Evaluation des pratiques de gestion de l'exploitation informatique
À l'usage de la société *SPECIMEN SA*
Rapport d'évaluation

Rapport final de l'évaluation relative à :

- **la qualité de l'infrastructure informatique, tant matérielle que logicielle, et le positionnement des choix technologiques ;**
- **le support reçu par les utilisateurs informatiques (helpdesk), la gestion des changements, des configurations et des versions ;**
- **sécurité du système d'information : protection et intégrité des données ;**
- **la gestion documentaire ;**
- **les activités de management du système d'information : gestion de projet, gestion des acquisitions et des fournisseurs, gestion financière ;**

Auteur(s) : Xxxxxx Xxxxxx

Date : xx/xx/200x — **Evaluation le xx/xx/200x**
Audit technique les xx & xx/xx/200x
Rapport présenté le xx/xx/200x
Référence : **Rapport Evaluation NOEMI V_01.doc**

Diffusion :

Validation :

Révisé par : **Date :**

Commentaires :

Historique du document

Version	Initiateur des modifications	Modifications	Date	Auteur(s)
0_1	Initial Version	Rédaction	xx/xx/200x	Xxxx Xxxxxxx
0_2	Xxxx Xxxxxxx	Relecture et validation	xx/xx/200x	Xxxx Xxxxxxx
0_3				

SPECIMEN

Table des Matières

1. Contexte 4
2. Démarche utilisée 5
3. Evaluation des pratiques en matière de management 6
   3.1 Synthèse 6
   3.2 Rapport détaillé 7
      3.2.1 Gestion des acquisitions 7
      3.2.2 Gestion de projet 7
      3.2.3 Gestion des fournisseurs 8
      3.2.4 Gestion financière 8
      3.2.5 Gestion des niveaux de service 9
   3.3 Recommandations 10
4. Evaluation des pratiques en matière de support 11
   4.1 Synthèse 11
   4.2 Rapport détaillé 12
      4.2.1 Gestion des problèmes et des incidents (helpdesk) 12
      4.2.2 Gestion des changements 13
      4.2.3 Gestion des configurations et des versions 15
      4.2.4 Niveau de satisfaction 16
   4.3 Recommandations 19
5. Evaluation de l'infrastructure informatique 21
   5.1 Synthèse 21
   5.2 Rapport détaillé 22
      5.2.1 Analyse du passif 22
      5.2.2 Analyse du réseau 22
      5.2.3 Serveurs 25
      5.2.4 PC 26
      5.2.5 Imprimantes 29
      5.2.6 Infrastructure groupware 30
   5.3 Recommandations 34
6. Evaluation des pratiques en matière de sécurité 36
   6.1 Synthèse 36
   6.2 Rapport Détaillé 38
      6.2.1 Le local technique 38
      6.2.2 La sécurité du serveur et sa résilience 38
      6.2.3 Alimentation secourue 39
      6.2.4 Back up 40
      6.2.5 Protection virale 41
      6.2.6 Utilisation des mots de passe 42
      6.2.7 La sécurité des données au niveau des serveurs 42
      6.2.8 La sécurisation des stations 43
      6.2.9 Les logonscripts 43
   6.3 Recommandations 44
7. Evaluation en matière de gestion documentaire 46
   7.1 Synthèse 46
   7.2 Rapport détaillé 46
      7.2.1 Ce qu'un document devrait contenir : généralités 46
      7.2.2 Documentation à disposition des utilisateurs 47
   7.3 Recommandations 48
      7.3.1 Recommandation relative au stockage des documents 48
      7.3.2 Recommandation relative à la gestion des versions 49
      7.3.3 Recommandations relatives aux documents contractuels 49
      7.3.4 Recommandations relatives aux documents d'expression des besoins 49
      7.3.5 Recommandations relatives aux documents d'analyse fonctionnelle 50

SPECIMEN

7.3.6 Recommandations relatives aux documents d'analyse technique..... 50
7.3.7 Recommandations relatives aux documents de support et d'exploitation..... 50
7.3.8 Recommandations relatives aux documents de gestion de projet informatique 50
8. Synthèse finale..... 51
8.1 Forces et faiblesses 51
8.2 Niveaux de maturité 53

SPECIMEN

1. Contexte

Le but de l'évaluation « Bilan de Santé » est d'évaluer la maturité informatique du client « *SPECIMEN SA* », entreprise de xxxxxxx, située à xxxxxxxx en Belgique.

