Evaluation of IT management practices
Intended for the company *SPECIMEN SA*
Evaluation report

Final report of the evaluation relating to:

- **the quality of the computer infrastructure, concerning hardware as well as software, and the positioning of technological choices;**
- **the support received by the users (helpdesk), change management, management of configurations and versions;**
- **information system security: data protection and integrity;**
- **document management;**
- **management of the information system: project management, management of acquisitions and suppliers, financial management;**

Author(s): Xxxxxxxxxx Xxxxxxxxxx

Date: xx/xx/20xx **Evaluation on xx/xx/20xx**
Technical audit and inventory on xx/xx/20xx
Report presented on xx/xx/20xx
Reference: **Rapport Evaluation NOEMI V_01.doc**

Distribution:

Validation:

Revised by: **Date:**
Comments:

Document history:

Version	Initiator of changes	Modifications	Date	Author(s)
0_1	Initial version	Draft	xx/xx/20xx	Xxxx Xxxxxxxx
0_2	Xxxx Xxxxxxx	Review and validation	xx/xx/20xx	Xxxx Xxxxxxxx
0_3				

SPECIMEN

Table of contents

1. Context 3
2. Approach ..... Error! Bookmark not defined.
3. Evaluation of the management practices ..... Error! Bookmark not defined.
   3.1 Summary 6
   3.2 Detailed report 7
      3.2.1 Acquisition management ..... Error! Bookmark not defined.
      3.2.2 Project management 7
      3.2.3 Suppliers management 7
      3.2.4 Financial management 7
      3.2.5 Service level management. 7
   3.3 Recommendations 9
4. Evaluation of the support practices ..... Error! Bookmark not defined.
   4.1 Summary 10
   4.2 Detailed report 11
      4.2.1 Problem and incident management (helpdesk) 11
      4.2.2 Management of configurations and versions 12
      4.2.3 Level of satisfaction 12
   4.3 Recommendations 13
5. Evaluation of the IT infrastructure ..... Error! Bookmark not defined.
   5.1 Summary 14
   5.2 Detailed report 15
      5.2.1 Analysis of passive devices 15
      5.2.2 Network analysis 16
      5.2.3 Servers 18
      5.2.4 PCs 18
      5.2.5 Printers. 19
      5.2.6 Groupware infrastructure 19
   5.3 Recommendations 21
6. Evaluation of the security practices 22
   6.1 Summary 23
   6.2 Detailed report 25
      6.2.1 Computer room 25
      6.2.2 Server security and resilience 25
      6.2.3 UPS ..... Error! Bookmark not defined.
      6.2.4 Backup 25
      6.2.5 Antivirus 25
      6.2.6 Password policy 26
      6.2.7 Data security on servers 26
      6.2.8 Station security 26
      6.2.9 Logon scripts 26
      6.2.10 Network security. 26
   6.3 Recommendations 27
7. Evaluation concerning document management 29
   7.1 Summary 29
   7.2 Detailed report 29
      7.2.1 Document contents: generalities 29
      7.2.2 User documentation. 30
      7.2.3 Directory structure and file names.. 30
   7.3 Recommendations 31
8. Final summary 32
   8.1 Strong points and weaknesses 32
   8.2 Maturity levels 34
   8.3 Conclusion 37

SPECIMEN

1. Context

The goal of this evaluation is to evaluate the IT maturity of the client "*SPECIMEN SA*", company of xxxxxxxx, situated xxxxxxxxx in Belgium.

The company employs 16 persons.

The principal suppliers are EXAMPLE SA for telecommunications, EXAMPLE SA for ICT and EXAMPLE SA for computer systems.

***SPECIMEN SA* has asked for this evaluation in order to validate the existing IT system and to consolidate the new installation's configuration as well as its security.**

The company has one office, located in Brussels, in the middle of the European institutions. The premises have 4 levels with offices, platforms, meeting rooms and a computer room.

SPECIMEN

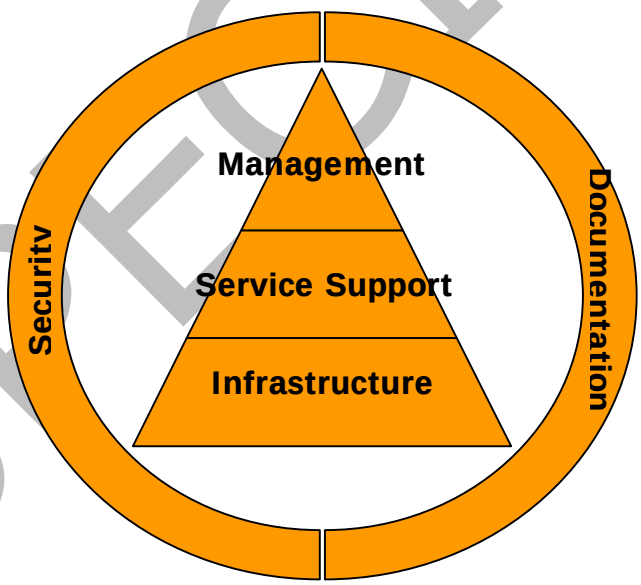
2. Approach

The objective is to evaluate the current situation of the company's IT exploitation and to recommend improvements.

The evaluation will relate to the five following fields:

1. **The quality of the IT infrastructure and the positioning of technological choices, both in terms of hardware (network, wiring, the fleet of PCs and printers, servers) and groupware;**
2. **The support received by the users of the computer system (helpdesk) and the management of changes, configurations and versions, referred to hereafter as "Service Support";**
3. **The activities associated with the management of the information system: financial management, project management, management of acquisitions and suppliers;**
4. **The security of the information system intended to ensure the protection and integrity of data, thanks to the reliability of the electric power supply, the back-up of data, the anti-virus measures and the management of passwords;**
5. **Document management through the inspection of documents.**

Schematically, the 5 areas of evaluation are represented as follows:



SPECIMEN

The present final report will include the following, for each of these areas:

- **a summary of strengths and weaknesses,**
- **a detailed analysis based on the conducted interviews and provided documents,**
- **pragmatic recommendations.**

A final summary will also set out an overview of the current situation in terms of the operation of the information system by means of:

- **an overall table of strengths and weaknesses,**
- **a graph of levels of maturity for the 5 areas for assessment,**
- **a proposal for a programme of improvement based on the list of recommendations.**

SPECIMEN

3. Evaluation of the management practices

3.1 Summary

This chapter refers to the management processes for the following IT functions:

- **acquisition management,**
- **supplier management,**
- **project management.**

Without being exhaustive, this list tries to target the most common activities of IT management.

