NGE Solutions

Building the Next Generation Enterprises

PISA

(Planning, Integration, Security and Administration)

An Intelligent Decision Support Environment for IT Managers and Planners

Sample IT Plan Generated

Note

This is a sample report that has been generated by the PISA environment. PISA generates many documents as a result of short (15 to 20 minutes) interviews. These documents are produced as html documents that can be easily modified by using MS Word (just open these documents in MS Word and edit them). For display only purposes, this document has been converted to PDF Format.

NGE Solutions, Inc. (www.ngesolutions.com)

IT Plan Generated by PISA PlanIT

PlanIT Executive Summary Report

You have worked through a complete session of the PISA planning process. This report gives a summary of all the results produced so far:

- **The Enterprise Model** that shows your company information (company type, company size, number of sites, what business processes are performed on what sites, what are the workgroups and where do they reside)
- **The Application Plan** that shows what business processes will be automated, what strategies (rent, buy, outsource, re-use) are used to automate the business processes, and any COTS (commercial-off-the-shelf) packages selected.
- **The Computing Platform plan** that shows the computing hardware and software needed to support the application plan.
- **The Network Plan** that shows the wireless as well as wired network to support your staff (called Intranet), your customers and your business partners and suppliers.
- **The Security Plan** needed to protect your corporate assets (databases, programs, computers, network links, network devices).

The next steps are:

- Develop an RFQ (Request for Quotation) to solicit proposals from consulting companies and service providers who will implement the plan
- Select and hire a consultant to refine and implement the plan

  This report can be used in all these steps. It is already in an RFQ format and can be used by the consultants to quickly understand what you are planning to do.

This report summarizes the results recommended by different components of CACIT based on the information provided in the interview

.

Total Work Force	
Sites	2
Mangers	11

Knowledge Workers	22
Operators	11

Application Packages

Automation Strategy for Business Processes

Business Process	Buy	Build	Outsource	Reuse	Rent
Corporate Management	X	-	-	-	-
Customer Support and CRM	X	-	-	-	-
Finance and Accounting	X	-	-	-	-
Human Resource Management	X	-	-	-	-
Logistics	X	-	-	-	-
Marketing	X	-	-	-	-
Production	X	-	-	-	-
Supply Chain Management	X	-	-	-	-
Sales	X	-	-	-	-
Warehousing and Distribution	X	-	-	-	-
e-Advertising	X	-	-	-	-

Network Plan	
Total Co-operative Networks	2
Total External Networks	1
Total Networks Devices	10
Total Networks	11

Computing Platform Selection

The computing platforms (hardware/software) are selected based on the type of work and workgroup. The following table shows an example of computing platforms selected:

Type	Operating System	Hard Ware

Security Recommendations

Object Type	Weakness	Solutions
hub	Device is not placed in a secure Location	Protect the network device by placing in a controlled area
LANSwitch	Device is not placed in a secure Location	Protect the network device by placing in a controlled area
Router	Device is not placed in a secure Location	Protect the network device by placing in a controlled area
wired	Unauthorized access to root password/ID	keep rooid ID/pw under strong security

DETAILED IT PLAN

Executive Summary

You have worked through a complete session of the planning process. This report gives a summary of all the results produced so far:

- **The Enterprise Model** that shows your company information (company type, company size, number of sites, what business processes are performed on what sites, what are the workgroups and where do they reside)
- **The Application Plan** that shows what business processes will be automated, what strategies (rent, buy, outsource, re-use) are used to automate the business processes, and any COTS (commercial-off-the-shelf) packages selected.
- **The Computing Platform plan** that shows the computing hardware and software needed to support the application plan.
- **The Network Plan** that shows the wireless as well as wired network to support your staff (called Intranet), your customers and your business partners and suppliers.
- **The Security Plan** needed to protect your corporate assets (databases, programs, computers, network links, network devices).

The next steps are:

- Develop an RFQ (Request for Quotation) to solicit proposals from consulting companies and service providers who will implement the plan
- Select and hire a consultant to refine and implement the plan

This report can be used in all these steps. It is already in an RFQ format and can be used by the consultants to quickly understand what you are planning to do.

This report summarizes the results recommended by different components of the system based on the information provided in the interview.

1. Enterprise Model

Profile Name: manuf1

1.1. Enterprise Model

Per your input, the summary of the enterprise model is as follows:

Industry Segment:	Manufacturing
Sites:	2 Local
Number of Employees:	44
Reliance on Web:	Basic Websites
Mobility Requirements:	No use of mobile computing
On Demand Services:	None

Summary of Business Functions and Personnel Distribution across the Organization

Locations	Business Functions	Personnel		
		Manager	Knowledge Worker	Operator
site1				
	Corporate Management	1	2	1
	Customer Support and CRM	1	2	1
	Logistics	1	2	1
	Marketing	1	2	1
	Production	1	2	1
	Supply Chain Management	1	2	1
site2				
	Finance and Accounting	1	2	1
	Human Resource Management	1	2	1
	Sales	1	2	1
	Warehousing and Distribution	1	2	1
	e-Advertising	1	2	1

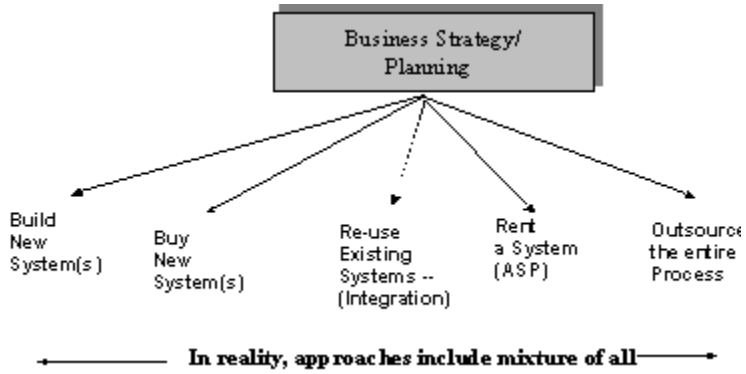
2. Application Plan

Summary Report from Application Advisor

Development of enterprise application planning consists of the following main steps.