La société est actuellement composée d'environ 110 personnes qui se décomposent en environ 90 ouvriers et 20 employés.

Quelques dates (Extraits du site Internet de *SPECIMEN SA*) :

La société *SPECIMEN SA* a demandé cette évaluation afin de connaître son état actuel au niveau informatique (bon ou mauvais), de corriger certaines pratiques, et éventuellement d'externaliser complètement son informatique à une société extérieure, profitant ainsi des connaissances poussées de cette société.

***SPECIMEN SA* dispose actuellement de**

- **4 serveurs,**
- **17 postes de travail : 15 desktops et 2 laptops,**
- **1 imprimante réseau centralisée,**
- **8 imprimantes locales,**
- **2 fax,**
- **1 switch 50 ports, 100 Mbps (dont 2 ports Gigabit),**
- **1 router.**

2 sociétés externes sont reliées par des lignes de réseau. Elles n'ont pas été prises en compte lors de cette évaluation.

Les 2 laptops de la société *SPECIMEN SA* n'ont pas non plus été recensés car indisponibles durant les périodes d'évaluation. Les données y afférant ne devraient cependant pas trop influencer les résultats de l'analyse.

L'analyse de son environnement permettra de proposer des recommandations concernant les différents domaines couverts lors de cette évaluation.

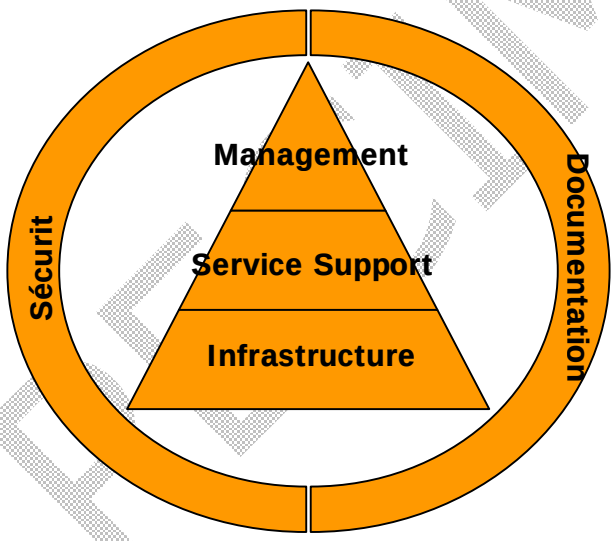
SPECIMEN

2. Démarche utilisée

L'objectif est d'évaluer la situation actuelle de l'exploitation informatique de l'entreprise et de préconiser des actions d'amélioration.

L'évaluation portera sur les cinq domaines suivants :

1. **La qualité de l'infrastructure informatique et le positionnement des choix technologiques, tant d'un point de vue du matériel (réseau, câblage, parc PC et imprimantes, serveurs) que d'un point de vue groupware ;**
2. **Le support reçu par les utilisateurs informatiques (helpdesk) ainsi que la gestion des changements et la gestion des configurations et des versions, désigné ci-après par le terme « Service Support » ;**
3. **Les activités de gestion du système d'information : la gestion financière, la gestion de projet, la gestion des acquisitions et des fournisseurs ;**
4. **La sécurité du système d'information visant à garantir la protection et l'intégrité des données grâce à la fiabilité de l'alimentation électrique, des sauvegardes des données, des mesures anti-virus et la gestion des mots de passe ;**
5. **gestion documentaire au travers de l'inspection de documents.**



Le présent rapport final comprend, pour chacun de ces domaines :

- **une synthèse des forces et faiblesses,**
- **une analyse détaillée basée sur les entretiens réalisés et les documents fournis,**
- **des recommandations pragmatiques.**

Une synthèse finale présente une vue d'ensemble sur la situation actuelle de l'exploitation informatique au travers :

- **D'un tableau global des forces et des faiblesses,**
- **D'un graphique des niveaux de maturité pour les 5 domaines de l'évaluation,**
- **D'une proposition de programme d'amélioration sur base de la liste des recommandations.**

SPECIMEN

3. Evaluation des pratiques en matière de management

3.1 Synthèse

Ce chapitre s'intéresse aux processus de management de la fonction informatique suivants :

- **la gestion des acquisitions,**
- **la gestion des fournisseurs,**
- **la gestion des projets,**
- **la gestion financière.**

Sans se vouloir exhaustive, cette liste tente de cibler les activités de gestion informatique les plus usuelles.