<u>In short:</u>

Strong point:

- **good relations with the privileged suppliers**

Weak points:

- **a contract allowing inappropriate limited interventions**
- **software licenses that aren't managed well**
- **hardware warranties that aren't managed well**

Practical recommendations are given at the end of the chapter.

SPECIMEN

3.2 Detailed report

3.2.1 Acquisition management

3.2.1.1 Hardware acquisition

Mr/Mrs xxx, the company's Accounts & Administration Manager manages and validates all IT acquisitions (purchases & donations).

After having moved recently, *SPECIMEN SA* has equipped itself with new work stations and a new server.

3.2.1.2 Software acquisition

The acquisition of software and licenses is mainly done when purchasing hardware. *SPECIMEN SA* has equipped itself with the latest versions available concerning software that is used in a standard way at *SPECIMEN SA* on work stations as well as on the new server.

3.2.2 Project management

The IT projects are initiated by Mr/Mrs xxx based on immediate needs.

3.2.3 Suppliers management

***SPECIMEN SA* is not satisfied, concerning IT services, of the collaboration with the company EXAMPLE SA and deplores their work method.**

Also, concerning telephony and internet, the supplier EXAMPLE SA does not reach the levels of quality and guarantee required by *SPECIMEN SA*.

On the contrary, *SPECIMEN SA* has very good relations with privileged suppliers such as HP, Symantec, IBM. A few of these suppliers provide IT and technological equipment (TV HD, etc.) by donating them.

The different contacts at these suppliers are managed by Mr/Mrs xxx.

3.2.4 Financial management

The person responsible for the bookkeeping of IT expenses is Mr/Mrs xxx.

The IT expenses are not managed by budget, since they are carried out as and when the need arises.

3.2.5 Service level management

***SPECIMEN SA* uses a service contract concluded with the company EXAMPLE SA for the necessary technical services.**

SPECIMEN

This service contract does not cover the logistics of hardware repairs.

SPECIMEN

3.3 Recommendations

The recommendations are as follows:

- **R.MGT.1 : Review of the needs in terms of software maintenance**
- **R.MGT.2 : Inventory of the used licenses and their validities**
- **R.MGT.3 : Review of the needs in terms of technical and logistic maintenance**

R.MGT.1 **Review of the needs in terms of software maintenance**	• **The current contract allows to obtain a certain number of free technical interventions, but it is limited. However, since the logistic aspect of park management and preventive maintenance is not covered, a more global and proactive contract would be a more appropriate solution. Nowadays, you don't have to wait for problems to arise anymore before modifying and improving your IT system.**
R.MGT.2 **Inventory of the used licenses and their validities**	• **Make an inventory of the available licenses (OEM, paper, mail, etc.) and compare with an inventory of softwares used in the entire park.** • **Certain softwares have valid licenses that limited in time.**
R.MGT.3 **Review of the needs in terms of technical and logistic maintenance**	• **There isn't any technical coverage in case of hardware failure. Even under manufacturer warranty, a hardware failure will completely paralyze IT services and consequently the company *SPECIMEN SA*. A hardware service contract will allow to extent the manufacturer's warranty coverage for the duration as well as high availability of the IT equipment.**

SPECIMEN

4. Evaluation of the support practices

4.1 Summary

The Support Service deals with:

- **incident and problem management (helpdesk);**
- **change management;**
- **management of configurations and versions.**

<u>In short:</u>

Strong points:

- **the IT equipment is new;**
- **the IT system on the work stations has been completely reinstalled with the latest software versions;**
- **the presence of substitute work stations already installed with standard *SPECIMEN SA* software.**

Weak points:

- **a non satisfying phone and Internet provider;**
- **a non proactive IT maintenance;**
- **access to data on the server not clearly defined;**
- **data are stocked on certain work stations.**

Practical recommendations are given at the end of the chapter.

SPECIMEN

4.2 Detailed report

4.2.1 Problem and incident management (helpdesk)

4.2.1.1 Helpdesk organization

Mr/Mrs xxx ensures user support. When he cannot ensure this assistance because of lack of time or lack of know-how, he will appeal to the service of the company EXAMPLE SA.

4.2.1.2 Incident management

The user support is internally taken on by Mr/Mrs xxx.

According to the type of incident, Mr/Mrs xxx will ask for assistance at EXAMPLE SA who will take care of the problem.

The follow-up and method applied for certain incidents has several times been questioned by *SPECIMEN SA*.

Incident management is thus mainly realized by phone. The company EXAMPLE SA can take over remotely via VNC in order to correct certain aspects.

For more recurring incidents or changes, it is sometimes necessary to intervene on-site.

In case of serious failure, there isn't any external support contract for the stations, nor for the server, which could lead to a reduced productivity. Until now there hasn't been any serious failures.

4.2.1.3 Problem management

Recent Internet and telephony failures linked to the operator EXAMPLE SA in collaboration with EXAMPLE SA have heavily disrupted, and even paralyzed, the good functioning of *SPECIMEN SA*'s activities.

Mr/Mrs xxx is not always kept informed of the solutions that have been used for the different encountered problems. There is no history management.

SPECIMEN

4.2.2 Management of configurations and versions

4.2.2.1 Hardware – PCs – Servers – Printers

The recent installation of new IT equipment allows a better use of the means and resources that are available for *SPECIMEN SA*'s collaborators. The standardization of the installed software simplifies its maintenance.

