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

Funded By U.S. Agency for International Development

Jordan e-Government Project

Request for Proposal

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

0.1 Document History

Version	Status	Reviewed/Approved by	Date

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 Needs reference GOJ.CONS.ANLS.028.1.0	

0.6 Abbreviations

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

1. Important Notices

1.1 Confidentiality

This Request For Proposal (RFP) and any related documents, information and discussions are to remain strictly confidential and must not be communicated to anyone in your organisation, not directly involved in the preparation of your proposal.

Further, you are requested not to inform any third party not involved in the issuing of the offer of the fact that MoICT has requested an offer and/or to pass on any information issued by MoICT in that connection.

The information provided by you shall also be handled as confidential within the MoICT organisation, whereby MoICT shall retain the right to pass on said information to relevant persons within the Government of Jordan or third party advisors, without informing the supplier hereof.

1.2 Joint Bids

MoICT is seeking a single service provider to lead the work. You may bid in conjunction with others but one organisation must act as prime contractor.

If you sub-contract any portion of the work, you must provide full details of the sub-contractor and the work that the sub-contractor will carry out.

1.3 Tender Conditions

In issuing the RFP, there is no implied obligation for MoICT to procure any of the services being reviewed.

Any statement made by service providers in their proposals concerning equipment, software, performance, services, personnel and costs will be considered to form part of any contract which may be entered into in the event that MoICT places an order with your firm.

The service provider should work on the basis of being appointed with responsibility for the success of the project overall. Any limitations of responsibility that service providers wish to negotiate should be clearly stated.

Service providers should respond on the basis that this is a fixed price contract. Where possible, prices should be given for all the hardware, software, consultancy, ancillary items and on-going support necessary to meet MoICT's requirements.

Service providers should state the length of time for which the prices quoted are valid but the offer should be valid for a minimum of 90 days following the date of receipt by MoICT.

This RFP is issued on the understanding that service providers will not charge for making their proposals, or for arranging and conducting reference site visits and demonstrations.

Service providers must be prepared to:

- Answer any ad-hoc questions on their proposal and provide additional information, when requested;
- Make formal presentations of their proposal;
- Nominate relevant reference sites for MoICT staff to visit.

The prices indicated must appear in JD, including VAT. This price information must as far as possible be specified for each functional section of the offer. If additional assumptions have been made in assessing the prices, such assumptions must be explicitly indicated. Price rises within the period of validity of the offer shall not be permitted.

Should MoICT accept your offer, it shall form part of the contractual agreement to be drawn up. Contracts will be subject to the laws of Jordan.

1.4 Communication

All questions relating to this RFP must be submitted in writing or via e-mail to the specified contact in MoICT. Full contact details are in Appendix A.

Contact by a service provider with anyone else employed by MoICT may be grounds for rejection.

1.5 Negotiation

MoICT reserves the right to negotiate with the service provider in response to this solicitation.

All proposals are subject to the provisions contained in this contract. Any other terms or conditions by the service provider, whether inadvertent or intentional, will have no force or effect.

1.6 Additions/Deletions to Qualified Proposal

The intent of this RFP is to establish an initial scope. MoICT recognizes that this scope may change in the initial stage of the project. The proposal should be completed in a way that allows these numbers to change; a minimum scope number can be specified within the vendor proposal.

2. Executive Summary

2.1 Change Programme

This Project continues with the initiative that established an integrated Secure Government Network (SGN) and electronic mail system for secure Government-to-Government (G2G) communication.

This Request For Proposal (RFP) relates primarily to a specific number of Institution (details in Appendix B) that will join the SGN and eMail initiative.

Section 3 of this RFP provides overview of requirements and format of response.

Section 4 of this RFP details the current status of the eGovernment initiative and the existing technical standards that need to be adhered to.

Section 5 of this RFP Details the scope of work that the vendor needs to complete.

2.2 IT Architecture

The IT Architecture of the SGN and eMail initiative is already defined. This project is defined within this existing architecture. Further details are in Section 4

2.3 Approach

MoICT is looking to partner with a suitably qualified service provider that can support it through the IT-related elements, purchasing, implementation, testing and handover, user and administrator training in this phase of the Government's SGN and eMail initiative.

The service providers to whom this RFP has been issued must respond to all requirement areas of this RFP.

Section 5 of this RFP describes the selection process that will be followed by MoICT in choosing that preferred service provider.

The critical objectives that MoICT are seeking to achieve in partnering with a service provider are as follows:

- A single outsourcing relationship
- Proven track record in similar projects
- Competitively priced proposal

2.4 Requirements

MoICT requires services in the following main areas:

- **Validation of institution's inventories**, it is important that the vendor meets with the institution and confirms that the inventories are complete and accurate. This allows the vendor to get a view of the work required and take ownership of the scope.
- **Infrastructure Acquisition & Installation**, The vendor is responsible for purchasing, installing and configuring the networking devices, servers, software and desktop equipment as defined in the scope.
- **IT Implementation**, where the chosen service provider will provide project management and systems integration support in conjunction with the Operations Centre in the implementation of the SGN.
- **Transition**, where the service provider will ensure the ease of transition of support to the Call Centre and the Operations Centre, providing the necessary support and documentation.
- **User Training,** ensuring that all the new outlook users will be fully trained in a timely manner, for example within four weeks of having their email client configured.
- **Local Administrator training with the Institution**, providing Microsoft Certified administrator training to 2 administrators within each institution, also providing overviews for the whole IT department detailing the impact of the initiative, an overview of the SGN and eMail infrastructure, overview of the administrative responsibilities.

3. Introduction

3.1 Purpose of This RFP

The purpose of this Request For Proposal (RFP) is to elicit responses from qualified service providers to partner with the Government of Jordan via MoICT in order to provide support in the following areas:

- Scope Validation
- Purchasing of Network devices, Leased lines, Servers, Software, Desktops and RAM
- Desktop Standardization
- Active Directory
- eMail
- SGN connectivity
- IP standardization
- Network security
- User training
- Administrative training

Details of the above areas are contained within this document, a brief summary is provided here below.

3.2 Summary of Requirements

All work to be completed by the successful vendor will be project managed by the vendor and the vendor will coordinate work with the relevant personnel. The vendor will also be responsible for ensuring that appropriate change control requests have been processed by the operations centre manager prior to completing any work that may effect existing services to the users or existing government institutions on the SGN.

3.2.1 Scope Validation

The scopes detailed within this document are provided by each institution's IT group. The first task of the successful Vendor is to validate this with the cooperation of each institution. This is to ensure that no assumptions have been made by any party, the vendor has a full picture of the scope of work and the details for purchasing equipment are correct.

3.2.2 Purchasing

Purchasing will cover the following for each institution:

- Two servers to be the domain controllers within the institution for the child domain
- Cisco devices to allow the institution to join the SGN and a cabinet to house all communications equipment provided under this project
- RAM upgrades for Desktops based on the inventory verified by the winner.
- New Desktops to replace those with insufficient specifications
- E1 Link and ISDN backup line
- User Outlook Training for all users within the institutions
- Administrative Training for 2 Administrators.

Additional Purchasing may be required to ensure that the Operations Centre has the required hardware and software to support the new joining institutions; details of any requirements are contained in Appendix C

3.2.3 Desktop Standardisation

The successful vendor will be responsible for completing the following within each institution:

- Ensure all desktops have a minimal OS of W2K installed with Office 2000 including the full Outlook Client.
- Ensure that desktops defined within the scope to have RAM upgraded is completed
- Replacement desktops are installed as defined within the scope.
- All desktops are joined to the new child domain
- eMail is configured on each users desktop using the full outlook client, any migration of email is also the responsibility of the vendor who ensure that an archive is available of each users old emails
- Anti Virus software is configured on each desktop and device attached to the institution's LAN.

3.2.4 Active Directory

Within each institution two servers will be build as domain controllers of a new child domain that is utilised only within that government institution. The Operations Centre will provide the standards used. All users will be defined within this domain and their personal information entered within the user details for publication with the enterprise directory.

3.2.5 EMail Rollout

The objective is that all users within the joining institutions will have an eMail account on the centralized system and the primary means of access will be via the full Outlook client. Where an eMail system existed prior to this project, the vendor will migrate the users with minimal disruption to their work.

3.2.6 SGN Connectivity

Installation of the new networking devices within the local government institution in a secured manner and configuration of the link to the appropriate standards, details of all standards will be provided by the Operations Centre. The vendor in conjunction with the Operations Centre will also complete configuration of the monitoring of the links and hardware devices.