<u>En résumé :</u>

Les principales forces sont :

- **L'évaluation des besoins (demandes au personnel ou suggestions) et l'écoute**
- **La fidélité vis-à-vis des fournisseurs**

Les faiblesses identifiées sont :

- **L'absence d'élaboration d'un budget informatique**
  - **Le manque de visibilité à long terme**
  - **La gestion des besoins au coup par coup**
- **L'absence de contrats de maintenance sur certains éléments vitaux**
- **L'absence de techniques de gestion de projet**

Des recommandations pragmatiques sont données en fin de chapitre.

SPECIMEN

3.2 Rapport détaillé

3.2.1 Gestion des acquisitions

3.2.1.1 Acquisition de matériel

Le matériel acheté/à acheter par *SPECIMEN SA* est sélectionné la plupart du temps par Jean Durand, qui se place ici comme décideur. Il est le point de contact final entre la société et le/les fournisseur(s) de matériel.

Des recommandations peuvent être émises par le personnel en ce qui concerne les problèmes matériels et le remplacement de certaines parties, et généralement, les utilisateurs sont écoutés.

Le prix de l'acquisition n'a que peu d'importance dans le processus décisionnaire d'achat. Le choix sera plus fonction des performances attendues et des capacités du produit.

Les acquisitions matérielles sont réalisées au coup par coup.

3.2.1.2 Acquisition de logiciel

L'acquisition des logiciels et des licences se fait généralement via l'achat du PC, qui inclut le prix de la licence Windows et Office.

En ce qui concerne les logiciels métier, les achats sont effectués avec plus de réflexion que pour le matériel. Une analyse complète des besoins est réalisée en collaboration avec les utilisateurs (Gebat, par exemple).

Les décisions sont alors prises en accord avec les demandes des utilisateurs et les différents fournisseurs possible.

Les utilisateurs sont impliqués dans le choix, la gestion de projet et l'optimisation/adaptation du logiciel.

3.2.2 Gestion de projet

Les projets informatiques chez *SPECIMEN SA* sont surtout des projets de modification de logiciels métiers. Peu de projets ont concerné le matériel.

Les contacts sont généralement répartis pour bien cerner les nécessités de chacun avec sa spécialité.
Les fournisseurs potentiels sont analysés et sélectionnés pour la réponse finale.

En ce qui concerne la gestion de projet en elle-même, peu de documentation existe, comme un template de gestion de projet, par exemple. La pro activité semble peu présente.

Notes : un projet d'achat et d'adaptation avec migrations des données de l'actuel système comptable est en cours de réalisation

SPECIMEN

3.2.3 Gestion des fournisseurs

Le fournisseur privilégié de matériel, ainsi que le conseiller en ce domaine est la société de service EXEMPLE SA située à Xxxxxx, et en particulier Mr Pierre.

EXEMPLE SA est le fournisseur attitré de *SPECIMEN SA*, même si d'autres sociétés sont contactées. Néanmoins, ces dernières ne sont sollicitées que pour comparaison et informations. EXEMPLE SA est également le fournisseur principal au niveau services.

Pour des commandes spécifiques, *SPECIMEN SA* peut faire appel au fournisseur en direct (on pense à l'imprimante réseau, par exemple).

En termes de logiciels métiers, *SPECIMEN SA* traite en direct avec les différents partenaires susceptibles de répondre à leurs besoins.

Les différents contacts auprès de ces fournisseurs sont gérés par Jean Durand.

3.2.4 Gestion financière

La personne garante de la tenue financière des dépenses informatiques est Jean Durand.

Les dépenses informatiques ne sont pas gérées par budget, étant donné que les dépenses sont effectuées au coup par coup.

En ce qui concerne le montant des dépenses à effectuer, le prix n'a que peu d'importance, pour autant que la demande soit justifiée.

Quelques informations sont disponibles concernant les dépenses informatiques. Le système comptable actuel, en cours d'amélioration, devra inclure cet aspect, et donc fournir plus d'informations financières.

D'après les responsables, l'informatique « coûte cher » pour les résultats obtenus. Pourtant, il ne manquerait « pas grand-chose » pour que cela aille mieux.

