CONVERSION OF A 300 USER UNCLASSIFIED NETWORK TO A RESTRICTED HIGH NETWORK

by
Roger M Griffin and Peter J Fischer

ABSTRACT

The United Kingdom Government Secure Intranet network (GSI), links the networks of its members, (typically Government departments) to each other via a common backbone. It also links them to the Internet and to other external networks. It provides facilities similar to those being used by many commercial organisations, including those found on the Internet. The facilities provided include email interchange between individual Government departments, email exchange between Government departments and businesses or persons connected to the Internet, access to World Wide Web pages held on servers in the GSI from client machines in Government departments and access to internal (Government only) web pages in Government departments. Some of the information interchange between Government departments may involve information at the RESTRICTED level of classification.

Government departments wishing to connect with GSI must go through a process of accreditation. We describe that process and the processes, undertaken by the Civil Service College with a Windows NT unclassified network of some 300 users, in order to achieve accreditation and connection to the GSI.

The Civil Service College runs a number of information security courses, some with the assistance of the National Authorities. The exercise was undertaken in a manner, which followed standard procedures as closely as possible, in order to supplement relevant courses and to maximise the benefits of relevant teaching points.

In particular, emphasis was given to the writing of the System Security Policy (SSP) and the risk analysis process.

INTRODUCTION

The Civil Service College (CSC) is an executive agency of the Office of Public Service of the Cabinet Office. In 1997 the Central Information Technology Unit (CITU) proposed that a Government Secure Intranet (GSI) be established which offered the facility for Her Majesty's Government (HMG's) Departments to share protectively marked information by electronic means and also to connect to the Internet.

Government departments wishing to connect to GSI must go through a process of accreditation, in which their ability to process responsibly protectively marked RESTRICTED information and to avoid prejudicing the security of the GSI is demonstrated. The authors describe that process and the processes undertaken by the CSC in order to convert their Windows NT unclassified network of some 300 users, to a RESTRICTED HIGH system with the aim of achieving accreditation and connection to the GSI.

THE CIVIL SERVICE COLLEGE

The College has two centres, one in Belgrave Road in London, the other at Sunningdale in Berkshire. At their Sunningdale location, CSC has residential accommodation for some 260 students with extensive grounds and recreational facilities.

In November 1996 CSC was recognised as "An Investor in People (IiP)" a Government standard and in that financial year achieved full recovery of costs from earned income. College staff consist of permanent and temporary members, its permanent staff members are established Civil Servants whilst the latter may also be established Civil Servants serving on 3 to 5 year loan periods with the College. Staff members are also recruited from the private sector on similar short-term contracts. The primary aim of the College is to develop personal, managerial and professional skills amongst Civil Servants and others; and to promote best practice throughout Government both in managerial and in key professional areas.

The College provides:

a. Management training for those at or aspiring to senior positions.

b. Specialist training in key professional areas or at advanced levels.

c. Related consultancy and research.

The College published business targets for the previous financial year as:

a.	Consultancy income (£000).	1, 600.
b.	Students from Senior Civil Service (SCS).	2, 400.
c.	Students from Private Sector.	1, 400.
d.	Throughput of all students.	29,969
e.	Course evaluations in boxes 1/2, highest 1, lowest 6.	83%.