1. Step1: identify the business processes (BP1,,,,BPn) for a given business based on type and size of business
2. Step2: For each business process, identify which ones will be done manually, which ones will be automated
3. Step3: For the automated services, determine a solution strategy (outsource, in-house development, buy, or reuse).

The following figure shows the main choices and the table summarizes the recommendations suggested by the Application Advisor.



Corporate Management
None Chosen
Customer Support and CRM
Product Name: Microsoft Business Solutions for Field Service Management o Vendor: Microsoft

- Product URL: http://www.microsoft.com/BusinessSolutions/fieldservice.aspx

Finance and Accounting

Product Name: Microsoft Business Solutions for Financial Management- Axapta

- Vendor: Microsoft
- Product URL: http://www.microsoft.com/BusinessSolutions/Axapta/financialmanagement.aspx

Human Resource Management

Product Name: Microsoft Business Solutions for HR Management - Axapta

- Vendor: Microsoft
- Product URL: http://www.microsoft.com/BusinessSolutions/Axapta/hrmanagement.aspx

Logistics

Product Name: Oracle E-Business Suite Logistics

- Vendor: Oracle
- Product URL: http://www.oracle.com/applications/logistics/intro.html

Marketing

None Chosen

Production

None Chosen

Supply Chain Management

Product Name: Microsoft Business Solutions for Supply Chain Management–Navision

- Vendor: Microsoft
- Product URL: http://www.microsoft.com/BusinessSolutions/Navision/supplychain.aspx

Sales

Product Name: Microsoft Business Solutions- Axapta Sales and Marketing

- Vendor: Microsoft
- Product URL: http://www.microsoft.com/BusinessSolutions/Axapta/salesmarketing.aspx

Warehousing and Distribution

Product Name: Microsoft Business Solutions for Distribution–Great Plains

- Vendor: Microsoft
- Product URL: http://www.microsoft.com/BusinessSolutions/GreatPlains/distribution.aspx

e-Advertising

None Chosen

3. Platform Recommendations

The computing platforms (Hardware/Software) are selected based on the type of work and workgroup. The following tables shows computing platforms selected:

Site # 1:

SITE1

Server Configuration		
Type	**Configuration**	**Business Software**

DataBase Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 Server	✔ MS SQL Server (*by* MicroSoft)

Server Configuration		
Type	**Configuration**	**Business Software**
Email Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 Server	✔ MS Exchange Server (*by* MicroSoft)

Server Configuration		
Type	**Configuration**	**Business Software**
Application Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 (84824su) Server (Pentium 4 3.2 GHz, 512 MB (DDR SDRAM), 80 GB HDD)	✔ Microsoft Business Solutions for Field Service Management (*by* Microsoft) ✔ Oracle E-Business Suite Logistics (*by* Oracle) ✔ Microsoft Business Solutions for Supply Chain Management–Navision (*by* Microsoft)

Business Function: Corporate Management

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Customer Support and CRM

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Logistics

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Marketing

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Production

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Supply Chain Management

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Site # 1:

SITE2

Server Configuration		
Type	**Configuration**	**Business Software**
DataBase Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 Server	✔ MS SQL Server (*by* MicroSoft)

Server Configuration		
Type	**Configuration**	**Business Software**
Email Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 Server	✔ MS Exchange Server (*by* MicroSoft)

Server Configuration		
Type	**Configuration**	**Business Software**
Application Server	**OS:** Microsoft Windows Server 2003 **Hardware:** IBM xSeries 206 (84824su) Server (Pentium 4 3.2 GHz, 512 MB (DDR SDRAM), 80 GB HDD)	✔ Microsoft Business Solutions for Financial Management-Axapta (*by* Microsoft) ✔ Microsoft Business Solutions for HR Management - Axapta (*by* Microsoft) ✔ Microsoft Business Solutions-Axapta Sales and Marketing (*by* Microsoft)

		✔ Microsoft Business Solutions for Distribution–Great Plains (*by* Microsoft)	

Business Function: Finance and Accounting

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Human Resource Management

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Sales

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: Warehousing and Distribution

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

Business Function: e-Advertising

Title	qty	Configuration	Software (Applications + Middleware)
Manager	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Knowledge Worker	2	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0
Operator	1	**Type:** wired **Hardware:** Dell Dimension 4400 **OS:** Microsoft Windows 2000	▸ MS Office XP ▸ MS Outlook Express ▸ MS Internet Explorer 6.0

4. Network Plan

Network Summary

The network recommendations are selected based on the organization design, the type of work being done at various sites, and the workload.
The following table and diagram shows the network configuration you have selected:

#	Campus	Users (Wired+Wireless=)Total	Bandwidth
1	site1	(24+0=)24	17520 kbps
2	site2	(20+0=)20	14600 kbps

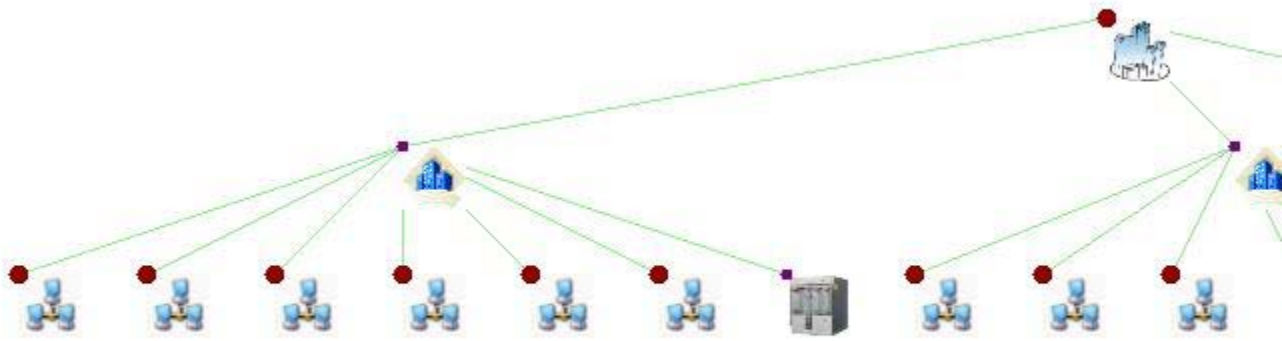


Figure: Network Diagram

#	Campus	Connection
1	site1	▸ Wireless Local Loop (LMDS) **Data Rate:** *37000kbps*
2	site2	▸ Wireless Local Loop (LMDS) **Data Rate:** *37000kbps*