Quelques chiffres récoltés :

Valeur à l'achat de :	
PCs et écrans (15) :	**33500 €**
Imprimantes :	**15000 €**
Scanner et Fax :	**29500 €**
Palms :	**2200 €**
Serveurs / UPS / Rack / Réseau :	**15500 €**
Interventions Année 2004 :	**7300 €**
Supplies Année 2004 :	**7000 €**

SPECIMEN

3.2.5 Gestion des niveaux de service

Les niveaux de service (SLA ou Service Level Agreement) sont inexistants chez *SPECIMEN SA* en ce qui concerne les interventions, le support ou le matériel informatique. Il n'y a pas non plus de contrats de maintenance hors ceux de la garantie fournisseur.

Il existe néanmoins des contrats en ce qui concerne la téléphonie, les copieurs et certains logiciels métiers.

Cette situation pourrait, en cas de problème grave, mener à des interruptions de service et donc des pertes de production pour l'entreprise.

SPECIMEN

3.3 Recommandations

Les recommandations sont les suivantes :

- **R.MGT.1 : Améliorer la gestion financière**
- **R.MGT.2 : Souscrire à un contrat de maintenance**
- **R.MGT.3 : Mettre en place un suivi de projets**

R.MGT.1 **Améliorer la gestion financière**	**Certaines entreprises ont rarement conscience des coûts financiers dus à la perte de productivité suite à une mauvaise planification ou liée aux incidents.** **Des pistes d'améliorations sont :** • **Etablir un budget annuel pour l'informatique.** • **Planifier à l'avance les besoins en matériel et licences en améliorant le suivi des achats.**
R.MGT.2 **Souscrire à un contrat de maintenance**	**Constatation est faite qu'aucun contrat de maintenance hors garantie du fabricant n'est pris chez *SPECIMEN SA*, ce qui peut mener à une interruption grave de service (notamment au niveau du serveur). La disponibilité des pièces de remplacement ou/et des ingénieurs compétents n'est pas toujours garantie sans ce genre de contrat.** **Un contrat de support ou de maintenance garantit, en cas de panne hardware, que les pièces sont disponibles très rapidement et donc que l'activité peut reprendre dans les meilleurs délais.** **Opter pour un contrat de maintenance au moins au niveau des éléments critiques (Server, ligne Internet, router)**
R.MGT.3 **Mettre en place un suivi de projets**	**Des expériences précédentes et désagréables ont un peu refroidi l'entreprise *SPECIMEN SA* en ce qui concerne les projets d'envergure (sur les logiciels métier). La situation s'est presque représentée avec la migration du logiciel de comptabilité, qui traîne depuis des mois, et qui maintenant semble repartis sur des bons rails.** **La mise en place d'une gestion de projet éviterait de perdre du temps et surtout de pouvoir tenir des délais en obligeant les fournisseurs à des résultats.**

4. Evaluation des pratiques en matière de support

4.1 Synthèse

Le Service Support regroupe :

- **la gestion des incidents et des problèmes (helpdesk) ;**
- **la gestion des changements ;**
- **la gestion des configurations et des versions.**

<u>En résumé :</u>

Les principales forces sont :

- **Les connaissances informatiques internes pour le helpdesk direct,**
- **Les versions récentes des systèmes d'exploitation et des versions Office,**
- **La disponibilité des personnes de contact de la société de service actuelle.**

Les faiblesses identifiées sont:

- **Les soucis quant à la compétence technique, et donc un impact sur la qualité de travail,**
- **Le manque de suivi dans les incidents et/ou les problèmes.**

Des recommandations pragmatiques sont données en fin de chapitre.

SPECIMEN

4.2 Rapport détaillé

4.2.1 Gestion des problèmes et des incidents (helpdesk)

4.2.1.1 Organisation du helpdesk

En fonction de la personne interrogée et de son niveau de connaissance des différents produits utilisés, la première source d'information est différente.

En interne, plusieurs personnes ont montré des compétences dans les différents domaines utilisés par *SPECIMEN SA* : Gebat, Link, la bureautique, certaines personnes comme la secrétaire utilisant plus la bureautique, par ex.