4.2.2.2 Software

The work stations are installed under Windows XP Sp2. The used office applications are Microsoft Office 2003 including Microsoft Outlook 2003.

We have noted that the antivirus is installed manually on the work stations.

4.2.3 Level of satisfaction

4.2.3.1 Office equipment

The level of satisfaction concerning office equipment has not been assessed during the audit. However, it seems to be of good quality, all work stations have been reinstalled by Mr/Mrs xxx personally.

4.2.3.2 Business tools

The level of satisfaction of the business tools has not been assessed during the audit. Mr/Mrs xxx has installed the operating system and standard applications on all work stations.

4.2.3.3 Internet access and e-mail

Internet access is realized through a EXAMPLE SA ADSL line with a Cisco 800 router. A Firebox WatchGuard X500 firewall ensures the incoming and outgoing filtering. All external mails go through EXAMPLE SA.

4.2.3.4 Server network and access

The network work stations are authenticated in a certain domain (*SPECIMEN SA*). There is a login script which is not personalized though. There is only one letter attributed for all network resources. The users clearly don't make a distinction between common data accessible by the entire company, data per work group or personal data.

It appears that not all data are stocked on the servers. Some work stations, especially laptops, can contain essential data which are not saved elsewhere.

SPECIMEN

4.3 Recommendations

The recommendations are as follows:

- **R.SUP.1 : Outsource the management and repairing of hardware and software**
- **R.SUP.2 : Centralization of data and synchronization**
- **R.SUP.3 : Access and data restructuring and securing on the server**

R.SUP.1 **Outsource the management and repairing of hardware and software**	• **In order to reduce time loss for repairs and ensuring the proactive maintenance of the park, a global management solution would be ideal. This allows *SPECIMEN SA*'s collaborators to focus on its core business.** • **A complete outsourcing of the IT system allows a better pro-activity and a better user support.**
R.SUP.2 **Centralization of data and synchronization**	• **In order to prevent loss of data located on the work stations, a centralized data solution on the server combined with synchronization, if needed for the laptops, can be implemented. The back-up of a great number of important data located on the work stations has been neglected before.**
R.SUP.3 **Access and data restructuring and securing on the server**	• **The users clearly don't make a distinction between common data accessible by the entire company, data for work groups and personal data. The structure of the directories on the server has to be reworked.**

SPECIMEN

5. Evaluation of the IT infrastructure

5.1 Summary

This chapter refers to the following IT infrastructure components, hardware as well as software:

- **Passive:**
  - **Computer room**
  - **Cabling**
  - **Patch panels**
- **Network:**
  - **Access / topology**
  - **Hubs and switches**
  - **Routers**
- **Servers**
- **PCs**
- **Printers**
- **Groupware**

Without being exhaustive, this list tries to give you an idea about the most significant components of the infrastructure.

<u>In short:</u>

Strong points:

- **a new IT park**
- **new cabling in good condition**
- **the presence of a rack**

Weak points:

- **a small computer room at risk**
- **patch cables of different quality**
- **a lack of structure and organization of the rack**
- **a rack that is too small to host the entire IT equipment**
- **a lack of guarantee of the phone and Internet provider**
- **a lack of security concerning e-mail**
- **a lack of clarity concerning data access**
- **local data are present on the work stations, mainly the laptops; there is no back-up whatsoever foreseen for these data**

Practical recommendations are given at the end of the chapter.

SPECIMEN

5.2 Detailed report

5.2.1 Analysis of passive devices

5.2.1.1 Technical room

A technical room hosts the company's IT and telecom infrastructure. This room is located in the basement, it's a small room of 2 x 5 m and its door is locked.

There is no window. The room temperature was normal at the time of the audit. There is no air-conditioning, but it will probably not get too hot there. If necessary, the company *SPECIMEN SA* will adapt this room.

This room does not have a fire detection and extinction system. There is however no flammable material such as paper.

Energy (electricity, gas, etc.) and telecommunications is also supplied in this room.

A small 14 inch telecom rack hosts a patch panel, 2 network switches, 2 EXAMPLE SA telecom switches, 1 FireBox firewall.

The server and screen are placed on a table. The UPS is placed on the ground.

5.2.1.2 Network cabling and patch panel

The network cabling of the various offices has been done with UTP Cat 5 cables. The patch panels are located in a small open rack on the ground. The access to this patch panel is difficult because of the narrow computer room.

The cables linking the patch panels to the 3Com switches are of different lengths (even 5 meter cables) and not homogeneous. The cables are not clearly identified.