#	COTS Selected	Features	Usage
1	Alcatel 7390 LMDS Network Termination	**Vendor:** *Alcatel*	**Location:** *site1*
2	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ CM* **Devices Attached:** *4* **Load:** *5.84Mbps*
3	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ CM* **Devices Attached:** *1*
4	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ CSrv* **Devices Attached:** *4* **Load:** *5.84Mbps*

5	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ CSrv* **Devices Attached:** *1*
6	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ Log* **Devices Attached:** *4* **Load:** *5.84Mbps*
7	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ Log* **Devices Attached:** *1*
8	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ MR* **Devices Attached:** *4* **Load:** *5.84Mbps*
9	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ MR* **Devices Attached:** *1*
10	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ Prod* **Devices Attached:** *4* **Load:** *5.84Mbps*
11	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ Prod* **Devices Attached:** *1*
12	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site1/ SCM* **Devices Attached:** *4* **Load:** *5.84Mbps*
13	3Com NJ 100 Network Jack -	**Type:** *Group level switch*	**Location:** *site1/ SCM*

	switch - 4 ports	**Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Devices Attached:** *1*
14	10/100 16-Port VPN Router	**Type:** *Campus level Router* **Ports:** *16* **Data Rate:** *100Mbps* **Vendor:** *Linksys Inc.* **Other Features:** *- Dinial of service ressistance* *- Firewall* *- VPN PassThrough*	**Location:** *site1* **Devices Attached:** *10*
15	Alcatel 7390 LMDS Network Termination	**Vendor:** *Alcatel*	**Location:** *site2*
16	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ FA* **Devices Attached:** *4* **Load:** *5.84Mbps*
17	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ FA* **Devices Attached:** *1*
18	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ HR* **Devices Attached:** *4* **Load:** *5.84Mbps*
19	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ HR* **Devices Attached:** *1*
20	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ SL* **Devices Attached:** *4* **Load:** *5.84Mbps*
21	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:**	**Location:** *site2/ SL* **Devices Attached:** *1*

		- Replicated to reduce Congession	
22	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ WD* **Devices Attached:** *4* **Load:** *5.84Mbps*
23	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ WD* **Devices Attached:** *1*
24	OFFICECONNECT ENET HUB 4	**Type:** *Hub* **Ports:** *4* **Data Rate:** *10Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ web1* **Devices Attached:** *4* **Load:** *5.84Mbps*
25	3Com NJ 100 Network Jack - switch - 4 ports	**Type:** *Group level switch* **Ports:** *4* **Data Rate:** *100Mbps* **Vendor:** *3Com Corp.* **Other Features:** *- Replicated to reduce Congession*	**Location:** *site2/ web1* **Devices Attached:** *1*
26	10/100 16-Port VPN Router	**Type:** *Campus level Router* **Ports:** *16* **Data Rate:** *100Mbps* **Vendor:** *Linksys Inc.* **Other Features:** *- Dinial of service ressistance* *- Firewall* *- VPN PassThrough*	**Location:** *site2* **Devices Attached:** *9*

5. Security Plan

Summary of Results

Different types of security choices are made in organizations
The following table shows the Security solutions you have selected:

Object type	Weakness	Solutions

Hub	Device is not placed in a secure Location	▸ Protect the network device by placing in a controlled area
Hub	No Authorization Required for access	▸ Turn id/pw on for Device access
Hub	Too much workload to allow jamming	▸ Replicate to avoid jamming
Switch	Device is not placed in a secure Location	▸ Protect the network device by placing in a controlled area
Switch	No Authorization Required for access	▸ Turn id/pw on for Device access
Switch	Too much workload to allow jamming	▸ Replicate to avoid jamming
Router	Device is not placed in a secure Location	▸ Protect the network device by placing in a controlled area
Router	No Authorization Required for access	▸ Turn id/pw on for Device access ▸ Use ACLs at network device that are highly protected
Router	Too much workload to allow jamming	▸ Replicate to avoid jamming ▸ Move to a more jamming resistant network such as IPV6
Wired Host	Unauthorized access to root password/ID	▸ keep rooid ID/pw under strong security ▸ require strong authentication for root ID/pw
Wired Host	Inherent weaknesses and bugs in OS	▸ install latest security patches ▸ Add FireWall
Application Server	Weak password or placed in obvious places	▸ Strong pw/id protection of application ▸ Additional PW for database access within the application ▸ Extremely strong, multilayered (with biometrics) authentication
Application Server	Application directly accessible from the Internet	▸ Add FireWall ▸ Replicated applications (if one is not available, the other takes over) ▸ Fragmented, replicated, and scattered (FRS) application so that no application goes down completely
Application Server	Unauthorized access to root password/ID	▸ keep rooid ID/pw under strong security ▸ require strong authentication for root ID/pw ▸ Harden the OS so that no program can go into supervisory mode
Application Server	Inherent weaknesses and bugs in OS	▸ install latest security patches ▸ Add FireWall ▸ Install Honeypots

AUDIT AND CONTROL CHECKLIST

A comprehensive checklist is essential for information security audits and controls. The following links show you various checklists that you can use to monitor, audit and control the technical as well as management aspects of your security:

The checklist is extracted from the book ("Information Security and Auditing in the Digital Age", A. Umar, NGE Solutions, 2004). It can be customized and expanded/reduced to take into account the following factors: type of company, size of company, specialized situations such as international trade. The checklist is written so that it can be filled out by an auditor. For each item, the answer may be yes, no, or some explanation (e.g., not needed, covered by another category, etc). After reviewing this checklist as part of an audit, the auditor would prepare a risk assessment report to highlight the main risk and suggest future steps.