3.2.7 IP Standardisation

Within each government institution, it is necessary to rollout a new IP structure in line with the standards defined. There are a number of scenarios already drawn up and where possible should be utilized but in the event that the requirements of the joining institution cannot be met by these scenarios, the vendor is responsible in con junction with the local IT group for drawing up a new scenario to meet these requirements and provide the updated documentation to the Operations Centre. The vendor will also implement this solution in conjunction with the local IT group.

3.2.8 Network Security

A detailed drawing exists for the current network within the institution, the vendor will verify this and in conjunction with the local IT group draw a revised network implementing a basic level of security as defined as standard within the SGN. The Operations Centre will review this prior to implementation and the vendor with the local IT group will implement.

The network design will include but is not limited to the following:

- ➢ All Internet traffic router via the SGN
- ➢ All web servers; firewalls or proxies will be placed on the DMZ of the SGN firewall
- ➢ All external links to the local LAN will be secured on a DMZ.

3.2.9 User Training

User training will be provided to all users within all the joining institutions. If required training will be divided into classes of similar students, the three main grouping being basic, advanced and VIP. (Basic and advanced classes are defined so that students with a similar background and understanding can be placed together) The institutions may request other groupings. Coordination of the training will be between the training coordinator within each institution and the vendor.

3.2.10 Administrative Training

Two administrators within each institution will be trained to MCSA level. The vendor will complete the coordination and scheduling.

3.3 Format of Response

3.3.1 General Format

Your response to this RFP should follow the following format:

- Executive Summary
- Company Profile
- Pricing Proposal
- Appendices and Attachments

3.3.2 Executive Summary

Brief summary that cites main points of your proposal.

3.3.3 Company Profile

In this section you should profile your company's capabilities in similar projects (and IT project management). You should provide details of similar projects, particularly in Jordan. In particular, the service provider should specify three references and contact names of clients who have undertaken similar arrangements with the service provider. These references may be contacted. MoICT will notify the service provider in advance before initiating contact with these references.

3.3.4 Pricing Proposal

Pricing proposal should be fixed price, however due to the nature of the scope, itemization for the following is a requirement.

- Replacement desktops
- Upgrade of client desktop (A minimum number can be specified)
- User rollouts, include desktop configuration and mailbox rollout (A minimum number can be specified)
- User Outlook training (A minimum number can be specified)

As much as possible the pricing should be broken down.

3.3.5 Appendices and Attachments

In the appendices, you should supply a sample of the standard contractual arrangements that you have put in place for similar IT projects. You should also include CVs for the staff that you propose for the work

4. Background of eGovernment Initiative

4.1 Overview

In support of the Government of Jordan's move towards becoming an electronic Government there is an agreed strategy to provide a corporate directory and an enterprise messaging service. These services will be made available to all registered Government employees and applications. They will be used as the source of business information as well as the primary method of communication and workflow within the government.

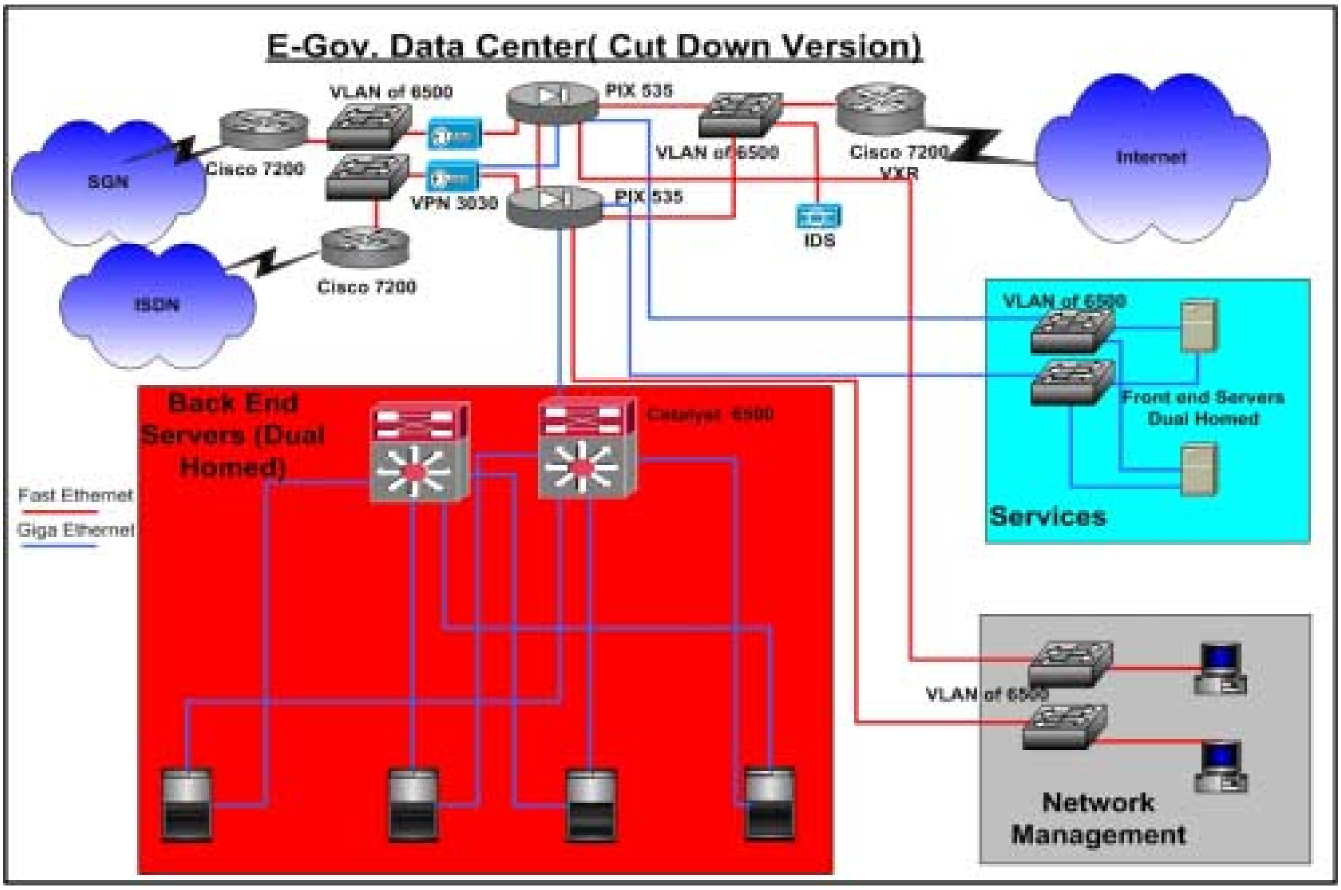
These services will allow the Government of Jordan to host multiple organizations on a shared hardware platform. MDS services can be offered in a scalable, reliable, fast and feature rich environment. Optimally these services have the potential to reduce the total cost of ownership for electronic communications and information flow. For example, one common MDS infrastructure may drive down the total cost of ownership by standardizing hardware, software, administration, maintenance, user interface and training.

4.2 Current membership of the initiative

Appendix D details the government institutions that have already joined the SGN and the number of eMail clients completed in each.

4.3 Current SGN Design

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.



4.3.1 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,

4.3.2 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.

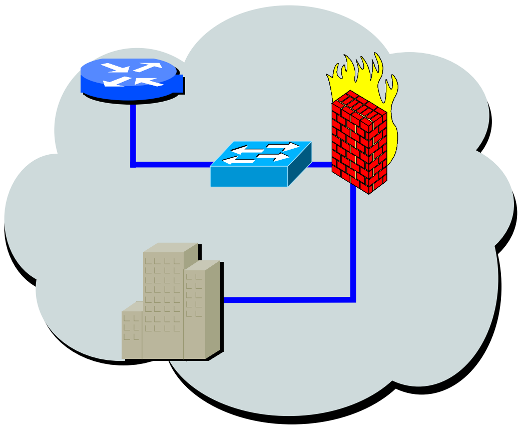
4.3.3 Connecting to the SGN

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.