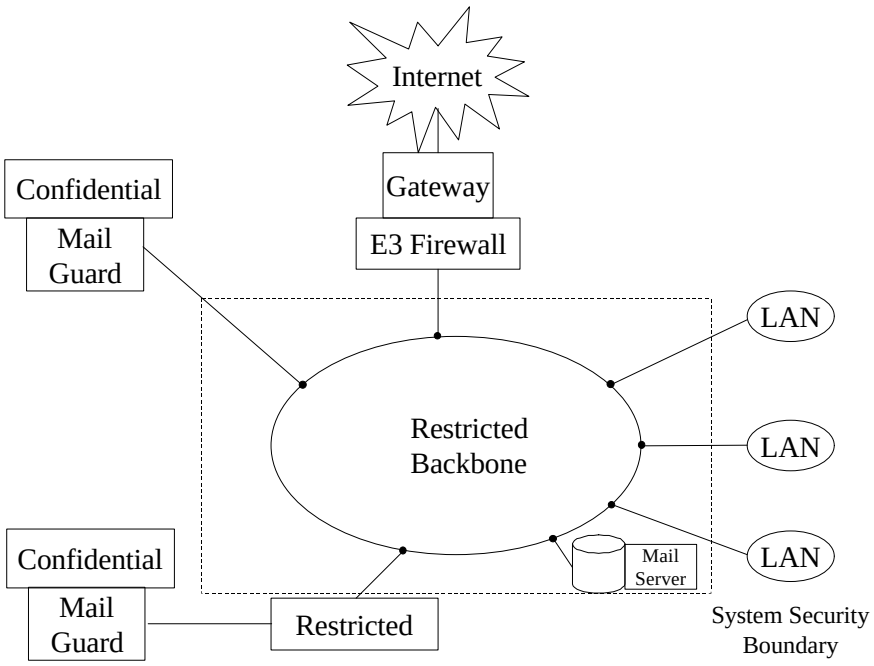
and achieved a total income for the year (£000) of 18, 251.

GOVERNMENT SECURE INTRANET

Role and Function

The United Kingdom Government Secure Intranet network (GSI), links the networks of its members, typically Government departments to each other via a common backbone. It also links them to the Internet and to other external networks. It provides facilities similar to those being used by many commercial organisations, including those found on the Internet.

Figure 1 Conceptual Schematic Diagram of the GSI



The facilities provided include email interchange between individual Government departments, email exchange between Government departments and businesses or persons connected to the Internet. Access to World Wide Web pages held on servers in the GSI is available from client machines in Government departments, as well as access to internal (Government only) web pages in Government departments. Some of the information interchange between Government departments may involve information at the RESTRICTED level of classification.

Requirements

The GSI Accreditation panel has issued a community security policy (CSP), Gladwyn and Collier (1997) for the GSI. Departments wishing to connect to the GSI are required to submit an application in the form of a completed certificate to the Accreditation panel. When submitting their application, potential users confirm their acceptance of the CSP as a minimum standard and that their system has been accredited to process the protectively marked material in question. More specifically that access control implementation was to the standard required by the GSI infrastructure and that their system conforms with a number of guidelines described in Communications Electronics Security Group (CESG) Memoranda. In particular, a System Security Policy in accordance with CESG memorandum 5 is in place, Security Operating Procedures (SyOPs) have been written and that users are authenticated using a password system in accordance with CESG memorandum 8.

Need to Connect

The fundamental issue concerning a need to connect is whether such connection is supported by an appropriate business case. At present there is considerable interest in support of the Open Government and Direct Access initiatives and connection to GSI is one way of speeding information flow between UK Government Departments.

Business Case for Connection

The Civil Service College obtains 96% of its business from the Civil Service. It runs courses in support of central initiatives, provides consultancy to Government Departments, and runs on-site courses when required.

At present its external email facility is through an external provider at significant annual cost. The growth in the use of external email is extremely fast, and it is becoming an essential communication channel for the College's business.

GSI is a central initiative and government departments are being encouraged to join this, both for the exchange of email, and for access to the Internet. The GSI is also seen as a means to fulfil the Prime Minster's requirement that in five years time 25% of government transactions with the public will be by electronic means.

Benefits from connecting to GSI

There are a number of benefits the College will gain from connecting to GSI. These are:

a. Annual savings on the present cost of external email.

b. Secure access to the Internet from the desktop, which is required for research purposes by College lecturers. This will replace the standalone systems that currently access the Internet.

c. Becoming part of the GSI 'club', and recognised by our customers as providing training for the Civil Service through online publicity.

d. Closer contact with the vast majority of our customers, through the use of email and (eventually) on line bookings.

e. Potential for raising revenue, by running courses and offering consultancy associated with the use of GSI.

f. Raises the possibility of even closer contact with our stakeholders and customers, by exchanging documents securely via email.

THE COLLEGE NETWORK

Introduction

The College network. Civil Service College Computing Infrastructure (CSCCI), is a client server system running Windows NT 4.0, serving 260 users. Users currently consist of College staff, lecturers, administrators, and visitors who may include lecturers and students from any country in the world and from public and private sector.