Color coding

The segments in Customized Checklist are color coded to represent the following:

- If the segment is ***"Black"***, no change needed to this segment
- If the segment is ***"Blue"***, you can reduce this segment or even remove it according to your requirement
- If the segment is ***"Red"***, you may need to expand this segment according to your requirements

1.2. Organizational Controls and Security Administration

These controls are intended for the entire firm and address the organizational structures, policies and procedures.

1.2.1. Documentation of the Information Systems Strategic Plan

- Management has developed and implemented long and short term plans that identify and fulfill the organizations strategies _____
- Information systems security is adequately addressed in the organizations long- and short-term plans _____
- The management of the information systems security was established and applied using a structured approach _____

1.2.2. Information Security Policies and Procedures

- Information security policies exist _____
- These policies are adequate to address Privacy, Integrity, Authorization, Authentication, and Availability (PIA4) in the following areas (circle the ones that are NOT adequately covered by the policies):
    - Web pages
    - Firewalls
    - Employee Surveillance
    - Electronic Banking
    - Viruses
    - Encryption
    - Digital Signatures/Certificates
    - Contingency Planning
    - Laptops/Portable
    - Logging Controls
    - Internet/Intranet
    - Privacy
    - Emergency Response
    - Micro-computers
    - LAN
    - Passwords
    - E-mail
    - Data Classification
    - Telecommuting
    - User Training
    - Ethics
- Procedures and practices are used by the ISSO to monitor compliance with the above policies _____
- Ensure the ISSO has been given the positional authority to address policy violations, or reports to an appropriate level of management _____
- Documented actions taken to address recent policy violations _____

1.2.3. Risk Assessment/Ongoing Analysis

- A framework exists to assess information security risks _____
- A methodology adopted for risk assessment _____
- Responsibility assigned for periodically performing risk analysis _____
- Risk assessment methodology adequately defines essential elements of risk, provides a qualitative/quantitative measurement of risk, and addresses acceptable risk conclusions _____
- Risk assessment is appropriately reported to senior management _____
- Action plan allows for the acceptance of the residual risks (risks that cannot be controlled) by the management _____
- Adequate insurance coverage for the residual risks has been obtained _____

1.2.4. Information Security Organizational (ISSO) Structure

- The reporting structure and placement of the ISSO function within the organization is defined _____
- The position is responsible to the appropriate level of management and is appropriately separated from the IS department _____
- Management has defined and implemented security levels related to the sensitivity of specific corporate information _____

1.2.5. Information Security Staffing

- Position descriptions exist for the information security position _____
- Position descriptions consistent with the ISSO responsibilities _____
- Staffing levels adequate in the information security environment _____

1.2.6. Compliance Requirements

- External compliance considerations (e.g., government regulations) documented (crucial for healthcare and government agencies) _____
- Impact of external relationships (e.g., partnerships) on compliance requirements, has been assessed _____
- Appropriate and timely corrective actions have been taken for information security deficiencies in compliance examinations, regulatory reviews, and/or audits conducted so far _____

1.3. Physical and Environmental Security

1.3.1. Secure Area

Objective is to prevent unauthorized access, damage and interference to business premises and information.

- Security Perimeters have been established to protect physical and IT assets (i.e., buildings with doors) _____
- Protected entry controls, such as the following, have been established to ensure that only authorized personnel are allowed access _____
    - Badges
    - Limited access to buildings
    - Guards on entrance doors
    - Properly secured and tamper proof wiring
    - Alarm doors
- Suitable intruder detection systems are installed for this area _____
- Additional controls established for personnel or third parties (i.e., aware of activities in a secure area on a needs to know basis only) _____
- Controls are in place for the delivery and loading areas _____
- Access from outside is restricted to formally authorized and identified personnel only _____
- External door is secured when the internal door is opened _____
- Packages checked for potential hazards before it is moved from the holding area to the point of use _____

1.3.2. Equipment Security

Objective is to prevent loss, damage or compromise of assets and interruption to business activities.

- Equipment is sited to reduce minimum unnecessary access into work areas _____
- Controls are in place to minimize the risk of theft, fire, explosions, smoke, water, dust, vibration, chemical effects, electrical supply interference and electromagnetic radiation _____
- A policy exists towards drinking, eating and smoking in proximity to information processing facilities _____
- Suitable electrical supplies are available should there be a power failure (i.e backup generator, UPS etc) _____

- Controls exist to ensure that power and telecommunications cabling is protected from interception or damage _____
- Equipment maintenance is done periodically _____
- Only authorized maintenance personnel carry out repairs and service _____
- Records kept of all suspected or actual faults _____
- Adequate insurance in place to protect equipment taken off -site _____
- Controls on authorized equipment exist for off site _____
- Sensitive information securely destroyed from retired equipment _____
- Name of the contractors recorded who get the retired equipment _____
- Fixed hard disks checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal _____

1.3.3. General Controls

Objective is to prevent compromise or theft of information and information processing facilities.

- A Clear (or Secure) Desk Policy or a Clean screen policy exists _____
- Other measures to reduce the risk of unauthorized access, loss/damage to information during and outside normal working hours _____
- Procedures in place to prevent unauthorized removal of property _____
- Spot checks in place _____

1.4. Operation Management

1.4.1. Production procedures and responsibilities

Objective is to ensure the correct and secure operations of information processing facilities.