SPECIMEN

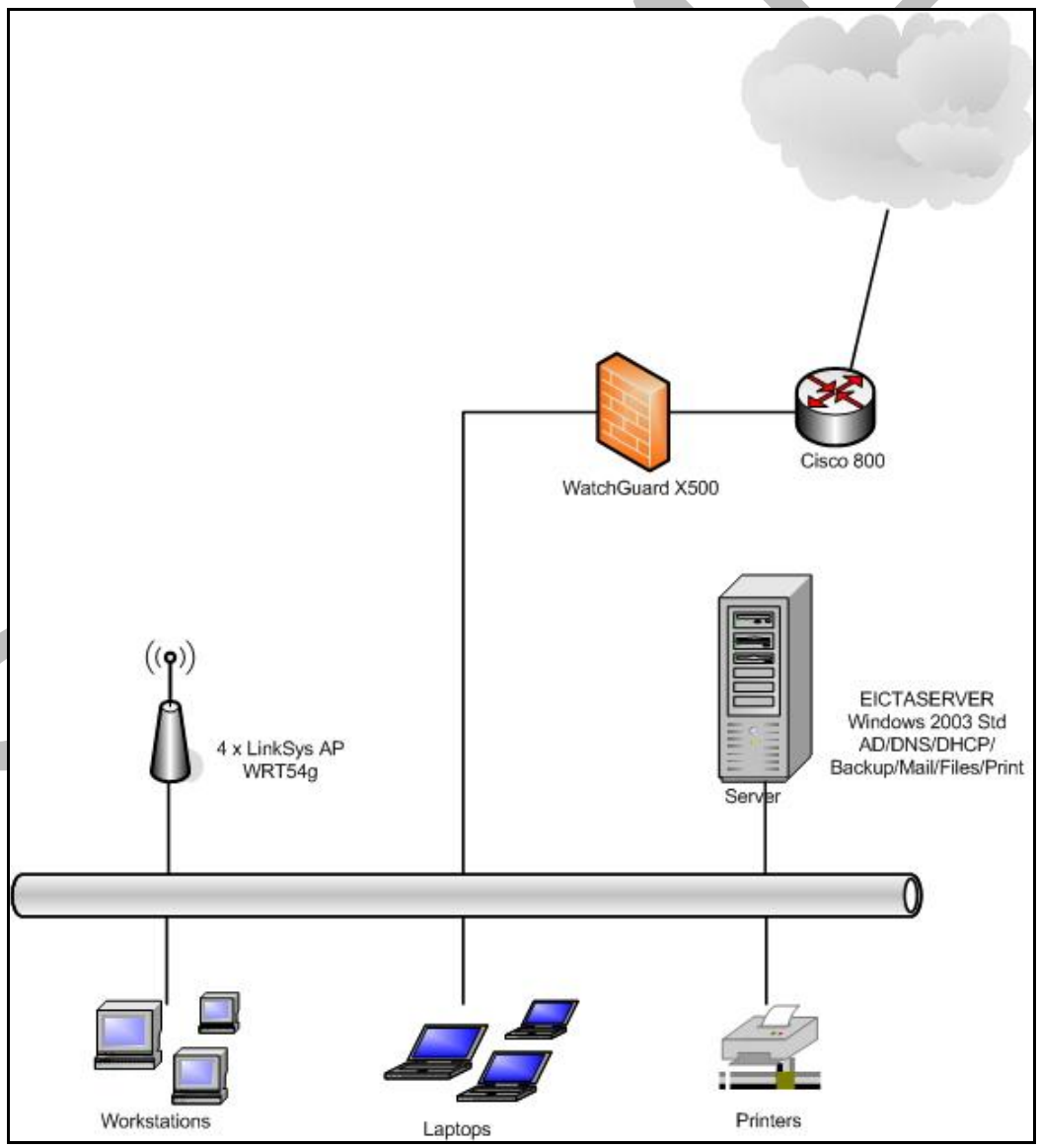
5.2.2 Network analysis

5.2.2.1 Access method / Topology

The attribution of IP addresses is realized in a poorly organized way. There is no table with the addressing plan despite the use of a DHCP server. In order to attribute an address to a new network peripheral device such as a printer, an access point, etc. a free address is trying to be found.

The used network parameters are not optimal in this configuration. There is a difference in configuration for the network peripherals. This may imply configuration errors.

The configuration of DNS on the work stations gives the addresses of the DNS Internet servers of EXAMPLE SA.



5.2.2.2 Hubs and switches

The connection of the stations is realized by 2 3Com 3C17300 switches which are non manageable 24 ports 10/100 switches. These 2 switches are interconnected through a 10/100 port to which the server, the 4 WIFI Access Points, the Firewall, the network printers and the work stations are connected. All EXAMPLE SA phones are connected to 2 specific HUBs in the rack.

The switches are non manageable which makes it hard to solve possible problems.

The WIFI access points are secured with a key type WPA Personal but the used key is not complex enough. An external user, such a member already connected to the wireless network, can easily remember the used WPA key. If this user wants to reconnect another day, he can easily reuse the WPA key even without taking note of the configuration.

Note that the access points are configured on the following channels: 10, 10, 11, 13. This means there is an overlap between the different WIFI frequencies. Also, an access point cannot communicate on a channel identical to another in its transmission area since this leads to disturbances and interferences between them.

There is a WIFI terminal which hasn't the same SSID as the other 3.

5.2.2.3 Router

Internet access is realized through a Watchguard X500 firewall managed by EXAMPLE SA and a Cisco 800 router managed by EXAMPLE SA.

SPECIMEN

5.2.3 Servers

A Windows 2003 Standard "Domain Controller" is installed on a HP Proliant Tower ML350-G4 Xeon 3.4 Ghz with 4Gb memory.

The installed physical memory uses 4 memories of 1Gb, there is no more space for a memory upgrade.

This server runs also DNS, DHCP, Wins, a backup system (Symantec BackupExec 10d), a mail system (Microsoft Exchange 2003), an antivirus (Symantec Antivirus Business Pack).

This server ensures the availability of the access to the files stored on the shared D disk. This 250 GB shared disk is used for 30 %. The storage system is configured in Raid-5 on three 146Gb to 10K RPM hard disks.

The entire equipment is covered by the manufacturer warranty but does not benefit from any additional maintenance contract. If a hardware problem occurs, the solution could take a certain amount of time and paralyze the company activities.

Certain parameters on the server are defined in an other language than English.
There are also software screens which are displayed in an other language than English. Since *SPECIMEN SA* is a multinational and their policy is to exclusively use the English language, the language used on the server should also be standardized.

5.2.4 PCs

During the audit, we have identified a PC park composed of 17 work stations with various characteristics (including 6 laptops).

Most of these work stations have a processor type Pentium 4 or equivalent with at least 1,8 Ghz. The memory is at least 256 Mb. The hard disks are at least 20 Gb and can even reach 150 Gb. These machines are equipped with a network card of 10/100 Mb.

Most of these stations have recently been reinstalled under Microsoft Windows XP Sp2 with Microsoft Office 2003 Professional.

Certain users, mainly laptop users, have local data. There isn't any backup foreseen for these data.

SPECIMEN

5.2.5 Printers

Besides a HP laser printer, all printers are shared on the server. There are 7 network laser printers including 1 colour printer.