The College has previously issued a College Notice "Computer Security Issues" No 42/97 and a short handbook entitled "Information Technology Security Handbook" in order to enhance infosec awareness amongst its staff. Specific guidance was provided on the need for virus checking of files before attempting to load them onto the College network. The College now uses products that prohibit the loading on files onto the network before they have been examined for malicious software.

System Configuration

The CSC architecture is based upon Compaq Proliant servers running Windows NT Version 4. The PC clients run Windows 95 as the standard desktop operating system. RDBMS systems in use are Oracle 7 Workgroup Server and Microsoft SQL Server. Users are provided with access to server resources via PC workstations.

Packaged Software

The CSC has a Select agreement with Microsoft for the provision of COTS software. All software is cleared and tested by the College Information Systems Services section before deployment. The current College standard is Office 97 as the Office Automation system.

System Architecture

The main IT systems are split over two locations for resilience. There are currently a number of servers running Windows NT 4 in a single domain configuration using TCP/IP as the networking protocol. The Oracle Workgroup server is on a Compaq Proliant 5000, which runs in-house developed software to manage the College business. The College financial systems run on a Compaq Proliant 4500 and uses Systems Union Sun Financial software which utilises Microsoft SQL Server as the RDBMS. A Compaq Proliant 5000 provides the main file and print services. The other systems run mainly on Compaq Prosignia 500 servers and provide DHCP/DNS/WINS, on-line anti-virus scanner, software source files, Intranet services, back-up services, Exchange mail/GroupWare services. External mail connections are available through an AT&T mail gateway.

The College has a 10BaseT/100BaseTX/100Base FX network installed at the Sunningdale site and 10BaseT in the London centre. The network was originally installed in 1991 using CAT 3 UTP, within buildings. Seven buildings are connected to the network using 10BaseFL and three using FDDI (100Mb) at Sunningdale. The cabling system at Sunningdale has recently been upgraded to enhanced CAT 5 UTP.

There is a central Hub in each building connected to the fibre backbone and all network points within buildings are wired back to a central Hub. A Megastream link between the London centre and Sunningdale is used primarily for voice communication. The data network uses 2 x 64K channels from the link with CISCO 2503 routers at either end interfacing with the network.

As mentioned above, there are currently 260 users. CSCCI has capacity for 830 connections at Sunningdale and 141 at the London Centre.

ACCREDITATION

An initial accreditation meeting was arranged to assess the security profile of the network and the physical, procedural and technical security measures in place. During this meeting a number of issues were identified which would need to be investigated and, if necessary, resolved before the network could be properly accredited and an application submitted to the GSI Accreditation Panel for approval. These issues fell into 4 categories: security documentation; protective markings (classification); security measures and mechanisms; and security management procedures. Where a Department's security is particularly dependent upon technical countermeasures, the Accreditation Panel could request penetration testing from a respectable organisation such as CESG or DERA

Security Documentation

At the outset of the exercise, the CSC network was not in possession of an SSP or SyOPs. It was agreed that this documentation should be produced as soon as possible as it formed an essential part of the accreditation process.

Protective Marking

Some data processed on the CSC network was commercially sensitive and/or included personal information requiring protection under the UK Data Protection Act. In these circumstances an overall system-high protective marking (classification) of RESTRICTED was considered adequate for appropriate protection of College data.

Security Management

A number of concerns over the security measures and mechanisms emerged during the discussions. These included:

a. Physical security of some network components.

b. User access control and password management, (including PCs being left logged in, necessitating a time out facility after a set period of time).

c. Configuration of NT servers to implement additional security requirements.

d. Backup and recovery arrangements.

e. Configuration management and change control.

f. User account management and security monitoring.

g. Uncleared users.

Remote Access

CSC lecturers can run courses in any country; often there is a wish to allow lectures to remotely access the CSC network in order to obtain access to their email messages. The majority of these connections, particularly when set up for lecturers working from home, operate on a dial back system using NT Remote Access Service (RAS). For lecturers operating in overseas locations, the CSC has allowed direct dial in facilities, giving remote access privileges equivalent to those at the lecturers' College location.

Firewalls

The GSI CSP advises use of a firewall to provide additional protection for Departments connecting to GSI. The College has considered and agreed to this option. An exercise to select the firewall most appropriate to the College requirements is currently underway.