1.4.1.1. Operating Procedures.

- Documented procedures exist that include instructions for each job _____.
- Procedures include the following:
    - Processing and handling of information _____
    - Scheduling requirements _____
    - Instructions for handling errors or other exceptional conditions _____
    - Support contacts _____

- Special output handling instructions _____
- System restarts and recovery procedures. _____
- Close down procedures _____
- Back-up procedures _____
- Computer room safety procedures _____

1.4.1.2. Production Change Control

Production programs should be subject to strict change control. The following items should be considered:

- An audit log containing all relevant information is retained _____
- Identification and recording of significant changes _____
- Assessment of the potential impact of such changes _____
- Formal approval procedure for proposed changes _____
- Communication of change details to relevant persons _____
- Identification of responsibilities for aborting and recovering from unsuccessful changes _____

1.4.1.3. Incident Management Procedures

a) Procedures for security incident including

- Procedures for information system failures and loss of service _____
- Denial of service _____
- Errors resulting from incomplete or inaccurate business data. _____
- Breaches of confidentiality _____

b) Actions to recover from security breaches and correct system failures that state: :

- Only authorized staff are allowed access to live system and data. _____
- All emergency actions are documented in detail _____
- Emergency action is reported to management _____
- Integrity of business systems and controls is confirmed with minimal delay. _____

1.4.1.4. Segregation of Duties

- Identification of activities which could be basis of fraud and/or crime

- To avoid collusion, duties have been segregated to ensure that 2 or more persons are involved

1.4.1.5. Separation of Development and Production Facilities.

- Separate facilities for development and production software _____.
- Different logon procedures for test and production systems to reduce risk of error and production problems _____

1.4.2. System Planning and Acceptance

Objective is to minimize the risk of systems failure.

1.4.2.1. Capacity Planning

- A capacity plan exists _____
- Critical components are included in the capacity plan _____

1.4.2.2. System Acceptance

- Acceptance criteria for new information systems, upgrades and new versions has been established _____
- Tests of the systems specified prior to acceptance _____.
- For major new development, the operations function and users consulted at all stages in the development _____
- Requirements and criteria for acceptance include the following:
    - Performance and computer capacity requirements _____
    - Error recovery and restart procedures and contingency plans _____
    - Testing of operating procedures to defined standards _____
    - Agreed set of security controls for new systems _____
    - Effective manual procedures in case of automation failure
    - Business continuity arrangements for new systems
    - Testing to show that the new system will not adversely effect existing systems particularly at peak processing times _____
    - Testing of the new system to understand security implications _____

1.4.3. Protection Against Malicious Software

Objective is to protect the integrity of software and information

Controls against malicious software should include:

- Policy prohibiting the use of unauthorized software _____
- Policy to protect against obtaining files and software from untrusted sources _____.
- Installation and regular update of anti-virus detection and repair of software _____
- Regular reviews of the software and data content of systems supporting critical business processes _____
- Procedures for checking files or programs for viruses before use _____
- Checking electronic mail attachments and downloads for malicious software before use _____
- Procedures for virus protection on systems, training in their use, reporting and recovering from virus attacks _____
- Business continuity plans for recovering from virus attacks _____
- Procedures to verify all information relating to malicious software before issuing warning bulletins _____

1.4.4. Housekeeping (Traditional, Mainframe Systems)

Objective is to maintain integrity and availability of information processing and communication services.

1.4.4.1. Information Back-up

- Back-up arrangement documented in restoration procedures _____
- Back-up information stored in a remote location _____
- At least 3 generation or cycles of back-up information is retained for important business applications _____
- Back-up/restore procedures tested to ensure that they will work in emergency situations _____

1.4.4.2. Operator Logs

- Operation logs of the system activities exist _____
- Logs contain critical data (e.g., start finish times, system errors and corrective action taken, name of the person making the log entry) _____
- Logs are subject to regular, independent checks against operating procedures _____

1.4.4.3. Fault Logging

- Fault logs show that all have been satisfactorily resolved _____
- Corrective measures exist to ensure that controls have not been compromised by personnel _____

- Actions taken to handle faults are fully authorized _____

1.4.5. Media Handling and Security

Objective is to prevent damage to assets and interruptions to business activities. Media should be controlled and physically protected.

1.4.5.1. Management of Removable Computer Media

Objective is to protect removable media such as tapes, disks, cassettes and printed reports.

- Contents of any re-usable media with highly sensitive information that are to be removed from the organization are erased _____
- Authorization is required and an audit trail is kept of all highly sensitive removable media _____
- Sensitive media stored in a safe, secure _____
- Procedures for disposal of sensitive media _____

1.4.5.2. Information Handling Procedures

- Procedures in place for handling and storing of sensitive information
- Controls in place for:
    - Handling and labeling of all media _____
    - Access restrictions to identify unauthorized personnel _____
    - Maintenance of a formal record of the authorized recipients of data _____
    - Ensuring that input, processing, and output is validated and verified for sensitive applications _____
    - Protection of spooled data is at a level consistent with sensitivity _____
    - Storage of media in secure areas _____
    - Keeping the distribution of data to a minimum _____
    - Review of distribution lists and lists of authorized recipients at regular intervals.

1.4.5.3. Security of System Documentation

- Systems documentation stored securely _____
- The access list for systems documentation kept to a minimum _____
- System documentation not held on a public or unsecure network _____

1.5. Enterprise Level Access Controls

1.5.1. Business Requirement for Access Control

Objective is to control access to Information

The access control policy should state:

- Security requirements for each application _____
- Standard user profiles for common categories of job _____
- Management access rights in a network environment _____

1.5.2. User Access Management

Objective is to prevent unauthorized access to information systems.