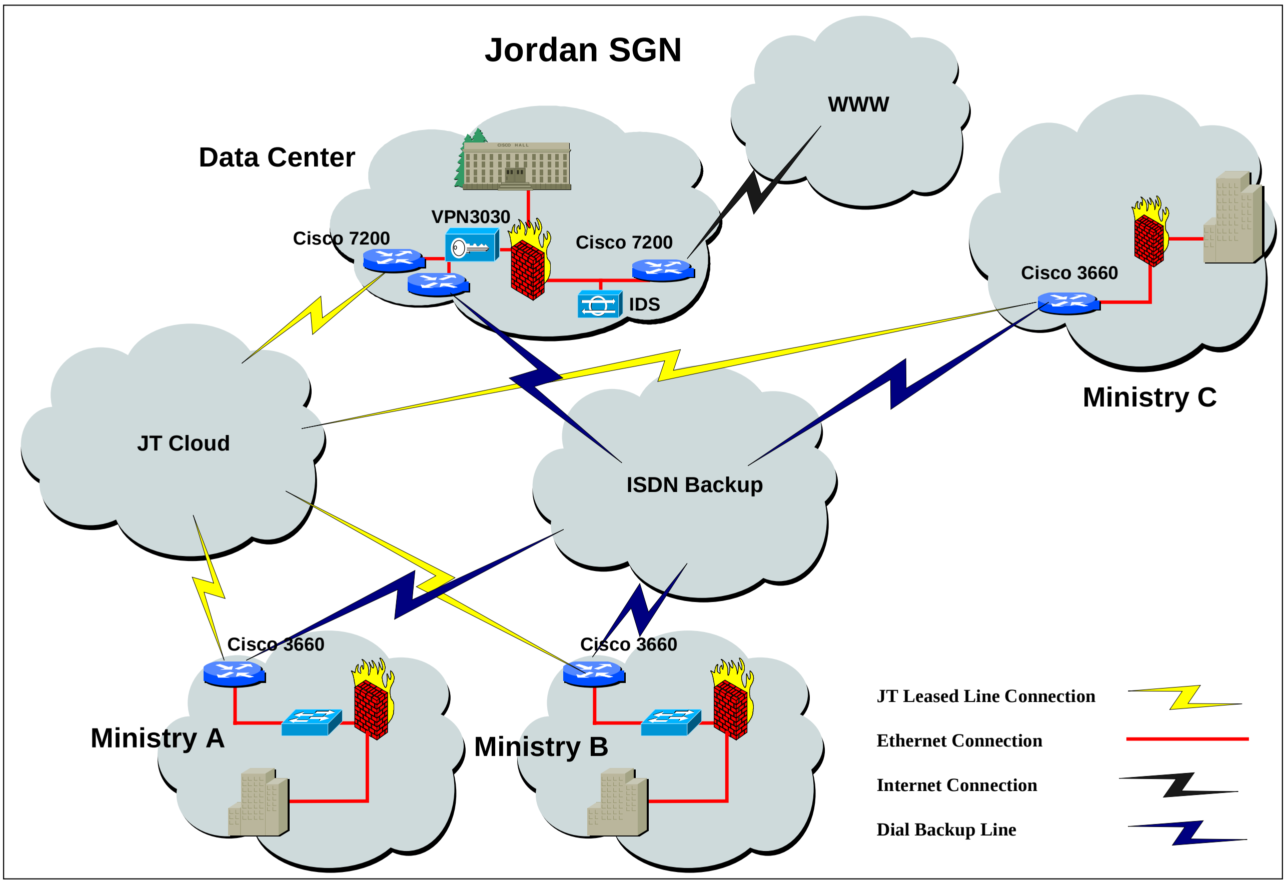
Each Institution will be required to have the following minimum configuration:

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.



4.4 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 E – 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

4.5 Enterprise Directory & eMail Design

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'.

4.5.1 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:

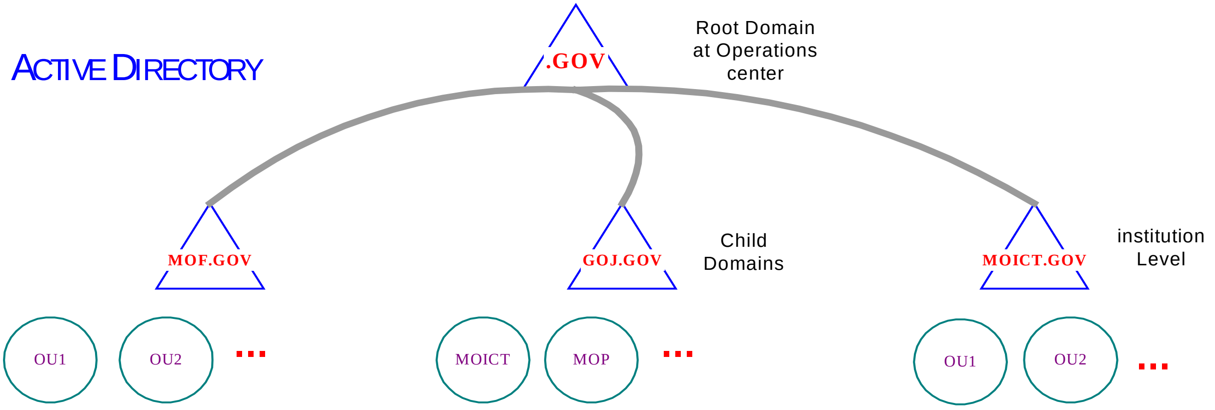


Figure – Domain structure

4.5.2 Technical design implemented

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 server 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.

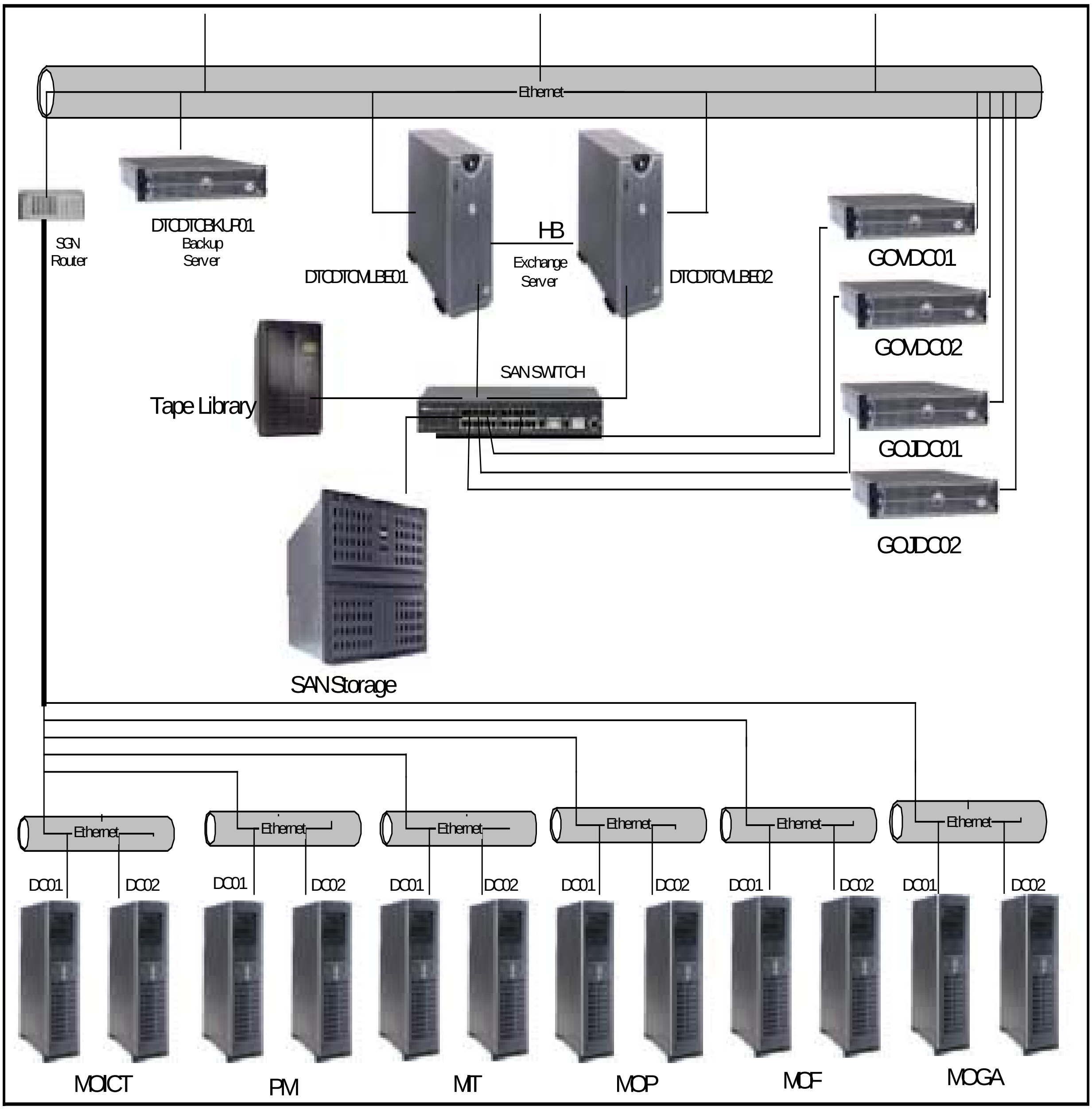


Figure - Initial implementation

4.5.3 Administration

4.5.3.1 Government of Jordan Child Domain

A Child Domain named **GOJ.GOV** (Government of Jordan) with a NetBIOS name of **GOJ** will be created in the Operations Centre site.