RESULTS

Whilst there is no doubt that the network is capable of accreditation to meet the requirements for connection to the GSI, there remains much work for the accreditation team to do. The target for completion of this work was set as June 1998 and by this date the necessary documentation had been passed to the College Business Executive prior to submission to the GSI Accreditation Panel. A description of this process, with updated information was submitted to, and accepted by, the Program Committee for the 21st National Infosec Conference and has resulted in our presentation today.

As already noted, a number of issues were identified and the process of their addressing is described below:

a. Risk Analysis. Risk analysis was in accordance with CESG Memorandum 10 (1996).

b. Penetration Testing. Penetration testing by a reputable organisation could be undertaken as part of the process. Informal testing by DERA has generated encouraging results.

c. Physical Security of Network Components. The mechanisms were inspected and found to be adequate. Management procedures were reviewed and improved.

d. User Access Control and Password Management. Under this heading we addressed; PCs being left logged in, the introduction of improved identification and authentication (I&A) for all users and the use of security modems for RAS users. The issue of PCs being left logged in was resolved by the implementation of password controlled screen savers. I&A improvements were achieved by use of Security Dynamics ACE hardware and software. Security modems from RACAL are under consideration for the improvement of access security for RAS users.

e. Configuration of NT Servers. Windows NT version 4.0 is currently under evaluation to ITSEC E3 by Logica. The College will continue to monitor the progress of the evaluation and will review its security practices and NT configuration on completion of the evaluation.

f. Backup and Recovery Arrangements. The existing College procedures were reviewed and improvements implemented.

g. Configuration Management and Change Control. The Security Manager has produced a list of criteria for re-accreditation purposes, which will be discussed with the Accreditor.

h. User Account Management and Security Monitoring. Procedures were re-assessed, but were considered to be adequate in this respect. The commissioning of CESG or DERA for further penetration testing at an appropriate time is under consideration.

i. Uncleared Users. To be issued with a reduced privilege account limiting access to a network server containing only non-protectively marked data.

The writing of the SSP provided the opportunity for a valuable review of all security associated with the Civil Service College Computing Infrastructure (CSCCI). All the topics identified and discussed above have been fully documented in the SSP.

CONCLUSIONS

The process has yielded considerable benefits in terms of enhanced procedures and quality control in the management of the CSCCI.

Connection to the GSI should provide the opportunity for realisation of the business benefits identified earlier in the paper.

The lessons learned in the Accreditation exercise and the resulting documentation will provide a valuable input to the College's range of Infosec courses and thus will provide benefit to HMG as a whole.

REFERENCES

Gladwyn, M. B. and Collier, A. Community Security Policy for the Government Secure Intranet, version 5.11, September 1997. *Central Computer and Telecommunications Agency*.

CESG Electronic Information Systems Security Memorandum No 5. System Security Policies, issue 3.0, July 1994. *Communications - Electronics Security Group.*

CESG Computer Security Memorandum No 8. Password Management, issue 2.0, June 1996. *Communications - Electronics Security Group.*

CESG Computer Security Memorandum No 10. Minimum Computer Security Standards for HMG, Information Handled by Information Technology Systems, issue 2.2 (Application to Networks), October 1996. *Communications - Electronics Security Group.*