Dans le cas où le souci est trop conséquent ou bloquant, la société de service EXEMPLE SA est appelée (Mr Pierre) par le responsable informatique ou même par les utilisateurs eux-mêmes

4.2.1.2 Gestion des incidents

En cas de panne ou d'incident, la réaction des utilisateurs de *SPECIMEN SA* est d'abord de trouver une solution par eux-mêmes, et surtout en interne (GEBAT, LINK,…).

Lorsque les connaissances ou l'aide ne suffisent pas, les utilisateurs ou le responsable IT prennent contact avec la société de service intervenant chez *SPECIMEN SA*.

La gestion des incidents est donc réalisée par téléphone. La société EXEMPLE SA peut prendre la main à distance via VPN pour corriger certains aspects.

Dans le cas des logiciels métiers (GEBAT, LINK), une personne qualifiée en interne (Paul, Jacques) est contactée en premier. Si la solution n'est pas trouvée, l'éditeur peut être appelé et dispose d'un helpdesk assez performant.

Pour des incidents ou des changements plus conséquents, un fichier est tenu à jour par *SPECIMEN SA* (à sa propre initiative), reprenant les questions, problèmes, pannes, manipulations et changements à effectuer au prochain passage de EXEMPLE SA. Malheureusement, cette liste n'est pas toujours bien suivie par EXEMPLE SA.

En cas de panne sérieuse, aucun contrat de support externe n'existe pour les postes ni pour le serveur, ce qui pourrait amener à des pertes de productivité. A priori, les délais d'intervention sont acceptables – il n'y a jamais eu de panne très grave.

On remarque également un manque de communication entre *SPECIMEN SA* et la société EXEMPLE SA, au niveau du suivi des interventions. Le travail n'est souvent fait qu'à moitié.

SPECIMEN

4.2.1.3 Gestion des problèmes

Il n'y a pas à proprement parler de gestion de problèmes, mis à part le remplissage du document de travail édité par *SPECIMEN SA* pour EXEMPLE SA, que ces derniers devraient compléter.

Pourtant des problèmes sont apparemment présents chez *SPECIMEN SA* (Problème de déconnexion du réseau, messages d'erreur sur le backup).

La société EXEMPLE SA gère apparemment les problèmes comme des incidents et avec des méthodes plutôt radicales (réinstallation des postes en Windows 2000 parce que ça ne va pas en XP). Les explications ne sont pas toujours fournies.

Les problèmes rencontrés ne sont pas forcément solutionnés, mais plutôt éliminés jusqu'à leur prochaine manifestation. Pas d'investigation sur la cause du problème. On essaie des solutions jusqu'à trouver celle qui arrange le mieux.

4.2.1.4 Conclusions relatives au helpdesk

En résumé, la technique de helpdesk est moyennement implémentée chez *SPECIMEN SA*, en ce sens que les personnes de contact sont bien établies (le responsable informatique, et les gens compétents dans chaque domaine) mais lorsque le problème devient conséquent, plutôt que se tourner vers un interlocuteur unique, chacun choisit sa ligne de conduite, encore une fois en fonction du type de problème (appel de l'éditeur pour chacun des logiciels métiers, appel de EXEMPLE SA pour les problèmes d'ordre général).

Les utilisateurs sont très moyennement satisfaits en ce qui concerne la résolution des incidents. Il convient de faire 2 distinctions :

- **Les éditeurs des logiciels métiers sont compétents en matière de rapidité et de qualité de service (GEBAT, LINK, Compta).**
- **Le prestataire de service EXEMPLE SA propose un service rapide (proximité et prise en main à distance), mais ne satisfait pas les utilisateurs en ce qui concerne la qualité technique des interventions et/ou des solutions.**

4.2.2 Gestion des changements

Au niveau des logiciels métier, des changements progressifs sont mis en place par certains utilisateurs, eux-mêmes (téléchargement Internet), lorsque le besoin s'en fait sentir, ou lorsque des fonctionnalités supplémentaires sont nécessaires (GBAT, LINK)

Pour ce qui est de la bureautique en général, les modification sont de 2 types : les mises à niveau et correctifs, et les réinstallations.