For fault tolerance, two Domain controllers will be created in this Domain**; GOJDC01** and **GOJDC02.** Each Domain controller will have ***DNS*** service with Active Directory Integrated Zones.

This Child Domain will have its own authoritative DNS server and its own-delegated zone.
GOJDC01 will point to itself as the preferred DNS server and to **GOJDC02** as the alternate DNS server.
GOJDC02 will Point to its self as the preferred DNS server and to **GOJDC01** as the alternate DNS server.

GOJDC01 will be a global catalogue server (GC). It will also host the PDC Emulator, RID master, and Infrastructure master for the Child Domain.

The Storage Location for **GOJDC01** and **GOJDC02** Active Directory database will be hosted on one RAID5 Group on the SAN Storage, and the LOG files will be hosted on a RAID1 Group.

4.5.3.2 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 F – Naming Conventions

4.6 Documentation

Currently all aspects of the configuration is documented, this library is owned by the Operations Centre. As part of the implementation the vendor is required to update the relevant documentation. Appendix L details the current library; the documents to be updated or created are not limited by this listing. It is the responsibility of the vendor to ensure that all documentation is current at the completion of this project.

4.7 Operations Centre & Call Centre

The SGN and eMail initiative is fully supported by a call centre and the operations centre.

4.7.1 Call Centre

All institutions connected to the SGN and using the eMail service use the Call Centre to report all issues. The Call Center endeavours to solve the case initially and obtains details of the issue. If escalation is required the case is passed to the operations centre, the call centre still maintains the case and follows up with the users and the operations centre on a regular basis until a satisfactory result has been obtained.

4.7.2 Operation Centre

The Operations centre maintains the current infrastructure and is the second line of support on issues. The staff completes the daily tasks, implement configuration changes, perform routine security audits and

Within the Operations centre the hardware and links are monitored on a 24hour basis with SMS messaging outside office hours. The support staff work on an on call basis to provide maximum service to the end users.

4.8 Project Assumptions

- All standards implemented to date will be adhered to within the new project; strict change control will be used if any of the current standards are to be changed. The Operations Centre will ensure that this is the case and will work with the vendor providing all required information.
- All Government institutions will have their network security analyzed to ensure that security on the SGN will not be compromised and whatever changes are required will be implemented prior to the institution being connected to the SGN.
- No user desktops will exist on the local network that does not meet the minimum standard configuration.
- All users will receive Outlook training and a mailbox configured within the new system.
- All ISP connectivity will be via the SGN; no external links will exist in any of the joined institutions.
- Work that may have a major impact on the users will be scheduled at a time of minimum disruption. This work may need to be completed out of working hours in the evening, during the night, or at the weekend. The vendor will agree the working times with the steering group and the local IT group where work will have a major impact on the users, for example IP migration to new schema, conversion of ISP connectivity etc.

5. Scope of work for this Phase of the eGovernment SGN & eMail initiative

5.1 Project Management

The vendor will appoint a project manager who will be a single point of contact for all aspects of the project for MoICT and the Operations Center. The project Manger will be responsible for timely updates/reports, updated project plan and continuous feedback to the MoICT, communication and resolution of issues. The following details the communications and escalation strategy that will be used during the project; the vendor project manager will attend the relevant meetings and will ensure that information is communicated in a timely and efficient fashion to all parties.

5.1.1 Communications and escalation

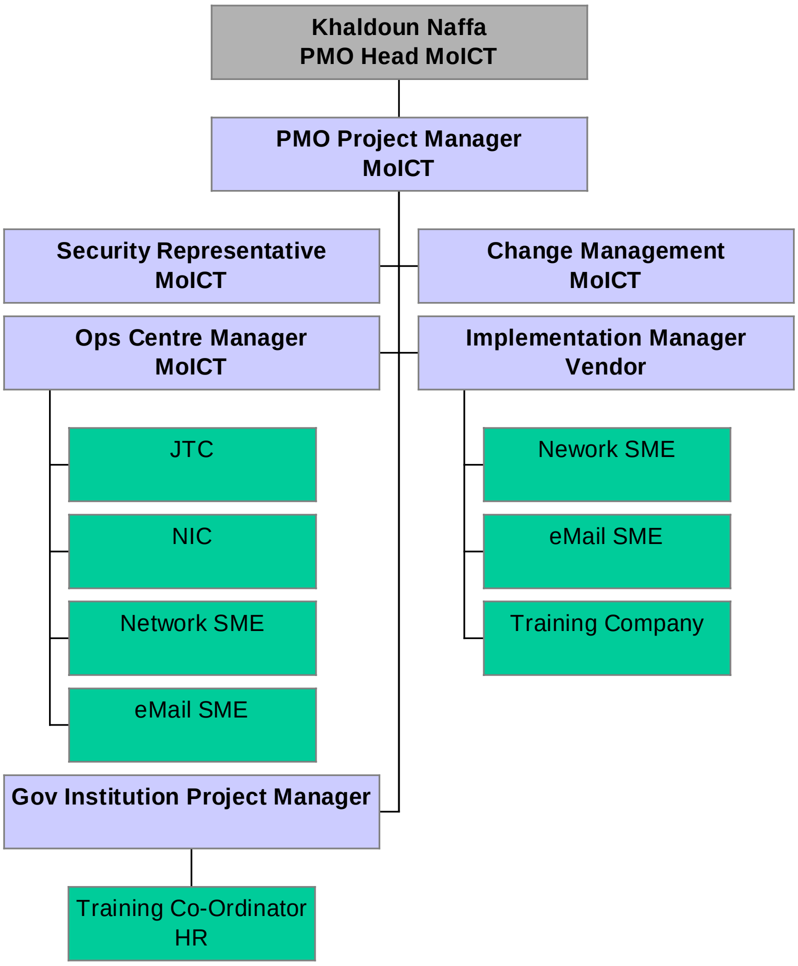


Diagram 5.1 – Communications & Escalations chart

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.