1.5.2.1. Access Set-up/Removal/Review

- Procedures and standards exist to grant access to new hires, department transfers, vendors, and consultants _____
- Procedures and standards to remove access from terminated employees, transferred employees, and discontinued vendors _____
- The access lists are reviewed for the sensitive systems _____
- Someone has the "ownership" of the user access reviews _____

1.5.2.2. User Registration

- A formal procedure exists for granting access to all information systems and services
- Use of unique user ID so they are responsible for actions _____
- Separate approval for access rights from management _____
- Checking that the access given is appropriate for the business purpose giving users a written statement of their access rights _____
- Requiring users to sign the statement so they understand the conditions of their access _____
- Maintaining a register of all persons registered to use the service _____
- Periodically checking for removing redundant User Id's from access _____
- Ensuring that redundant user IDs are not issued to other users _____

1.5.2.3. Privilege Management

- Controls in place to disallow un-authorized users to override system or application controls _____

- A formal management process in place re the allocation of passwords _____
- Review of user access rights done reviewed on a regular basis ie every 6 months _____

1.5.3. User Responsibilities

Objective is to prevent unauthorized user access.

- Users advised of the security practices to be followed re Passwords (i.e., keep confidential, avoid keeping a paper record, do not share passwords) _____
- Users advised to ensure that unattended equipment has appropriate protection:
    - Terminate active sessions when finished _____
    - Logoff mainframe systems when session finished _____
    - Secure PC's or terminals by a key lock or password access when not in use _____

1.6. System Development and Maintenance

1.6.1. Security Requirements of System

- Organization requires that security is built into the information system _____
- Security requirements analyzed and specified at the design state of new system or enhancement to existing system _____

1.6.2. Cryptographic Controls

Objective to protect the confidentiality, authenticity or integrity of information.

- Policy exists on the use of cryptographic controls (i.e., encryption) for the protection of sensitive information _____
- Digital signatures are used for authentication where needed _____
- Asymmetric encryption used where appropriate _____
- Non-repudiation services used where needed to resolve disputes involving the use of a digital signature on an electronic contract or payment _____
- Proper key management system such as PKI used _____

1.6.3. Security of System Files

Objective is to ensure that IT projects and support activities are conducted in a secure manner.

1.6.3.1. Controlof Production software

- Updating of operational program libraries is only performed by the nominated librarian _____
- Operational systems only hold executable code (source code not included for security purposes) _____
- Executable code is not implemented on operational system without evidence of successful testing _____
- An audit log is maintained of all updates to operational program libraries _____
- Previous versions of software is retained as a contingency measure _____
- Vendor supplied software is maintained at the level supported by the supplier _____

1.6.3.2. Protection of System Test Data

The following are put in place to protect production data when used for testing:

- The access control procedures, which apply to production application systems, also apply to test application systems _____
- Separate authorization needed each time production information is copied to a test application system _____
- Production information is erased after testing is completed _____
- Copying and use of production information is logged for audit trails _____

1.6.3.3. Access Controls to Program Source Library

The following controls are in place to protect potential corruption of computer programs in the source library:

- Program source libraries are not held on the operational systems _____
- A program librarian has been be assigned for all sensitive applications _____
- IT support staff does not have unrestricted access to program source libraries _____
- Programs under development or maintenance are not held in production program source libraries _____
- Updating of program source libraries and issuing of program sources to programmers is only performed by the authorized librarian _____
- Program listings are held in a secure environment _____

1.6.4. Security in Development and Support Processes

Objective is to maintain the security of application system software and information.

- Change control procedures are in place to ensure security and control procedures are not compromised _____
- Periodic technical reviews are completed of all operating changes _____
- Restrictions exist on changes to vendor software packages (e.g., vendor consent before changes, someone who will maintain future maintenance) _____
- Protection in place for backdoors and Trojan code through careful buying practices (i.e., buying programs from reputable vendors) and inspections of source code before production use _____

1.7. Business Continuity Management

Objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failure or disaster.

- A business continuity plan is in place to cover your business _____
- Redundancy and fault tolerance has been built into the systems to minimize the impact of attacks _____
- The continuity plan contains the following:
    - Identification of attacks (natural, malicious)_____
    - Key personnel responsible for responding to attacks _____
    - System to notify the key personnel _____
    - Offsite location for system backups _____
    - Offsite location for system operation _____
    - Physical arrangements (personnel moved to off-sites, hotel accommodations in the target areas, etc) _____
    - Other considerations (specify) _____
- The plan is reviewed periodically _____
- Plan tested and exercised periodically _____
- Key personnel familiar with the plan and any changes _____

1.8. Compliance

1.8.1. Compliance with Legal Requirements

Objective is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual.

- Intellectual property rights, copyrights, and trademarks are complied with through procedures _____

- Proprietary software is registered under license agreements that limits the use of the products to specified machines _____
- Safeguarding of organizational records is in place to ensure their use within regulatory retention periods _____
- Cryptographic keys associated with encrypted archives or digital signatures are kept securely _____
- Data protection and Privacy Laws are adhered to _____
- A data protection officer has been assigned _____
- Cryptographic controls have been implemented which include:
    - Import and/or export of computer hardware and software for performing cryptographic functions _____
    - Import and/or export of computer hardware and software which is designed to have cryptographic functions added to it _____
    - Mandatory and discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content _____

1.9. Application Controls

Application controls concentrate on individual (usually sensitive and critical) applications and encompass the whole sequence of application processing.

1.9.1. Application Access Controls

Objective is to prevent un-authorized access to information held in application systems.

- Access controls are in place to ensure users are restricted to Read, Write, Execute, Delete based on the organizational information access policy _____
- Organization has a dedicated (isolated) computing environment for hihly sensitive systems _____

1.9.2. Exchanges of Information and Software

Objective is to prevent loss, modification or misuse of information exchanged between organizations.

- Information and software exchange agreements verified before exchange of critical information and software between organizations _____
- E-commerce security in place to protect from threats such as fraudulent activity, contract dispute, and disclosure or modification of information _____
- Security of sensitive electronic mail is enforced through packages such as PGP, MIME, or others _____

- Security of electronic office systems (e.g., word documents) is enforced through guidelines, policies, and technologies _____
- Publicly available systems are protected through policies and technologies _____
- Security of media in transit is enforced through:
    - Reliable transport/courier company used _____
    - Packaging to protect the contents from physical damage _____
    - Special controls to protect sensitive information (i.e., use of locked containers, delivery by hand, tamper evidence packaging, splitting of the consignment to take different routes, use of digital signature and confidential encryption) _____

1.9.3. Input, Output and Processing Controls in Application Systems

Objective is to prevent loss, modification or misuse of user data in application systems.