Conversion of a 300 User Unclassified Network to a Restricted High Network

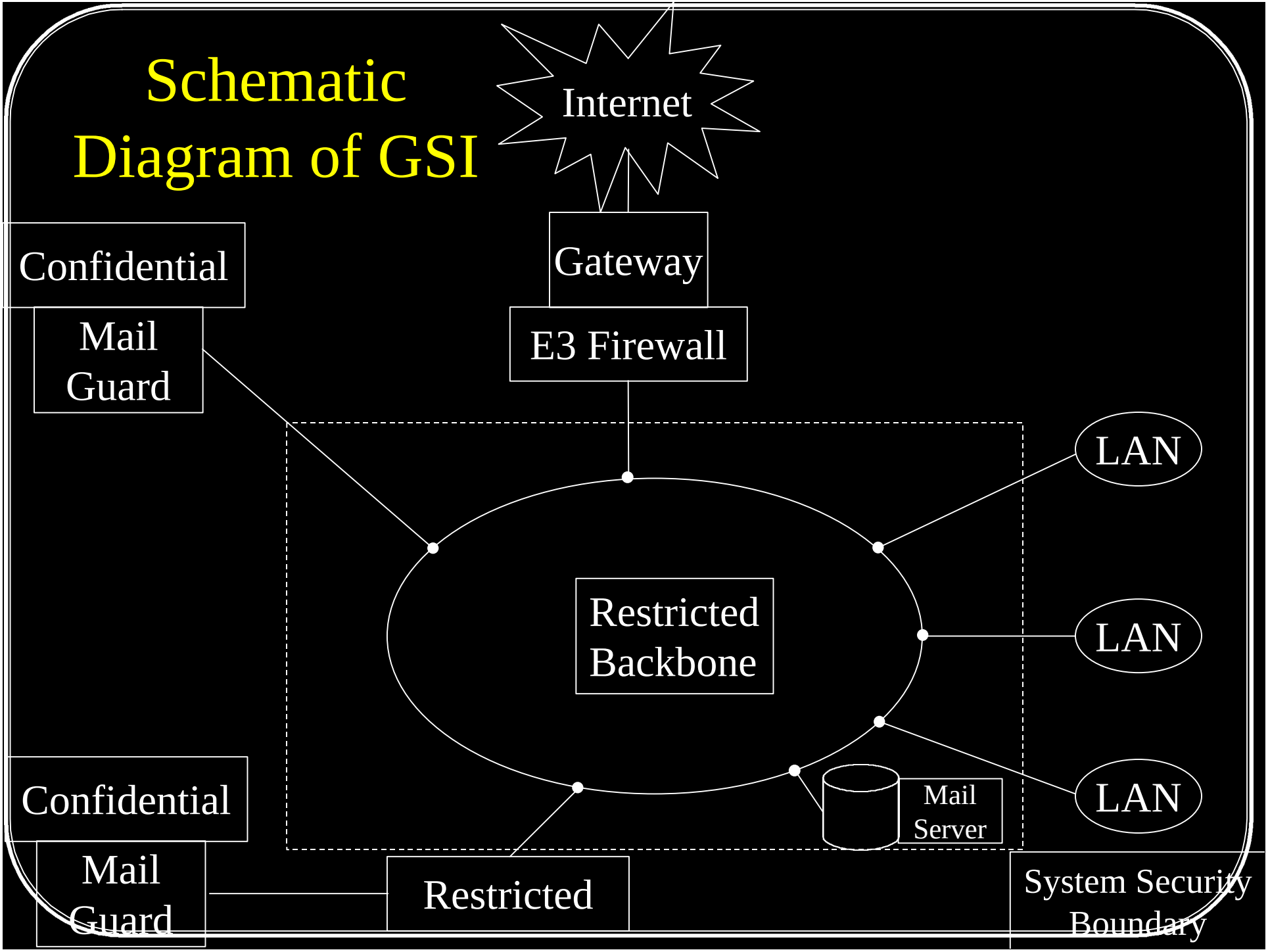
By

Dr Roger M Griffin

Mr Peter J Fischer

Introduction

- Government Secure Intranet (GSI).
- Connection.
- The Civil Service College (CSC).
- The CSC Computing Infrastructure (CSCCI).


Schematic Diagram of GSI
Internet
Gateway
E3 Firewall
Confidential
Mail Guard
LAN
Restricted Backbone
LAN
LAN
Mail Server
Confidential
Mail Guard
Restricted
System Security Boundary

Accreditation Issues

- Security Documentation.
- Protective Marking (Classification).
- Security Management.
- Remote Access.
- Firewalls.

Discussion of Issues

- Risk Analysis.
- Penetration Testing.
- Physical Security of Network Components.
- User Access Control and Password Management.

Discussion of Issues

- Configuration of NT Servers.
- Backup and Recovery Arrangements.
- Configuration Management and Change Control.
- User Account Management/Security Monitoring

Conclusions

- Improved Security.
- Improved Quality Control and Management.
- Realisation of Business Benefits.
- Training and Education Benefits across Government.