5.1.1.1 Technical Weekly Meeting

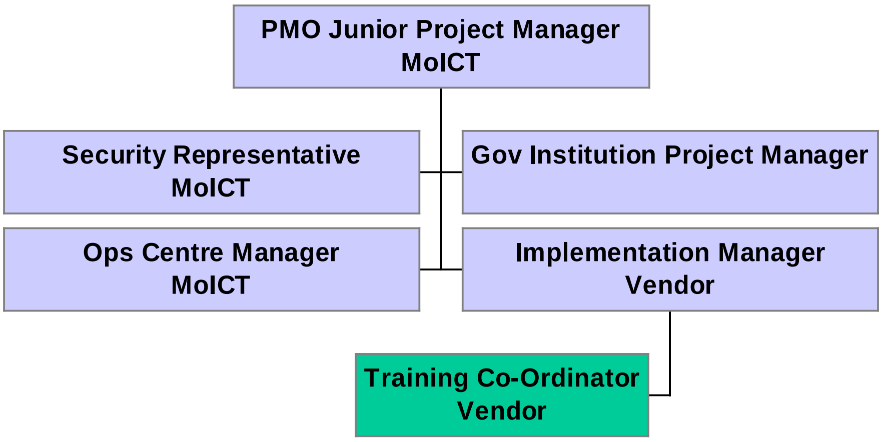


Diagram 5.2 – Technical Committee

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

5.1.1.2 Steering Group Bi-Weekly meeting

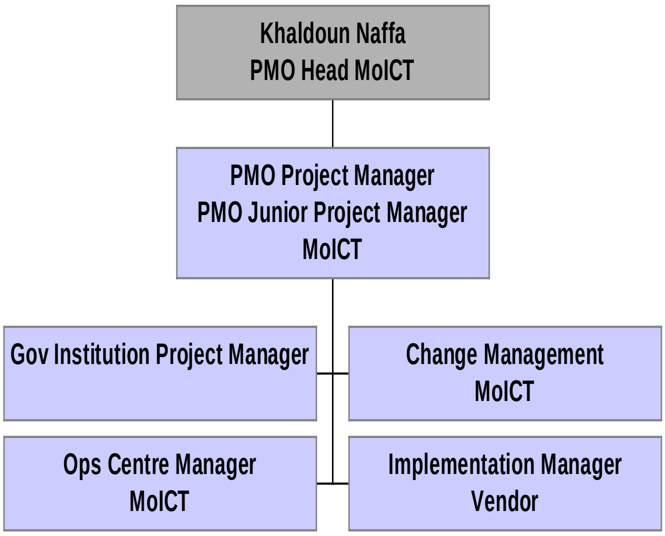


Diagram 5.3 – Steering Group

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

5.1.1.3 Monthly Operations Meeting

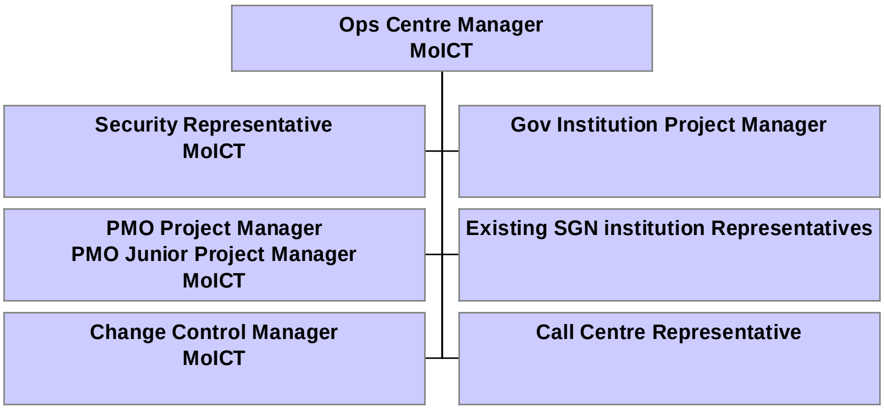

Ops Centre Manager
MoICT
Security Representative
MoICT
Gov Institution Project Manager
PMO Project Manager
PMO Junior Project Manager
MoICT
Existing SGN institution Representatives
Change Control Manager
MoICT
Call Centre Representative

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 affect 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 SGN

5.2.1 Purchasing

5.2.1.1 Hardware

For each joining institutions the hardware specified in Appendix G needs to be purchased. Hardware requirements for the Operations centre are detailed in Appendix C if required. For all hardware and software purchased full maintenance contracts are also required.

The successful vendor will be responsible for completing the purchasing of the above hardware including customs duty documents and delivery to the relevant sites.

Note: During implementation the successful vendor will work with the Operations Centre manager to ensure that maintenance contract match existing contracts where possible.

5.2.1.2 Links

For each joining institution, an E1 link and ISDN line is also required from JTC to connect from the joining institution to the Operations Centre. The successful vendor will coordinate the installation of these links with JTC, the Operations Centre and the joining institution.

Details of the specific links that will be provided by JTC are detailed in Appendix H

5.2.2 Installation

5.2.2.1 Hardware

The successful vendor will install the cabinet in the local institution, ensuring that the cabinet is located in an appropriate position (adheres to industry standards, for example that it is easily accessible and not placed beside in appropriate equipment). That appropriate power and ventilation are available (adheres to industry standards). That the cabling and mounting of equipment within the cabinet are completed in a professional manner and adhere to industry standards for example all cable labeled and secured, ease of access to individual components without disturbing other devices within the cabinet.

5.2.2.2 Links

The installation of the JTC links will be the running of JTC cables up to the ministry buildings. The Vendor will be responsible for implementing any links required at the joining government institution from JTC termination points to the communications room where the networking equipment will be housed. If termination points are required within the communications room these need to be provided and installed by the vendor. 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.

Within the Operations center, the vendor will coordinate the connectivity of the new links with the Operations center utilizing change control for all access to the production environment. The vendor will label and document the new links to the standards already in use by the operations center.

5.2.3 Implementation

The Vendor’s installation team will complete the SGN installation, however coordination with the Operations Centre Manager is necessary 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 vendor will ensure that change control approval has always been received prior to completing any work within the production environment including physical connections.

At all stages during the implementation, the vendor will ensure that the configuration on the links is secure and only allows the relevant traffic. When it is required to open the configuration on the link for testing or implementation, it should only happen within the change control environment.

The Operations Centre will provide administrative accounts and details of the standard configurations required that the vendor will use on existing devices. These administrative accounts are only operational within the change control periods.

Change control process is included in Appendix I

The Configuration to be completed by the vendors includes but is not limited to the following:

- All configuration on network devices within the local institution
- Configuration including VPN on the link between the institution and the operations center
- Automatic fail over configured on all devices
- Monitoring setup for all links and hardware devices
- Documentation of the implementation

Note: For each of the above, the vendor with work in conjunction with the Operations Centre to ensure that the current standards are implemented. Details of existing standards are documented within the Operations Centre, list of documents are found in Appendix L.

5.2.4 Testing

The Vendor will complete testing at each stage of the implementation and will receive signoff from the local institution and the Operations Centre which ever is appropriate before proceeding to the next stage.

5.2.5 Handover

The Vendor will complete the handover of support to the Call Centre and the Operations Centre and receive signoff.

5.3 Desktop Standardization

5.3.1 Purchasing

Attached in Appendix J are the Analysis reports from each government institution

From these reports the vendor is required to complete purchasing for the following items

- RAM (details attached in the analysis report)
- Replacement Desktops – Specifications attached in Appendix K – Desktop Specifications

Note: The vendor will be required to validate these figures with each institution prior to commencing purchasing. For this reason it is requested that the response to this request details prices in unit figures, for the purposes of this request, it is expected if any changes occur to these figures they will be within a 10% margin.

Note: The successful vendor will be responsible for completing the purchasing of the above hardware including customs duty exception documents and delivery to the relevant sites.

5.3.2 Installation & Implementation

From the analysis reports in Appendix J, details are supplied of the scope of work required in each of the following areas. The vendor will complete the following work and ensure that no user desktop remains on the LAN that does not meet these criteria.

- Perform the necessary RAM upgrade
- Perform the necessary OS upgrades
- Installs the replacement desktops
- Reconfigures all the desktops as members of the child domain.
- Ensures that at least Office 2000, with a full outlook client install, is on all desktops.
- Configured Anti Virus software
- Configures the relevant users eMail account on the desktop

Note: In all of the above the vendor is responsible for minimal user downtime, ensures that no users data is lost; users receive adequate notification of work, reinstallation of any client application that the user requires to complete their function

5.3.3 Testing & Handover

The vendor will ensure that testing is carried out as appropriate and that signoff is received for all work completed. Signoff is received per desktop completed; when the eMail service is completed and handover is complete support will be from the Call Centre and the Operations Centre.

The vendor will conduct an on-site training for the government institution IT department and the Operations Center for all installed devices.

5.4 Active Directory and eMail configuration

5.4.1 Purchasing

Two child domain servers are required for each joining institution that will become the domain controllers. The required specifications for these servers is found in Appendix K – Server Specifications

Note: The successful vendor will be responsible for completing the purchasing of the above hardware including customs duty exception documents and delivery to the relevant sites.

5.4.2 Installation & Implementation

5.4.2.1 Servers

The Vendor will install the servers to the standard build, details of the build required will be provided by the Operations Centre. The operations centre will provide the administration account required to build the servers within the new child domain.

The vendor will ensure the following are completed:

- The child domain is secured so that no other administrators from the root or other child domain have any access.
- Individual accounts created for each administrator and administrator software installed on specified workstations.

5.4.2.2 Users

Within Appendix J, details of the scope of users to be created are found under item K - Total Number of Users to be created. When creating the users, a mailbox is also required (details of the configuration to be used when creating the mailboxes within each institution will be provided by the operations center) and the following details will need to be entered into the users properties (the local institution will provide this information).

First Name
2nd Name
3rd Name
Last Name
Directorate/Unit
Job Title
Job Description (optional)
National ID
OfficeTelephone
OfficeTelephone Extension
Direct Line
Office Fax
Work Mobile
Home Telephone (optional)
Gender Salutation
EmployeePhoto (optional)

5.4.2.3 eMail

Within Appendix J, H specified the number of existing eMail users within each institution. If any email users exist then email migration is required. The Vendor will ensure that email migration will happen so that there is minimal downtime for the users and that emails on the existing systems are archived to a personal folder on the client’s desktop at the time of configuring their new email account. Aliases will be created in the event that the existing email address does not conform to the naming standards so that users will still receive email sent to their old address after migration.

In the event of no existing email service then the vendor will create the email address defined by the standard naming conventions and configure the outlook client for all users.

5.4.3 Testing & Handover

The vendor will ensure that testing is carried out as appropriate and that signoff is received for all work completed. When the eMail service is completed, the vendor will coordinate to the Call Centre and Operations Centre.
The vendor will conduct an on-site training for the government institution IT department and the Operations Center for all installed devices.

5.5 Training

5.5.1 User Training

All users are to complete Outlook training. The number of users will be the same as detailed in Appendix J K – total number of users. The training provider will schedule the training in conjunction with the government institutions training coordinators to best fit their requirements. Training should cover but is not limited to the following items:
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.

5.5.2 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
- Supporting Microsoft Windows 2000 Professional & Server
- Managing MS Windows 2000 Network Environment
- Implementing and Managing Microsoft Exchange 2000

The training provider is required to coordinate the training schedule with the administrators to create a schedule that best fits their needs.

