	No	RFP Completed and Published	6	24
24	No	Tender Process	23	25
25	Yes	Vendor Choosen	24	26,28
26	No	Vendor Project Manager Assigned	25	30,71,70,107,112
27	No	Project definition		
28	No	Vendor Contract written	25	29
29	Yes	Contract Signoff	28	
30	No	Steering Group Kick off meeting	26	32
31	No	Institution Defination		
32	No	Vendor verify Analysis Report	30	33,80,83
33	No	List of Hardware/Software to be purchased finalised	32	52,57,62
39	No	Purchasing		
40	No	Ops Centre confirms RFP		42,47
41	No	SGN Cisco Equipment		

42	No	Ordering Process	40	43
43	No	Purchase order completed	42	44
44	No	Delivery & Customs clearance	43	45
45	No	Delivery of goods to Site	44	87
46	No	JTC Leased E1 Line & ISDN Backup		
47	No	Ordering Process	40	48
48	No	Purchase order completed	47	49
49	No	E1's Installed	48	50,88
50	No	ISDN Links installed	49	90
51	No	Active Directory Servers & Desktops		
52	No	Ordering Process	33	53
53	No	Purchase order completed	52	54
54	No	Delivery & Customs clearance	53	55
55	No	Delivery of goods to Site	54	77,94
56	No	RAM		
57	No	Ordering Process	33	58
58	No	Purchase order completed	57	59
59	No	Delivery & Customs clearance	58	60
60	No	Delivery of goods to Site	59	76
61	Yes	Software		
62	No	Ordering Process	33	63
63	No	Purchase order completed	62	64
64	No	Delivery & Customs clearance	63	65
65	No	Delivery of goods to Site	64	
66	No	Institution Implementation		
67	No	Operations Centre		
68	No	SLA between institution and Operations Centre signed	21	
69	No	Latest relevant Documentation supplied to joining entity	21	79,84,85,87
70	No	eMail settings supplied to vendor	21,26	100
71	No	Child domain created and administrator account details given to vendor	21,26	95
72	No	Monitoring configured for new institution	89,90	92,120
73	No	Ops Centre Documentation updated to include institution	21	120
74	No	Desktop		
75	No	Client Desktop OS Upgrade		81
76	No	Client Desktop Memory Upgrades	60	81
77	No	Client Desktop	55	81

		Replacements		
78	No	DHCP configured on Clients	84	86
79	No	AntiVirus configured on all Desktops	85,69	81
80	No	New Login Names & email address list	32	99,101
81	No	All Desktops upgraded	75,76,77,79	
82	No	Network		
83	No	New IP Plan and Network Diagram completed	32	84,86
84	No	DHCP Server Installed	83,69	78
85	No	AntiVirus distribution Server installed	69	79
86	No	IP Rollout	78,83	92,89
87	No	New Network Hardware Installed and configured	45,69	
88	No	E1 Link installed and tested	49	92,89
89	Yes	SGN connected via E1	88,86	95,91,72
90	No	ISDN connectivity configured and tested	50	72
91	No	ISP Routed via SGN	89	92
92	Yes	Network & IP Complete	88,86,91,72	118
93	No	Active Directory		
94	No	Server Hardware Installation In Comms Room	55	95
95	No	Child Domain Installed	94,89,71	96,97,99
96	No	DHCP and Anti Virus Configured correctly	95	97
97	Yes	Server configuration complete	96,95	98
98	No	Desktops Added to new domain	97	
99	No	All User accounts/mailboxes created	80,95	100,102
100	No	Email Rollout to clients	99,70	103
101	No	All functional mailboxes and distribution lists created	80	103
102	No	Acceptance testing complete by local IT team	99	103
103	Yes	Email rollout complete	100,102,101	118
104	No	Training		
105	No	User Training		
106	No	HR Training Manager assigned	21	107
107	No	Training plan completed	106,26	108
108	No	Training	107	109
109	Yes	User Training complete	108	
110	No	Administrator Training		
111	No	Staff to be trained nominated	21	

112	No	Training plan completed	26	113
113	No	Training	112	114
114	Yes	Administrator Training complete	113	
115	No	Call Centre		
116	No	Initial meeting with Call Centre	21	117
117	No	Information required by Call centre complete	116	118
118	Yes	Call Centre activation date	117,92,103	120
119	No	Entity Signoff		
120	No	Entity closedown checklist complete & Handover	118,73,72	123
121	Yes	Entity accepted by Operations Centre		
122	No	Project Closedown		
123	No	Closedown meeting	120	