Les mises à niveau des différents softwares (service packs, service releases, versions Windows) sont effectuées au besoin. Il n'y a pas d'installation préventive. Les

SPECIMEN

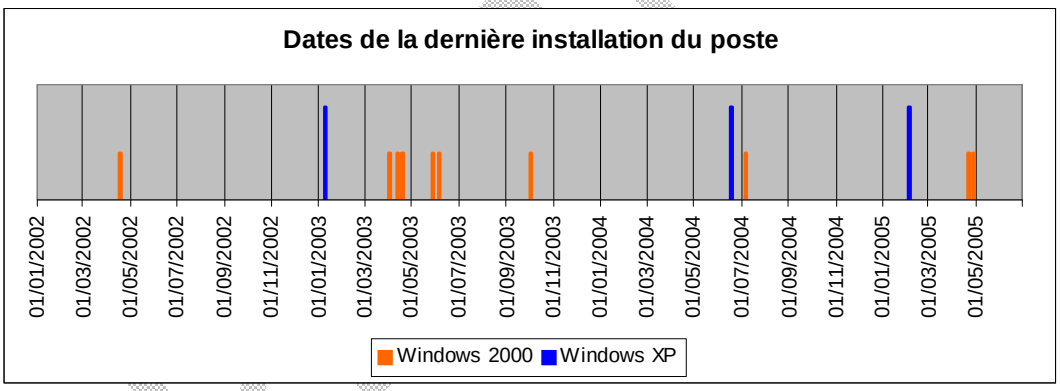
correctifs, quant à eux, sont appliqués à la demande (cfr. document rempli par *SPECIMEN SA* et par EXEMPLE SA) et lors des interventions de Mr Pierre.

Par manque de temps et de compétences, toutes les modifications demandées ne sont pas toujours effectuées ou le sont à moitié, ce qui implique une deuxième intervention. Ce genre de changement amène parfois à des problèmes (mots de passe, accès, plantages, arrêts de travail).

Lors de réinstallations, l'oubli de softwares est monnaie courante. Pourtant, un tableau réalisé par *SPECIMEN SA* indique les différents softwares à installer en fonction du poste. Les dernières réinstallations de postes sont assez récentes, elles datent du mois d'avril (cfr tableau suivant). Un tableau d'installations, édité par *SPECIMEN SA*, aurait dû être mis à jour par EXEMPLE SA.

Note : Une mise à niveau en Windows XP avait été faite sur certains postes, puis, suite à de gros problèmes, EXEMPLE SA a décidé de revenir en arrière pour retrouver Windows 2000. Le problème qui était apparu a été réglé en revenant à la version précédente.

Lorsque des tests sont à effectuer, le poste de Frédéric Mathieu peut être utilisé pour valider les nouvelles installations.



4.2.3 Gestion des configurations et des versions

4.2.3.1 Matériel hardware – PCs – Serveurs – Imprimantes

L'entreprise *SPECIMEN SA* dispose de matériel de différents types :

- **PCs « produit blanc » (15), portables (2) non pris en compte**
- **4 serveurs « produit blanc » dont 1 dispose d'un tape**
- **1 imprimante réseau Xerox**
- **8 imprimantes locales (deskjet/Laserjet, B&W/color)**
- **Switch 50 Ports**
- **Boîtiers Wireless**
- **Connexion vers Internet à travers un routeur**

Le matériel présent est relativement récent, aussi bien pour les postes de travail que les serveurs. En ce qui concerne les postes de travail, 2 postes sont assez anciens, et d'ailleurs installés en Windows 95 et Windows 98.

Les serveurs sont de deux types : l'un est récent (Xeon 2.6 GHz) , les 3 autres sont plus anciens (Pentium III 1 GHz).
Note : le serveur vidéo est installé en Windows 98.

L'imprimante réseau est récente et les imprimantes locales semblent convenir à leur utilisation quotidienne.

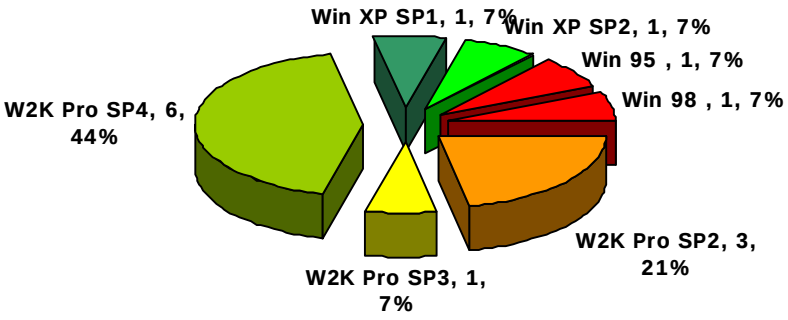
4.2.3.2 Logiciel

Les différentes versions de système d'exploitation et de Office suite bureautique ne sont pas forcément installées par *SPECIMEN SA*. Elles sont préchargées sur les PCs et dont utilisables immédiatement par les utilisateurs dès l'arrivée d'un nouveau PC. EXEMPLE SA se charge de la réinstallation éventuelle et des mises à jour ponctuelles
Par le biais de cette technique d'installation, des versions différentes de système d'exploitation, de service Pack, de version d'Office différentes se retrouvent sur tous les PC's et sur le serveur.