5.6 Operations Centre

Within Appendix C, the operations centre may define software or other hardware requirements for this phase of the implementation. All hardware and software defined within this Appendix must be purchased, customs cleared, delivered to appropriate site, installed, implemented, tested and handover to the operations centre.

5.7 Institution’s network standardization

5.7.1 Design

5.7.1.1 Network

For each institution, the vendor will verify existing network diagrams and work with the local IT team to draw up revised network design where appropriate. This revised design will be required for the following:

- Internet traffic will be router via the SGN
- All web servers and firewalls within the institution should be placed on the DMZ of the SGN firewall.
- All external links to the institution should be placed on a DMZ

5.7.1.2 IP

For each institution an IP design that conforms to the standards, see Appendix E for existing scenarios, must be agreed by the vendor and the local institution. The scenarios in the Appendix are just two variations of the standards; additional scenarios can be added if these do not meet the joining institution’s requirements.

5.7.2 Implementation

Once the above Network and IP designs have been agreed and submitted to the Operations centre and approved. The vendor plans their implementation with the local institution. Once project approval of the plan is obtained the vendor completes the required changes with the local institution. It is important that the users have minimal disruption of their services so planning to work outside working hours is most likely.

5.7.3 Testing and handover

Prior to the implementation of the new network design and IP design, the vendor draws up a test plan with the local institution that will test all functionality and services provided within the institution. Once the change over is complete the testing is carried out and signoff obtained, the new network and IP schema belong to the local institution.

5.8 Anti Virus

The vendor will ensure that the anti virus client is installed on each client on the institution’s network and on relevant servers connected to the LAN. The master server will be installed within the institutions local network, this may be on one of the new domain controllers and that it receives updates from the operations centre. All installations of this software must adhere to the standards already defined; these are obtained from the operations centre.

5.9 Networking Services

5.9.1 DNS

The Root DNS server is installed in the Operations Centre. A DNS server is required in each Domain created and will be installed on each DC (Domain Controller) in these Domains. All DNS servers will be Active Directory Integrated Zones.

The Root DNS server will be configured to forward lookup for external DNS resolution to the public DNS.

5.9.2 WINS

One WINS server will be placed in each ministry, and will be installed on the First Domain Controller in each Domain (DC01).

5.9.3 DHCP

One DHCP server will be placed in each ministry, and will be installed on the Second Domain Controller in each Domain (DC02).

5.10 Project Deliverables

- Confirmed inventories for each government institution, desktop, user, existing email users and network.
- Network diagrams of current design and proposed design if necessary with implementation plan
- Proposed IP schema for each government institution with implementation plan.
- Implementing the new Network and IP designs within each government institution.
- Delivery documents and maintenance agreements for all necessary hardware and software including handover of hardware and licenses to relevant groups. Inventory lists of new equipment.
- Signoff on upgrade/replacement of desktops within each institution by local IT group.
- Implementation of ant virus on all desktops and relevant servers within institution, configuration as per standards.
- Network services configuration and roll out to all desktops and relevant servers within institution; this includes DHCP, DNS and Wins.
- Installing the child domain within the institution, creating user accounts, updating user profiles, and creating mailboxes. Ensuring that administrative accounts and workstations configured for local IT group to administrator the domain.
- Rollout of new email accounts to every user within each institution, detailed implementation plan agreed with local institution beforehand and submitted to Project steering group.
- Outlook training for all users within all joining institutions
- Administrative training for 2 administrators within each joining institution.
- Handover of administration of child domain to local IT group, this includes providing detailed documentation and workshops to ensure that each local IT group can take ownership.
- SGN connectivity to each joining institution with signoff obtained by both the local IT group and the Operations Centre.
- Configuration of relevant components within the email environment to facilitate the rollout to the existing standards
- Configuration of all network components to existing standards
- Monitoring of all new elements of the SGN and eMail environment implemented and signed off
- Update of all related documents, with regard to configurations, monitoring, maintenance, etc

The winner is required to update the following documentation as part of the SGN phase 2 project and reflect any changes to the architecture and implementation of the SGN and E-mail system.

No	Phase Name	Area of Project	No	Document Final Name
1	**Overview / Design**	Networking	1	IP Planning Design Document
		Networking	2	Physical Design Document
		Networking	3	Functional Design Document
		AD / E-mail	4	Enterprise Directory Overview Document
		AD / E-mail	5	Active Directory Architecture
		AD / E-mail	6	Exchange 2000 Architecture
		AD / E-mail	7	Naming Conventions Standard
		AD / E-mail	8	Email Backup Policy
		AD / E-mail	9	Email Usage Policy
		AD / E-mail	10	Anti-Virus Policy
		AD / E-mail	11	Workshop Presentation - AD & E-mail
2	**Client Roll Out**	AD / E-mail	1	Client Roll Out Check List
		AD / E-mail	2	Employee Roll Out Notification - Arabic
		AD / E-mail	3	Employee Roll Out Notification - English
		AD / E-mail	4	File Type and Application Extension List

3	**Proof of Concept**	AD / E-mail	1	Exchange B/E Build Standard
			2	Proof Of Concept Test Script
4	**Implementation**	Networking	1	Firewall Implementation
		Networking	2	Network Intrusion Detection
		Networking	3	SGN Test Acceptance Document
		AD / E-mail	4	Server Build Standard
		AD / E-mail	5	DHCP Configuration Standard
		AD / E-mail	6	WINS Configuration Standard
		AD / E-mail	7	Exchange F/E Build Standard
		AD / E-mail	8	Domain Controller Standard
		AD / E-mail	9	Backup Server Build Standard
		AD / E-mail	10	Backup & Restoration Standard
		AD / E-mail	11	Anti- Virus Build Standard
		AD / E-mail	12	SAN Configuration Document
		AD / E-mail	13	Exchange Cluster Build Standard
		AD / E-mail	14	NIC Test Acceptance Document
		AD / E-mail	15	DNS Configuration Standard
		AD / E-mail	16	Exchange & Active Directory Modifications
		AD / E-mail	17	Servers Operating System Hardening Checklist
5	**Ministry Side**	AD / E-mail	1	Ministries Test Acceptance Blank Document
		AD / E-mail	2	Acceptance Criteria For E-mail Migration
6	**Operations / NIC**	AD / E-mail	1	NIC Dell Rack Physical Layout
		AD / E-mail	2	Operations Daily Checklist
		AD / E-mail	3	Operations Weekly & Monthly Checklist
		AD / E-mail	4	Call Center Log Sheet
		AD / E-mail	5	User Object Process Document
		AD / E-mail	6	Email + SGN Change Control Procedure

Appendix A – Contact details for response or query to RFP

MoICT need to provide the following details here:

Address to whom the response to RFP is posted, whether eMail, Fax Number or postal address. MoICT should also provide details of communication method to be used in the event of a vendor having a query on the RPF if different.

Appendix B – List of Institutions within this Phase

The full list of all government institutions to be included in this phase should be listed here.

Appendix C – Purchasing requirements defined by the Operations Centre

The Operations Centre is responsible to ensure that all additional hardware and software requirements required to facilitate the joining of the new institutions is detailed here.

This list should include but is not limited to the following:

- eMail Anti Virus licenses (there should be sufficient client licenses for all email users, current and those within this current scope)
- Client Anti Virus licenses (should cover all desktops with joined and joining institutions, operations center and functional devices and servers on the expanded SGN)
- Network devices required to support the joining institutions (this could be a router card or an additional router)
- Servers to support the expanding eMail service (could be additional clustered back-end servers, load balanced front-end servers or additional disk space)
- Any necessary communication lines to support the joining institutions (E1 Lines, BRI lines, PRI Lines and Fiber Lines)
- Maintenance and support on all the above

SGN:

The Vendor is required to purchase the required network cards for the SGN routers within the Operations Centre to match the solution that JTC are providing. Termination of the E1 links within the Operations Centre will be via the optical channalized STM1. Details of the existing solution within the Operations Centre are provided in Section 4.3.2

eMail:

The Vendor is required to provide a recommendation for the expansion of the current SAN solution within the Operations Centre to facilitate at least an additional 2,000 users, where the maximum mailbox size is set at 100MB. The solution should be easily expandable, ensure that maximum use is made of the SAN solution.

Since the solution is going to have major growth over the coming years, the vendor should detail how the solution should be grown on a phased approach, with the maximum size being for a solution that would support 100,000 users.