All printers are of the brand HP except one Konica.

5.2.6 Groupware infrastructure

Groupware: definition:

Group of software destined to be exploited by several users at the same time, on the same project – software for group work. Work method, based on the relations between the members of a group (linked through a network).

Range of tools destined to optimize team work. For example software allowing a group of users to work together on the same project without needing them to be reunited. Within this software there is a mail server. It is generally completed by tools for document sharing, calendar, contacts, workflow, videoconference, etc.

A groupware infrastructure is thus destined to ease information sharing and access for all users of a work group.

5.2.6.1 File servers

The file server is realized by shared data stored on the D disk of the server. Only a few shares allow access:

Finances$	**D:\Shared\Finances**
Data	**D:\Shared\Data**
Aida$	**D:\temp\Aidaresult**
Install	**D:\Shared\Install**

There is no clear structure on the D disk. The data directories are only accessible through a W: network letter. The access is not clear for the users.

The users perceive personal directories of other users without having access.

Only the DATA share is used.

SPECIMEN

5.2.6.2 E-mail

The e-mail system is realized by Exchange 2003 Sp1. The work stations use the client Outlook 2003.

All internal and external messages go through this Exchange server.

***SPECIMEN SA* uses the existing anti-spam module in the Exchange 2003 Sp1 version. This is only a light version of anti-spam programme. There is no other installed anti-spam programme. The company *SPECIMEN SA* is burdened with spams.**

There are contacts adopted in Exchange distibution groups. This list of contacts is not always updated.

5.2.6.3 Calendar

There is no shared calendar even if this is very necessary.

SPECIMEN

5.3 Recommendations

The recommendations are as follows:

- **R.INF.1 : Replacement of the rack and reorganization of the network**
- **R.INF.2 : Obtain service guarantees of the provider**
- **R.INF.3 : Reorganization of data access and security**
- **R.INF.4 : Realization of a site survey for WIFI access**
- **R.INF.5 : Delocalization and synchronization of the work station data**
- **R.INF.6 : Installation of an anti-spam programme**

R.INF.1 **Replacement of the rack and reorganization of the network**	• Even if there's a rack present, it is too small to host all the IT equipment. A bigger rack will allow to host the server, UPS, ADSL router. This prevents IT equipment from being located on the ground. • In order to avoid network problems, certain RJ45 cables are too long and have to be replaced. • A well organized cabling and well identified cables allow to reduce time loss for repairs and to ensure a good network maintenance. During a modification or failure of the cabling, it is almost impossible to find the cause of the problem. • For a good rack maintenance this should be easily accessible in front and behind. • The rack has to be stabilized since the ground is not entirely flat.
R.INF.2 **Obtain service guarantees of the provider**	• It is possible to avoid or reduce the number of telecommunication failures at certain telephone providers and at certain Internet providers thanks to service level agreements (SLA).
R.INF.3 **Reorganization of data access and security**	• The data are not clearly accessible for the users. There are no differences of access to data shared and acceded by the users.
R.INF.4 **Realization of a site survey for WIFI access**	• The WIFI access points are not well configured since the used channels are superposed (overlap). This can lead to slowing down of the

SPECIMEN

	network due to disruptions between the WIFI terminals. • There are 2 terminals of which the channel is identical (10). • A site survey should check if the configuration used in the company doesn't lead to internal network problems due to the configurations of the WIFI networks detected in the environment.
R.INF.5 **Delocalization and synchronization of the work station data**	• Data are presented on certain work stations, mainly laptops. It is dangerous to leave these data unprotected. • It is recommended to move these local data on the server to back up these data. • In order to have information at your disposal outside the company, it is possible to configure a synchronization of data between the server and the laptops. However, because of the nature of certain data, this can sometimes lead to synchronization problems. • It is also possible to use secured remote accesses to the network. This will allow the concerned users to have access to all their authorized data. This method has the following advantages: - Avoiding synchronization problems - Avoiding treatment errors - Centralization of data on the server - Always the latest data - Data that are backed up
R.INF.6 **Installation of an anti-spam programme**	• It is strongly advised to install an anti-spam programme to avoid undesirable mails.

SPECIMEN

6. Evaluation of the security practices

Data security is based on three important cornerstones:

- **Confidentiality**
- **Integrity**

- **Availability**

(CIA)

These three cornerstones as well as the peripheral aspects have been assessed during the audit.

6.1 Summary

This chapter relates to the following IT infrastructure components:

- **computer room;**
- **server security and resilience;**
- **UPS;**
- **backup;**
- **antivirus;**
- **password policy and station security;**
- **data security on servers.**

Without being exhaustive, this list tries to target the most needed security elements.

<u>In short:</u>

The strong point is:

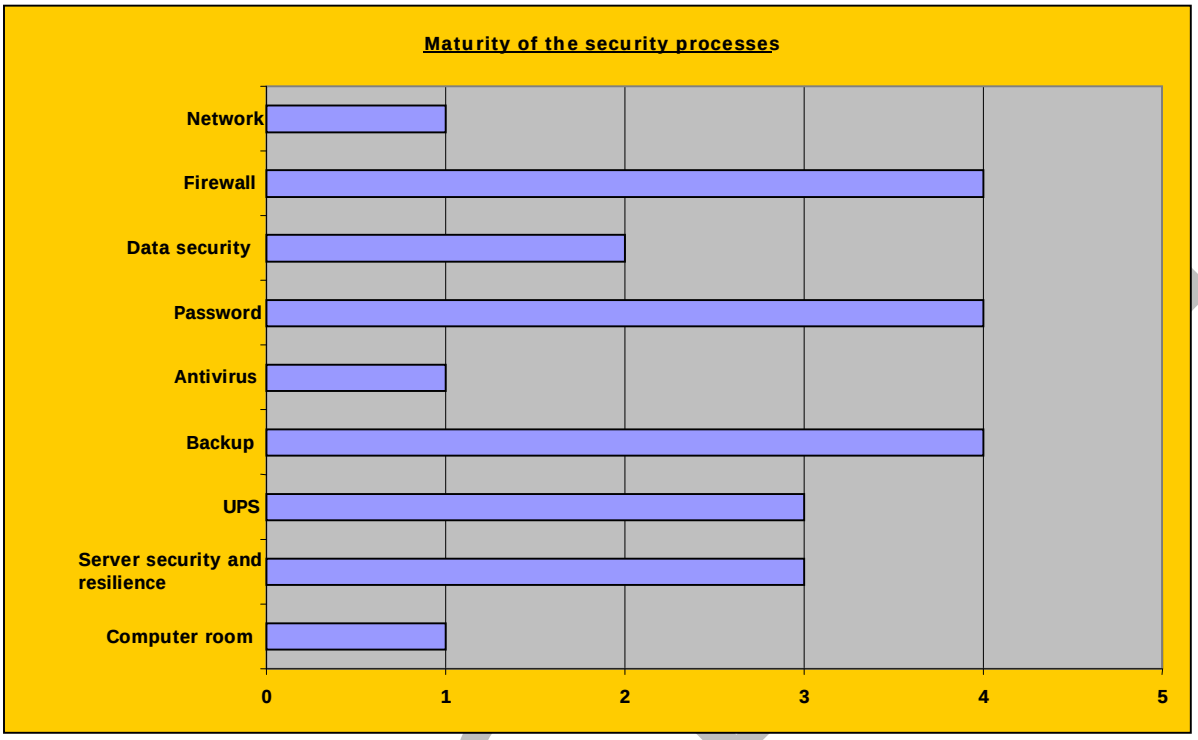
- **the configuration of the WIFI network security is correct.**

The weak points are:

- **the computer room has several risk factors;**
- **a partial antivirus protection;**
- **the access to the data is not clearly defined;**
- **the configuration of wireless terminals (channels) has to be revised.**

SPECIMEN

The following graph shows the maturity levels of the different security processes of the analyzed information system.



Recommendations are given at the end of the chapter.

SPEC

6.2 Detailed report

6.2.1 Computer room

Since the computer rooms are already described at chapter 5.2.1, we will only repeat that besides the absence of fire alarm systems and air-conditioning, the computer room contains access to other energies and is fairly small.

6.2.2 Server security and resilience

The server is not equipped with redundant power supplies. However, the server has an array disk of circa 280 Gb total capacity. There are 3 HDD of 146 Gb of 10K RPM configured in Raid5.

There is no maintenance contract on the equipment except for the initial manufacturer warranty.

6.2.3 UPS

The active equipment is not connected to the UPS. The configuration in case of power interruption is maybe not sufficient in terms of time period.

6.2.4 Backup

The server is entirely backed up with Symantec BackupExec 10d on tape in an internal HP LTO Ultrium 460 tape drive with the appropriate media. The backup is programmed at 23h00 every day except week-ends. This takes about 1h30 and leads to about 67 Gb backed up data.

The backup method is complete and the rotation of media is 4 for Monday to Thursday and 5 for Fridays. The backup operator outsources the last backup.

No disaster test has been carried out as from the backup tapes.

There is no backup of data located on the work stations.

6.2.5 Antivirus

The antivirus installed on the server is Symantec Anti-virus 10.0 Business Pack. The updates are realized by the method LiveUpdate as from the parent server on time every day at 6h00. This update method is not the best configuration for a company. The recommended method is Intelligent Updater.

The work stations are not being correctly updated. We establish that certain stations are not up to date since 15 days, or even since January.

The antivirus solution on the server is not adapted to the mail exchange server.

SPECIMEN

The Business pack version is developed for protection against viruses in files. An antivirus solution should be used for mail, for example, the programme Symantec Mail Security for Exchange.

This programme allows an antivirus protection of mails but also Exchange mailboxes (real-time protection and scanning).

6.2.6 Password policy

Normally, all users have a password to connect to the network. The security for a user remote access is defined on the firewall. This password is more secure than on the internal network.

It seems there is no policy of password changing at *SPECIMEN SA*.

6.2.7 Data security on servers

The data are secured by limited accesses according to the users. However, these are not properly structured on the server.

The sharing of data between the users takes place through their personal directories. The users are responsible for the security. There is no access policy in terms of security of the directories by groups. It is recommended to create several user groups, for example according to department, in order to simplify the management of rights on the server.

The use of groups:

- reduces the list of accounts to which rights are attributed;
- simplifies the change of department of a certain user (change of rights by heritage of the groups);
- simplifies the data availability for a new user;
- simplifies the restriction for a outgoing user;
- allows a simpler hierarchy.

6.2.8 Station security

Work station users have no access to the systems. They don't have the rights to install or delete applications.

6.2.9 Logon scripts

A simple logon script executes the same mapping (W :) for all users. Two other scripts connect the Konica printer or the HP Colour printer.

6.2.10 Network security

SPECIMEN

There are 4 WIFI access points. These terminals are located in the offices, 1 per floor. The details of the access points have already been described in section 5.2.2.2.

6.3 Recommendations

The recommendations are as follows:

- **R.SEC.1 : Security of the computer room.**
- **R.SEC.2 : Review of the configuration of the backup battery.**
- **R.SEC.3 : Server restore test.**
- **R.SEC.4 : Review the antivirus solution.**
- **R.SEC.5 : Review the configuration of the WIFI terminals.**

R.SEC.1 **Security of the computer room**	**The computer room has not been protected against fire nor by detectors nor by automatic extinction systems.** **Other energy also passes through this room.** **During the audit, the temperature didn't seem to be a problem, but it would be good to verify if an air-conditiong system would be necessary.**
R.SEC.2 **Review of the configuration of the backup battery**	**The UPS configuration is programmed to do a complete power stop on battery when the charge level is under 30%. This pause is programmed for 2 minutes. It is recommended to verify if a secured server stop is possible within this period.**
R.SEC.3 **Server restore test**	**The backup seems to be correct even if it seems there hasn't been any restore test or disaster test.** **It is important to verify if it possible to realize a data restoring test (even partial) on a regular basis. But it is also important to do a disaster test occasionally.**
R.SEC.4 **Review the antivirus solution**	**It is important to be well protected against viruses. The used method is a file protection. It is recommended to install an antivirus solution for the mail system.** **The configuration of signatures updates should be revised since the applied method is not the best one. Furthermore, it appears that not all stations are up-to-date.**