Le tableau suivant montre les différentes disparités entre les versions Windows Installées sur les PCs.

SPECIMEN

Répartition des Systèmes d'exploitation



Les versions Office, quant à elles, sont toutes quasi sur le même pied d'égalité : Office 2000 Professional (2 postes sont en Office 2000 Pro SR-1).

Des réinstallations de postes ont déjà eu lieu, mais dans ce cas, il n'y a pas forcément de cohérence dans le choix d'une version de système d'exploitation ou d'une version d'Office.

Les serveurs, eux, sont installés en Windows 2000, Service pack 4, exception faite du serveur vidéo, installé en Windows 98.

4.2.4 Niveau de satisfaction

Du côté matériel et infrastructure, les utilisateurs se sont tous montrés contents, que ce soit au niveau des imprimantes que des postes ou encore des écrans. L'utilisation des différents logiciels est également satisfaisante. Les softwares métier sont régulièrement adaptés en fonction des demandes de chacun.

En ce qui concerne le helpdesk, les utilisateurs sont contents au niveau temps de réponse et délai de réparation.

La qualité de service dépend du point de contact. Lorsqu'il s'agit de logiciels métier (GEBAT, LINK), les utilisateurs sont satisfaits du support et des produits. Lorsque l'on parle de la bureautique, les compétences techniques de la société de service EXEMPLE SA sont remises en cause, de même que la réalisation incomplète des installations et le suivi. On parle de « Kamikaze » ou de « bidouilleur ».

Des améliorations sont à pourvoir dans le domaine de l'organisation de la structure fichiers du serveur.

La cote de satisfaction au niveau informatique a été estimée à 14/20 en moyenne.

SPECIMEN

4.2.4.1 Bureautique

Les utilisateurs sont contents de leurs outils (PC, écran, imprimante, …) et estiment que cela leur est suffisant pour réaliser leur travail de tous les jours. Même si des versions différentes de Windows sont détectées sur les différents PCs, cela n'apparaît pas comme problématique au niveau de l'utilisateur.

Aucun logiciel pirate n'a été installé, ni même détecté.

Lors de l'inventaire, des versions différentes d'antivirus ont été détectées (Norton antivirus, Mcafee, Panda et Bit Defender). En ce qui concerne les signatures, elles sont différentes en fonction de l'antivirus installé sur les postes de travail. Certains postes n'ont pas d'antivirus – Ceci est critique.

Les mises à jour Antivirus se font en direct via Internet , à chaque démarrage du poste ou de l'antivirus. Chaque poste est configuré pour accéder aux téléchargements en direct, sans passer par un serveur interne. Il peut arriver que les signatures datent d'une semaine, voire plus.

Le serveur de fichiers est équipé d'un antivirus : NAV (signature Jan 2004)
Les serveur de mails, de compta et vidéo n'en ont pas.

4.2.4.2 Accès Internet et e-mail

L'utilisation d'Internet et surtout de l'outil de mailing sont importants pour *SPECIMEN SA*. Microsoft Outlook est l'outil indispensable en ce qui concerne les contacts avec l'extérieur.

Pour ce qui est de l'interne, LINK est généralement préféré, car il intègre les fonctions de mémos et d'agenda, et peut même être lié avec Outlook le cas échéant. L'utilisation de l'agenda partagé est journalière et très fréquente.

En ce qui concerne les adresses mail, chaque utilisateur a sa propre adresse, mais localisée parfois à des endroits et chez des providers différents. En effet, il existe des adresses mail chez EXEMPLE SA (specimen.com) et chez WIN (*Specimensa.be*). Ces adresses sont des adresses POP3 et nécessitent donc une connexion Outlook vers l'extérieur. Tous les PCs sont donc connectés en permanence sur Internet.