The following details the current implementation:

SAN Hardware

The Clariion :		
	Dell /EMC FC4500 SAN Box	10 X 36 GB
	Dell /EMC FC DAE Expansion Box	10 X 73 GB
	Dell /EMC Control Box	
Dell /EMC FC-2 Switch	16 Ports	
Dell Power Vault PV128 T		
Optical HBA		
5M Multi Mode Fibre Cables		
5M Optical Fibre Cables		

SAN Software

EMC Navisphere Management Software Package v 5.3.0.
EMC Navisphere Agent Software Package.
San Card Driver for Windows 2000 Server.

The SAN Clariion consists of 19 Hard disks and One Hot Spare. Total storage space on the SAN is shown in the following table:

Clariion			
Location	**No. of Disks**	**Storage / Disk GB**	**Total Storage GB**
Clariion FC4500	10	36	360
Clariion DAE Expansion	9	73	657
Hot Spare	1	73	73
Total Array Size			1090

Clariion Hardware box components

Piece #	Description	Abbreviation	Contents
1	Enclosure 0	DPE	Disk Processor Enclosure
2	Enclosure 1	DAE	Disk Array Enclosure
3	SPA SPB Power Supply		Storage Processor A Storage Processor B Stand By Power Supply - Fans

System Configuration Information

Choose DPE type	FC4500
Array number	1
Total # of Disk Modules	20
# of Hot Spares	1

Server Name	Array Number	Host Name Conn-cted to	RAID Type	RAID Group #	Driver Modules*	Driver Size	LUN #
					0_4,0_5	36 GB	
GOJBEX01	Srv 1 &	Quarum	Raid 1	0x01	(Useable Capacity =32.74GB)		0x01
GOJBEX02	Srv 2						
GOJBEX01	Srv 1 &	MDB1	Raid 5	0x01	1_5,1_6,1_7,1_8	73 GB	0x02
GOJBEX02	Srv 2				(Useable Capacity =199GB)		
GOJBEX01	Srv 1 &	MDB2					0x03
GOJBEX02	Srv 2						
GOJBEX01	Srv 1 &	MDB3	Raid 5	0x02	0_6,0_7,0_8,0_9	36 GB	0x04
GOJBEX02	Srv 2				(Useable Capacity =98.23GB)		
GOJBEX01	Srv 1 &	MDB4					0x05
GOJBEX02	Srv 2						
GOJBEX01	Srv 1 &	PF 1	Raid 5	0x03	1_0,1_1,1_2	73 GB	0x06
GOJBEX02	Srv 2				(Useable Capacity =132GB)		
GOJDCO01	Srv 5 &	ADDB1					0x07
GOJDCO02	Srv 6	ADDB2					0x08

GOJBEX01	Srv 1 &	SG1 LOGS	Raid 1	0x04	1_3,1_4	73 GB	0x09
GOJBEX02	Srv 2				(Useable Capacity =66.36GB)		
GOJBEX01	Srv 1 &	SG2 LOGS					0x0A
GOJBEX02	Srv 2						
GOVDCO01	Srv 3	ROOTLOG1					0x0B
GOJDCO01	Srv 5	ADLOG1					0x0C
GOJDCO02	Srv 6	ADLOG2					0x0D
GOVDCO02	Srv 4	ROOTLOG2					0x0E
GOVDCO01	Srv 3		Raid 5	0x05	0_0,0_1,0_2,0_3	36 GB	0x0F
GOVDCO02	Srv 4	ROOTADDB2			(Useable Capacity =98.23GB)		0x10
			HotSpare		1_9	73 GB	0X00

Anti Virus Licences:

Sybari
Currently there exists an agreement for 700 users with Sybari. The operations center requires an agreement that will allow easy expandability of this number as the number of email clients expands. The agreement should be such that with each expansion of the SGN the same agreement applies, requiring an upgrade on a regular basis is ok as long as it covers all users regardless of when they joined. For eMail the Anti Virus will be Sybari.

The minimum requirement is that the agreement obtained covers all existing users (utilizing the existing agreement) and those to be implemented within this phase plus the projected growth of all joined institutions over the next six months. Within the agreement there needs to be a clear process for adding additional users, maybe upgrade on a yearly basis.

Client Anti Virus
Currently there are 700 Norton client licenses available. The Operations Centre required that an agreement be put in place that will cover all existing clients on the SGN and will be easily upgradeable/expandable as additional clients join the SGN. The agreement should be such that with each expansion of the SGN the same agreement applies, requiring an upgrade on a regular basis is ok as long as it covers all users regardless of when they joined

The current software is Norton but an alternative of similar caliber will be acceptable.

Appendix D – Current Membership of SGN & eMail Initiative

Initial Phase:

During the initial phase which was completed the end of February 2003 the following government institutions were connected to the SGN and had the following number of eMail users online.

Ministry	**No. Of eMail clients**
Ministry of Finance	101
Prime Ministry	79
Ministry of Information, Communications & Technology	60
Ministry of Planning	150
Municipality of Amman City	124
Ministry of Trade	102

MoICT will need to update this appendix every time a phase in the initiative is completed.

Appendix E – IP Scenarios

The Operations Centre must verify that all published IP Scenarios used with existing joined government institutions are detailed in this section.

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.AAAOOOOO.SSSSSNNN.HHHHHHHH**.
Where, AAA represents the area ID, 8 areas are available
OOOOO 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.AAAOOOOO.SSSSSNNN.HHHHHHHH**.
It is going to be divided as follows:

10.AAAOOOOO.0.0 -->10.AAAOOOOO.7.0 Netmask 255.255.248.0	**Reserved**
10.AAAOOOOO.8.0 -->10.AAAOOOOO.15.0 Netmask 255.255.248.0	**Main site**
10.AAAOOOOO.16.0 -->10.AAAOOOOO.23.0 Netmask 255.255.248.0	**Reserved for main site**
10.AAAOOOOO.24.0 -->10.AAAOOOOO.31.0 Netmask 255.255.248.0	**Reserved for large sites**
10.AAAOOOOO.32.0 -->10.AAAOOOOO.39.0 Netmask 255.255.248.0	**Reserved for large sites**
10.AAAOOOOO.40.0 -->10.AAAOOOOO.47.0 Netmask 255.255.248.0	**Reserved for large sites**
10.AAAOOOOO.48.0 -->10.AAAOOOOO.55.0 Netmask 255.255.248.0	**Reserved for large sites**
10.AAAOOOOO.56.0 -->10.AAAOOOOO.63.0 Netmask 255.255.248.0	**Reserved for large sites**
10.AAAOOOOO.64.0 --> 10.AAAOOOOO.127.0 Netmask 255.255.252.0	**Reserved for medium sites (16 networks)**
10.AAAOOOOO.128.0 --> 10.AAAOOOOO.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.AAAOOOOO.SSSNNNHH.HHHHHHHH**. **Only for the main site**

10.AAAOOOOO.0.0 -->10.AAAOOOOO.31.0 Netmask 255.255.224.0	**Reserved**
10.AAAOOOOO.32.0 -->10.AAAOOOOO.63.0 Netmask 255.255.224.0	**Main site**
10.AAAOOOOO.64.0 --> 10.AAAOOOOO.127.0 Netmask 255.255.252.0	**reserved for Large to medium site (16 networks)**
10.AAAOOOOO.128.0 --> 10.AAAOOOOO.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 F – Naming conventions

The Operations centre needs to verify that the details enclosed within this appendix are current at the time of publishing; any updated required are the responsibility of the Operations Centre.

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 1ST 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***

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***

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**:	*min* @ *min*.gov.jo
For the "**Minister**":	minister @ *min*.gov.jo
For the "**Secretary General**":	sg@ *min*.gov.jo
For the "**Mayor**" at Amman City:	mayor @ amm.gov.jo
For the "**Deputy Mayor**" at Amman City:	dmayor @amm.gov.jo
For the "**Under Secretary**" at Amman City:	wakeel @amm.gov.jo

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 G – Institution SGN Hardware and Cabinet

The Operations Centre is responsible to ensure that any changes to the standard hardware within the joining institution are updated here.