SPECIMEN

R.SEC.5 **Review the configuration of the WIFI terminals.**	**The configuration of access points on the used channels as well as the used WPA key should be reviewed.** **In addition, a site survey would allow to verify and validate the configuration to be applied and to avoid performance problems due to the WIFI networks of the neighbourhood.**

SPECIMEN

7. Evaluation concerning document management

7.1 Summary

The strong points are:

- **a little documentation at suppliers;**
- **some configuration files or passwords on the server console.**

The weak points are:

- **no documentation for the users;**
- **no document designation;**
- **no directory structure on the file server.**

Practical recommendations are given at the end of the chapter.

7.2 Detailed report

7.2.1 Document contents: generalities

The document inspection procedure consists of reading and of a detailed exam based on the criteria regarding to the contents of the document, such as structure, completeness, coherence and clarity.

The inspection checks the conformity of the document with the document standards to be used for the project implementation, management and follow-up. This inspection analyzes the following aspects of the documents:

- **Identification**
- **Storage**
- **Usefulness, completeness and exactness**

For each analyzed document, the following information should be inserted:

- **Identification**
- **Name of the document**
- **Author**
- **Status (draft/final)**
- **Publication date**
- **Version**
- **Number of pages**
- **Identification of each page (header or footer)**
- **Number of copies/distribution list**
- **Storage**
- **Holder of the document**
- **Format of the document (paper or electronic)**
- **Usefulness of the document**
- **Usefulness for the company**

SPECIMEN

Work instructions relating to the use of shared resources, updating of anti-viruses, etc. should be available.

Ideally, this entire documentation should contain a large number of screen shots for a smooth guidance of the user.

The collaborators ask for a procedure on the nomenclature of the file names in order to be more efficient while treating documents created by others.

Finally, all already existing procedures have to be followed. Therefore it is necessary to verify which persons have to follow this procedure and take appropriate measures in case of non compliance.

Without being exhaustive this list gives the most important security elements.

7.2.2 User documentation

The personnel of *SPECIMEN SA* hasn't practically any documentation relating to the use of the IT tool. Systemat has a minimum of information which are regroupings of basic information that have been of use in this evaluation report.

Concerning the available documentation, certain user guides (for example Windows or Office) are available, but it is limited to the documentation provided by the programme editors.

A user manual with all the provided information should be produced and distributed. This would allow the improvement of everyone's knowledge.

Example of general procedures to be implemented:

- **procedure in the field of data security;**
- **procedure in the field of data storage;**
- **procedure for printer use;**
- **procedure for network access (LAN, WIFI, remote).**

7.2.3 Directory structure and file names

The directory structure is not clearly defined. There is only one data access through a letter W:. The users see the directories but cannot enter them.

It is very difficult to distinguish data belonging to a user, a group or accessible by all the personnel of *SPECIMEN SA*.

SPECIMEN

7.3 Recommendations

The recommendations are as follows:

- **R.DOC.1 : Reorganization of the file server**
- **R.DOC.2 : Documentation of the IT infrastructure**

R.DOC.1 **Reorganization of the file server**	**The current structure of the directories on the file server doesn't allow a proper data access and management.** **A restructuring with standard directory entries such as « User », « Group », « Company » would simplify it.**
R.DOC.2 **Documentation of the IT infrastructure**	**A documentation of the network, hardware and software infrastructure and of the functioning of the applications would allow a better maintenance of the IT systems.**

SPECIMEN

8. Final summary

8.1 Strong points and weaknesses

The report below adopts the strong points and weaknesses of the 5 evaluation fields such as highlighted in the various chapters of this report.

Domain	Main forces	Main weaknesses
Management	• Good relations with the privileged suppliers	• An inappropriate contract for selective interventions • Non-managed software licenses • Non-managed hardware warranties
Service Support	• The IT hardware is recent • The IT system on the work stations has completely been reinstalled with the latest software versions • There are spare work stations already installed with the standard software	• An unsatisfying phone and Internet provider • Non-proactive IT maintenance • Data are stored on several work stations
Infrastructure	• A new IT park • New cabling in good condition • The presence of a rack	• A narrow computer room at risk. • Cable patches of different quality. • Lack of rack structure and organization. • A too small rack to host all the IT equipment. • A lack of guarantee of the phone and Internet provider. • A lack of mail security. • A lack of clarity concerning data access. • Local data are present on the work stations, mainly the laptops. There isn't any backup foreseen for these data.
Security	• The configuration of the WIFI network security is correct	• The computer room has several risk factors • Partial antivirus protection • The data accesses are not clearly defined • The wireless terminals configuration should be revised

SPECIMEN

Documentation	• **A little documentation at the suppliers** • **Some configuration or password files on the server console**	• **No user documentation** • **No document designation** • **No directory structure on the file server**