- Data validation (input edit) is in place to ensure that data input is correct and appropriate before processing _____
- Validation checks are incorporated into systems to detect corruption by processing errors or through deliberate acts _____
- Authorization controls are in place to verify the authority of input providers _____
- Data conversion controls are in place to minimize conversion errors as data is transcribed from one form to another _____
- Checks and controls are in place to reconcile data file balances after transaction updates and software download/upload _____
- Application processing controls are in place to include the following:
    - Matching controls that compare the input data with information held on system files. _____
    - Processing edits to verify for reasonableness or consistency during processing of applications_____
    - Control totals during processing to reconcile the input control totals with the totals of items processed _____
- Data produced by an application system is validated to ensure the processing of stored information is correct. This validation may include:
    - Checks to test whether the output data is reasonable _____
    - Reconciliation control counts to ensure processing of all data _____
    - Providing sufficient information for a reader or subsequent processing system to determine the accuracy and completeness of the information _____

- Procedures for responding to output validation tests _____
- Identifying the personnel involved in the data output process _____

- Periodic synching and checking of outputs is done with actuals _____
- Message authentication is implemented in hardware or software for sensitive message exchanges _____
- Message authentication is required where needed _____

1.9.4. Controls for XML-based Applications

This is a new area of work in which the XML document itself but also the DTD are also properly controlled.

- Sensitive XML documents are encrypted by using XML Encryption, XML Signatures or other suitable schemes _____
- DTDs of sensitive XML documents are properly controlled so that only authorized personnel can update them _____

1.9.5. Application and Shared Data Security Controls

- Additional sets of passwords and security restrictions are in place for sensitive applications _____
- Additional sets of passwords and security restrictions are in place for sensitive applications _____
- Security profiles have been created to allow different people different access (e.g., online users, medical record processing, etc) _____:
- These profiles are established and maintained by a data security system _____.

1.9.6. Controls on Mobile and Web Services Applications

The objective is to properly control the mobile client, Web tier, and the back-end transaction control issues for mobile applications.

- Mobile clients are authenticated before they can invoke applications _____
- Security checks are done at the wireless gateway (e.g., WAP Gateway) _____
- Transactions have proper controls for remote invocations _____
- Proper controls for Web Services applications are in place:
  - Services defined with WSDL have been properly checked _____
  - Services advertised through UDDI are properly checked _____

1.10. Network Security Controls

Objective is to ensure the safeguarding of information in networks and the prevention of the supporting infrastructure.

1.10.1. Network Access Controls

Objective is protection of networked services:

- There is a security policy concerning the network and network services in the enterprise _____
- Policy indicates the network and network services allowed to be accessed, authorization procedures for determining who is allowed access to which networks and networked services _____
- Only restricted paths (e.g., dedicated and/or encrypted lines, security firewalls, limited menu and submenu options for users) allowed to sensitive databases and programs _____
- User authentication for remote users for external connections _____
- Segregation of networks (separate logical network domains, firewalls) is in place _____
- Network connection controls exist for electronic mail, file transfers, interactive access, etc. _____
- Network routing controls exist for isolating networks and preventing routes to propagate from the network of one organization into the network of another _____
- Public Internet access used to access corporate resources _____
- VPN used for external network access _____
- A warning message is initiated for users accessing the proprietary network. The wordings may be "You have connected to a proprietary system. Only authorized users may access this system. Access by unauthorized individuals is prohibited and will be prosecuted to the full extent of the law. This system is monitored for unauthorized usage." _____

1.10.2. Network Firewalls and Controls

- A firewall policy is in place _____
- Firewall does the following type of filtering:
    - Packet filtering _____
    - Application filtering_____
    - File transfer filtering _____
    - Other filters (specify) _____

- Firewall rules are kept in a secure area and can only be modified by authorized personnel _____
- Responsibility for network firewall security is separated from computer operations where appropriate _____
- Responsibilities and procedures for the management of remote equipment has been established _____
- Special controls have been established for confidentiality and integrity of data passing over public networks _____

1.10.3. Remote Access Service (RAS) Controls

- Remote Access Services (RAS) is installed on the server being reviewed _____
- Remote access authorization is granted based on corporate standards _____
- Remote access is granted within the job function _____
- Encryption has been set on all RAS logon and authentication information _____
- Remote access users are monitored and reviewed _____

1.11. Server Platforms Controls

1.11.1. Overview

Most organizations at present have servers that are dispersed to different organizational units. Some of these servers are used for departmental or regional computing. For example, a regional office in Atlanta may have a server that handles all the applications and databases at Atlanta. Some servers are used for specialized purposes such as email servers, portal servers, database servers, etc. Although the overall administrative controls discussed previously apply to these servers, the following checklists are intended to assure that these servers are also under proper controls. Some checklists will appear to be redundant with previous lists but they have a different purpose ? controls on servers and their compliance to the corporate standards and policies. This is a general procedure that can be and should be customized for different types of server platforms such as Windows NT, XP, 200x, Linux, Unix, and others.