Part No	Description	Qty
	Main Link Router	
MEM3600-16FS-INCL	16MB FLASH DEFAULT FOR CISCO 3600	1
WIC-1B-S/T	1-Port ISDN WAN Interface Card(dial and leased line)	1
WIC-1T	1-Port Serial WAN Interface Card	1
NM-2W	2 WAN Card Slot Network Module(no LAN)	1
PWR-3660-AC	AC Power Supply for Cisco 3660	1
PWR-3660-AC	AC Power Supply for Cisco 3660	1
ACS-3600ASYN	Auxiliary/Console Port Cable Kit for the Cisco 3600 Series	1
CISCO3660-BP	Backplane for Cisco 3660	1
CISCO3660-BEZEL	Bezel for Cisco 3660	1
NM-BLANK-PANEL	Blank Network Module Panel	5
S366C-12205	Cisco 3660 Series 10S IP	1
CISCO3662-AC	Dual 10/100 E Cisco 3660 6-slot Modular Router-AC with IP SW	1
MEM3600-32SD-INCL	Included 32MB S DRAM for 3660s at NO COST	1
CAB-ACU	Power Cord UK	2
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	1
	Cat 2950-12	
WS-C2950-12	12 port, 10/100 Catalyst Switch, Standard Image only	4
CAB-ACU	Power Cord UK	4
	PIX 525-UR	
PIX-525-UR-BUN	PIX 525UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	1
CAB-ACU	Power Cord UK	1
SF-PIX-6.1	PIX v6.1 Software for the PIX Chassis	1
PIX-4FE	PIX Four-port 10/100 Ethernet interface, RJ45	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	PIX 525-FO	
PIX-525-FO-BUN	PIX 525FO Bundle (Chassis, failover SW, 2 FE ports, VAC	1
CAB-ACU	Power Cord UK	1
SF-PIX-6.1	PIX v6.1 Software for the PIX Chassis	1
PIX-4FE	PIX Four-port 10/100 Ethernet interface, RJ45	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	Cabinet	
Cabinet	42U 600x600x2000,with fans and 4-way power Strip, appropriate ventilation, Glass fronted, Wall Mounted/Full Standing	1
	Cabinet shelf for E1 & ISDN termination boxes if required	1

Appendix H – JTC specification

It is the responsibility of the Operations Centre to ensure that the details specified here are the expected specifications for the hardware that exists within the Operations Centre and that they match.

For each institution the following links are required:

E1 link from the Operations Centre based at the NIC to the joining institution. Termination of the link within the Operations Centre will be via the Fiber optic channalized STM1, at the institution end the termination type will be V.35.

ISDN link from the Operations Centre based at the NIC and the joining institution. This is the backup link for the E1.

Appendix I – Change Control Process

The Operations Centre Manager (This process is owned by the change control manager please change if not the Ops Center manager) is responsible for ensuring that the following process is the most up to data at time of Publication

All Change control must be submitted to the change control Manager via eMail to the following address Ops.Centre.Change.Control@goj.gov.jo in writing. Using the form attached.

The request will be processed at the next monthly Operations meeting; so all requests must be submitted in a timely fashion.

Operations Centre

CHANGE REQUEST

Change Number: .... (Allocated by the Operations Centre Systems Administrator)

Server/Network Host Name: ....

Please delete explanatory text (in italics) below and overwrite <u>all fields</u> with required information.

SINGLE LINE DESCRIPTION OF CHANGE	**Change Description**	*A brief summary in less than 10 words.*
AFFECT ON OPERATION OF HIGH AVAILABILITY SOFTWARE	**Yes/No**	*If "Yes", provide details of how change will affect HA. If no implications, enter"No".*
REQUESTOR OF CHANGE	**Name** **Location** **Tel No/Email**	*Name* *Location* *Contact Information*
APPROVAL STATUS **"Four steps for approval" apply to MOICT-related CRs:** Business Owner (MoICT, Ministries) Operations Centre Manager (or nominee) Ops Centre Systems Administrator Defined Contacts for the Change		TRANSMISSION OF THIS CHANGE REQUEST (CR) TO THE CHANGE CONTROL MANAGER (CCM) SIGNIFIES FULL LOCAL TECHNICAL AND MANAGEMENT APPROVAL HAS ALREADY BEEN GRANTED AND ANY FINANCIAL IMPLICATIONS HAVE BEEN ADDRESSED. PLEASE KEEP THE CCM INFORMED IF THE STATUS OR REQUIREMENTS OF THIS CR ALTER.
	Name **Date** **Role** **Tel No/Email**	Details of Business Owner entered here for the system, who should provide an approval email to the CCM to support the CR, prior to the next approval step. *Conditional approval is given by the Ops Centre Manager, dependent on a technical evaluation and risk assessment by the Systems Administrator.*
DATE REQUIRED OR PLANNED	**Date** **Times**	*Date when the change needs to be implemented, including start and end times.*
DETAILED DESCRIPTION	**Detailed Description**	*A technical description of the planned change, or requirement, in as much detail as known, or appropriate. Indicate areas of significant potential impact. Reference may be made to other relevant documents, which should be attached when this CR is submitted.*
JUSTIFICATION	**Reason**	*The reason the change is required, and by whom.*
CATEGORY Ops Centre team standard lead time is 5 days, although best efforts is aimed to achieve < 5 days, in most cases	**<u>Cat</u>** **<u>Lead Time</u>** 00 Best efforts Major 31 days Signif. 17 days Local 5 days	Indicate appropriate Category:
CLIENT IMPACT	**H/M/L** **No/% Clients Impact**	*High, medium or low.* *Number or % of clients/users who may be affected.* *Text to define who might be impacted, and by how much.*
RISK ASSESSMENT	**H/M/L** **Risk**	*High, medium, or low.* *Detail the risk(s), as appropriate.*

TEST ARRANGEMENTS	**By Whom** **To Test** **Other Parties**	*Who will undertake the testing.* *What will be tested.* *Other parties who will need to be involved.*
BACK-OUT PLAN	**Description**	*Describes how to recover if the change is not successful.*

Ministerial Authorisation (or Ops Centre Manager Authorisation, if Change Request affects Ops Centre only)

Please send the completed form to the CCM: Ops.Centre.Change.Control@goj.gov.jo

Appendix J – Analysis Reports

MoICT need to include an analysis report for each institution included within this scope – template included…

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 K – Institution Desktop & Servers Hardware Specifications

The operations Centre are responsible for ensuring that these specifications are current at time of publishing.

Client Desktops

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 required)
Microsoft Windows XP Professional
Microsoft Outlook 2000

Child domain Servers

Domain controllers recommended Specs

Processor:	1 processor, Pentium 4 1.7 GHz speed or more.
Memory:	512 MB RAM or More
Locally attached storage	
Drive controller:	SCSI 3
Hard Drives:	20GB or more
Hard Drive bays:	2-4 (RAID 1 recommended)
Network Interface Card:	One 10/100 Fast Ethernet adapters supporting PXE (Pre-boot Execution Environment).

Appendix L – Document Library

The operations Centre are responsible for ensuring that this list is current at time of publishing.

No	Phase Name	Area of Project	No	Document Final Name
1	**Overview / Design**	Networking	1	IP Planning Design Document
		Networking	2	Physical Design Document
		Networking	3	Functional Design Document
		AD / E-mail	4	Enterprise Directory Overview Document
		AD / E-mail	5	Active Directory Architecture
		AD / E-mail	6	Exchange 2000 Architecture
		AD / E-mail	7	Naming Conventions Standard
		AD / E-mail	8	Email Backup Policy
		AD / E-mail	9	Email Usage Policy
		AD / E-mail	10	Anti-Virus Policy
		AD / E-mail	11	Workshop Presentation - AD & E-mail
2	**Client Roll Out**	AD / E-mail	1	Client Roll Out Check List
		AD / E-mail	2	Employee Roll Out Notification - Arabic
		AD / E-mail	3	Employee Roll Out Notification - English
		AD / E-mail	4	File Type and Application Extension List
3	**Proof of Concept**	AD / E-mail	1	Exchange B/E Build Standard
			2	Proof Of Concept Test Script
4	**Implementation**	Networking	1	Firewall Implementation
		Networking	2	Network Intrusion Detection
		Networking	3	SGN Test Acceptance Document
		AD / E-mail	4	Server Build Standard
		AD / E-mail	5	DHCP Configuration Standard
		AD / E-mail	6	WINS Configuration Standard
		AD / E-mail	7	Exchange F/E Build Standard
		AD / E-mail	8	Domain Controller Standard
		AD / E-mail	9	Backup Server Build Standard
		AD / E-mail	10	Backup & Restoration Standard
		AD / E-mail	11	Anti- Virus Build Standard
		AD / E-mail	12	SAN Configuration Document
		AD / E-mail	13	Exchange Cluster Build Standard
		AD / E-mail	14	NIC Test Acceptance Document
		AD / E-mail	15	DNS Configuration Standard
		AD / E-mail	16	Exchange & Active Directory Modifications
		AD / E-mail	17	Servers Operating System Hardening Checklist
5	**Ministry Side**	AD / E-mail	1	Ministries Test Acceptance Blank Document
		AD / E-mail	2	Acceptance Criteria For E-mail Migration
6	**Operations / NIC**	AD / E-mail	1	NIC Dell Rack Physical Layout
		AD / E-mail	2	Operations Daily Checklist
		AD / E-mail	3	Operations Weekly & Monthly Checklist
		AD / E-mail	4	Call Center Log Sheet
		AD / E-mail	5	User Object Process Document
		AD / E-mail	6	Email + SGN Change Control Procedure