SPECIMEN

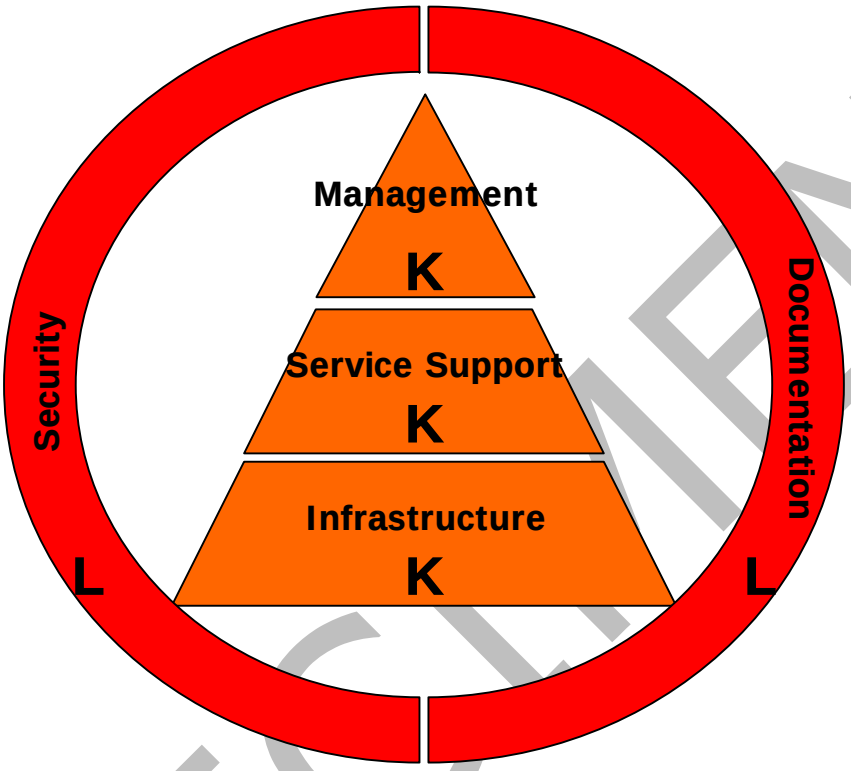
8.2 Maturity levels

In order to evaluate the maturity of each process, it is possible to define the following references:

Maturity	Description	Colour code	Symbol code
Strategic	The activities of a strategic maturity field are developed, implemented and managed in a satisfactory way as a whole. The concepts of pro-activity and medium-term are generally present. In terms of added value, a strategic field of maturity offers a competitive advantage to the company.	Green	J
Tactical	The company carries out significant efforts to develop and establish the activities of a tactical field of maturity. The concepts of reactivity and short-term are generally present. However, a tactical field of maturity is not capable to offer to the company all the benefit which it could expect.	Orange	K
Critical	The activities of a field of critical maturity are partially implemented, most often following specific needs. Many prerequisites are missing. The positive contributions of a field of critical maturity are counterbalanced by lacks of effectiveness and productivity within the company. Moreover, the field can present a potential risk for the company.	Red	L

Based on the analysis of the strong points and weaknesses listed in chapter 8.1 of this document and based on good practice relating to these fields, the levels of maturity of the company are presented in the graph below. The next table lists the actions to be taken which are classified according to the importance and the urgency of the implementation.

SPECIMEN


Management
K
Service Support
K
Infrastructure
K
Security
L
Documentation
L

SPECIMEN

The recommendations for the 5 fields of evaluation are the basis of the program of improvement. Accordingly, the following synopsis proposes a classification of the recommendations according to their importance and their urgency.

Urgency

R.INF.4 : Realization of a site survey for WIFI access **R.SEC.5 : Review the configuration of the WIFI terminals I** **R.DOC.1 : Reorganization of the file server** **R.INF.3 : Reorganization of data access and security**	**R.SEC.1 : Security of the computer room** **R.SEC.4 : Review the antivirus solution** **R.SEC.2 : Review of the configuration of the backup battery** **R.INF.2 : Obtain service guarantees of the provider** **R.SUP.3 : Access and data restructuring and securing on the server** **R.INF.6 : Installation of an anti-spam programme** **R.DOC.2 : Documentation of the IT infrastructure**
R.MGT.2 : Inventory of the used licenses and their validities **R.SEC.3 : Server restore test**	**R.INF.1 : Replacement of the rack and reorganization of the network** **R.MGT.1 : Review of the needs in terms of software maintenance** **R.MGT.3 : Review of the needs in terms of technical and logistic maintenance** **R.SUP.1 : Outsource the management and repairing of hardware and software** **R.SUP.2 : Centralization of data and synchronization**

8.3 Conclusion

The IT maturity level of *SPECIMEN SA* is sufficient to support the IT activity of the company.

It remains however perfectible and the IT system at *SPECIMEN SA* contains several problems.

The antivirus solution is poorly implemented. It is absent for mail and badly configured for updates and badly distributed on the work stations.

We establish also a lack of security concerning the WIFI network allowing members to disconnect without *SPECIMEN SA*'s knowing. Furthermore, the configuration of the different terminals is not sound. The current configuration could lead to performance, reliability and access problems.

The used computer room is not only for IT use. The replacing of the existing rack would be a good solution in order to regroup the IT equipment in the rack. This would for example avoid the server to be placed directly on the ground or on a table. However, this room is also equipped with water and energy pipes (gas, electricity). The greatest inconveniency of a bigger rack in this room would be its difficult accessibility due to the size of the room.

It is important to verify the backups through restoration procedures and tests. Also for the UPS, battery tests and checks should be carried out. The batteries are constantly being recharged and like all batteries, they will wear out after certain time. Due to the updating of the IT park, there should be no battery problems but the configuration should be verified today.

Moreover, even though the production can do temporarily without the IT tool, telecommunication or telephony means, it can be disrupted by a partial temporary unavailability. Recent telecommunication or Internet access problems have made it difficult to work for the entire company.

It is recommended to have a proactive support and global management of the IT park in order to limit potential problems. It is not only that when there is a problem, one should act on it. For example, there exist update policies for Windows, Office, antivirus, etc. which avoid a lot of problems.

These different aspects explain why we have given an average rating for the different domains that have been assessed (except for security and documentation).

We think that improvements in the field of the file structure and data access (shares) on the server as well as synchronization for the laptops, its proactive maintenance, regular check of its good functioning and continuous improvement of the IT tool should offer a better quality service with more security.

SPECIMEN

The documentation aspect should not be neglected. The most important element of IT management is a detailed documentation of the existing systems. This documentation should be realized when implemented and updated when modified. This explains our low rating for security and documentation.

SPECIMEN