1.11.2. Server Security Administration

- Someone is responsible for operating system administration and maintenance for the platforms _____
- Administrators are made aware of system standards and Information Security Standards _____
- System and security administration procedures have been formally documented and up-to-date _____

- The following standards are being followed:
    - A standard naming convention is being used _____
    - Each user is assigned a unique user id _____.
    - Group IDs and shared/generic account should not be used _____.
    - The system has been configured to authenticate all users through a valid ID and password
- Procedures are in place to review server configuration using commercially available tools _____
- Procedures are in place to ensure that system level accounts are disabled and/or removed for terminated employees _____
- Procedures are in place to ensure that user system access rights are appropriately modified for transferred employees _____
- Human Resources department provides security administration personnel with periodic reports of terminated and transferred employees _____
- Global password rules have been established by setting appropriate account policies. Examples of the rules are:
    - Minimum Password Age (allow changes in 1 day)
    - Maximum Password Age(60 days)
    - Minimum password length (6 characters)
    - Account Lockout (allow 3 bad attempts)
    - Account Lockout (reset count in 1440 minutes)
    - Lockout Duration (Forever)
    - Password History (Remember 3 passwords)

1.11.3. Monitoring System Access and Use

Objective is to detect unauthorized activities.

- Audit logs of event logging is being kept for an agreed period _____
- Audit logs contain User Id's. dates & times for logon, logoff, terminal identification or location if possible, records of successful and rejected systems, data, and other resource access attempts _____
- Procedures are set for monitoring the use of information processing facilities _____
- Results of the monitoring are reviewed regularly to assess risk factors _____
- System clocks are reviewed to ensure accuracy (correct setting of computer clocks is important to ensure the accuracy of audit logs) _____

1.11.4. Operating System Access Controls

Objective is to prevent unauthorized computer access.

- Automatic terminal identification in place to authenticate connections to specific locations and to portable equipment _____
- Logon procedure not display system or application identification until logon successfully completed _____
- A general notice is displayed that the computer should only be accessed by authorized users _____
- Number of unsuccessful logon attempts is limited to 3 _____
- Unsuccessful attempts are recorded rigorously _____
- The password management system:
    - Enforces the use of individual passwords to maintain accountability _____
    - Allow users to select and change their own passwords _____
    - Enforces a choice of quality passwords _____
    - Enforces password changes periodically (e.g., passwords expire once a month or twice a year) _____
    - Stores password files separately to application system data _____
    - Stores passwords in encrypted form _____
    - Alters default vendor passwords following installation of software _____

1.11.5. User Accounts

- Guest account has been disabled _____
- Administrator account has been renamed to stop intruders from accessing this account _____
- Strong password has been set for the administrator accounts _____
- Administrator has his unique account assigned to only him, and not shared by other administrators _____
- Logon scripts are secured with restricted access permission _____
- User is required to change the password at the time of initial logon _____
- Length of time restrictions are placed on system accounts provided to contractors and temporary workers _____

1.11.6. Groups

- A structure exists to group user IDs by department or job functions in order to be efficiently administered by security _____
- The rights have been assigned to the global groups and the group membership and privileges are appropriate _____
- The rights have been assigned to the local groups. Verify that group membership and privileges are appropriate _____
- There is a business purpose for each global group _____
- There is a business purpose for each local group _____
- The number of users with privileged access is limited _____

1.11.7. User Rights

- Standard user access rights (read, write, execute) specified _____
- Any user given rights outside standard require special authorization _____
- Periodic review of user access rights in place to ensure that access rights remain commensurate with user job responsibilities _____
- Audit software is used as part of the regular reviews _____

1.11.8. System Registry Security

- File and directory permissions are appropriate for groups with access _____
- Permissions set for the critical Registry keys are configured to recommended standards _____

1.11.9. Operating System Configuration

- Formal procedures are in place over the installation of new servers to ensure the consistency of operating system configuration settings throughout the processing environment _____
- Formal standards and procedures are in place over the implementation of operating system upgrades _____
- Operating system installations/upgrades are thoroughly tested and hardened before being loaded into the production environment _____
- Fallback procedures are in place for operating system upgrades _____
- Controls are in place to ensure that operating system security configuration changes are authorized and approved _____
- Records are maintained to document all modifications and fixes to operating system security _____

- Secure passwords for predefined system accounts (i.e., Administrator, Guest, etc.) are assigned immediately upon installation or upgrade _____
- Powerful system utilities that assist system administrators (i.e., disk management, system registry editing, etc) are appropriately restricted to authorized system personnel only _____
- Appropriate trust relationships have been established based on corporate standards _____
- Formal standards and procedures exist over the configuration of security at the directory and file level _____
- Key system directories are secured _____
- Access to key system directories is restricted to system administration personnel _____
- Permissions assigned to shared resources within the environment have been restricted _____

1.11.10. File and Directory Protection

- Critical production application directories, subdirectories, and files have been identified _____
- Critical directory and file permissions are set based on corporate standards _____
- Users are not granted access to modify key system programs _____

1.11.11. Monitoring/Auditing/Reporting

- Systems have been configured to log audit events such as:
    - Log-on and log-off activity (failure) _____
    - Security policy changes (failure) _____
    - Restart and Shutdown (failure) _____
- System audit log files are secured _____
- Audit logs are backed up on a regular basis _____
- Audit logs are reviewed by appropriate security/system administration personnel on a regular basis _____
- Escalation procedures are in place to ensure that detected security events are appropriately investigated in a timely manner _____
- Reports are produced to evaluate trends in the audit log information _____
- Procedures established to prevent, detect, and recover from computer viruses _____
- Invalid attempts to exercise administrative rights are tracked _____

1.11.12.Server Backup Recovery

- Backup and recovery procedures are in place _____

1.11.13.Server Physical Security

- Critical servers are physically secured from unauthorized access.

1.12. Additional IT Infrastructure Controls

These controls are overall controls governing the organization's information technology infrastructure. The following starter checklist can be extended considerably. :

- Database management system resources, such as Oracle and SQL Server dictionaries are properly protected _____
- IDEs (Integrated Development Environments) such as IBM's Websphere Studio and Microsoft's .NET Visual Studio are properly protected from potential attacks and failures _____.
- Middleware services are placed in protected areas with proper authentication and authorization controls _____
- The integrity of application servers is protected against compromised. _____
- Controls in place to ensure that computer hardware is physically secure and can be accessed only by authorized individuals _____