Note : les envois de mails des adresses *Specimensa.be* sont gérés par le serveur de mails Artisoft XtraMail. Par contre, la réception est purement en POP3.

L'utilisation faite du serveur XtraMail est un point à soulever. En effet, d'après l'analyse, Il apparaît clairement que les mails ne sont pas stockés au niveau du serveur, mais bien sur les postes locaux, téléchargés directement depuis Win et EXEMPLE SA.

On conviendra donc d'un remodelage de la configuration mail aussi bien au niveau serveur que station.

SPECIMEN

4.2.4.3 Les souhaits des utilisateurs

Les pistes d'amélioration suivantes ont été émises par les utilisateurs :

- **Une meilleure qualité de service au niveau de la société EXEMPLE SA.**
- **La résolution des problèmes de mails et de déconnexions**
- **Une meilleure organisation de la société EXEMPLE SA.**
- **Un meilleur suivi de la part de EXEMPLE SA.**
- **Une meilleure gestion des projets (migration compta, par exemple).**
- **Un travail correctement effectué et achevé, et non toujours partiellement (les oublis).**
- **Une compétence plus « professionnelle » de la part de EXEMPLE SA.**

SPECIMEN

4.3 Recommandations

Les recommandations sont les suivantes :

- **R.SUP.1 : Adopter une politique de gestion des versions antivirus**
- **R.SUP.2 : Adopter d'une politique de gestion des problèmes**
- **R.SUP.3 : Mettre à niveau des différentes versions**

R.SUP.1 **Adopter une politique de gestion des versions antivirus**	**Bien qu'un antivirus soit présent sur quasi tous les postes, la mise à jour des signatures antivirus répond dans le cas de *SPECIMEN SA* à des contraintes différentes concernant le téléchargement des mises à jour antivirus. Des versions différentes impliquent des configurations différentes et une gestion différente. Actuellement, chaque poste télécharge ses signatures. Cette solution, viable à court terme, est à améliorer par exemple :** • **En souscrivant un abonnement « corporate » qui permettrait de ne pas avoir à gérer un abonnement par PC.** • **En changeant de version d'antivirus pour en venir à une solution centralisée (serveur et client), qui elle, autorise le téléchargement sans abonnement, et l'envoi automatique des mises à jour sur les postes de travail.** **Tenir des versions d'antivirus à jour et surtout le suivre tient du challenge avec 4 éditeurs différents sur les 15 postes.** **Il est recommandé de centraliser la gestion des antivirus sur un serveur ou établir une procédure de mise à jour et de lancement régulier d'un scan antivirus des PCs**
R.SUP.2 **Adopter d'une politique de gestion des problèmes**	**Le but de cette recommandation est de diminuer au cours du temps le nombre d'incidents et/ou de pannes que ce soit au niveau du serveur ou des stations de travail.** **Lorsqu'un incident devient récurrent, on parle de « problème ». Il convient, dans le cas d'apparition d'un problème, de chercher des solutions définitives à ceux-ci, de façon à les éliminer, ainsi que les incidents s'y rapportant.** **Actuellement, le suivi n'est que peu établi. En améliorant ce suivi, les résultats seront :** • **un règlement plus rapide des problèmes,** • **une satisfaction au niveau des utilisateurs,** • **une stabilité accrue grâce à la justesse de la solution apportée.**

R.SUP.3 **Mettre à niveau des différentes versions**	**Les différents postes sont tous mis en place au moment de leur achat, sans toucher aux différentes versions (Windows / Office / Antivirus) de softwares installées sur ces postes.** **Les mises à jour de Service Packs de Windows et/ou Office ne sont pas réalisées.** **Il convient de mettre tous les postes au même niveau, au moins Windows et Office, et de prévoir une politique de mise à jour de ces versions : STANDARDISER.** **Cette recommandation s'applique également au niveau des serveurs.** **On peut également préconiser d'automatiser et de suivre les techniques Windows Update grâce à une configuration des postes et/ou un serveur SUS (Update Services).** **Mise à niveau des postes en Windows XP SP2** **Mise à niveau des versions Office en Office 2003 SP1** **Politique de gestion des versions**

SPECIMEN

5. Evaluation de l'infrastructure informatique

5.1 Synthèse

Ce chapitre s'intéresse aux composants, tant matériels que logiciels, de l'infrastructure informatique suivants :

- **Le passif :**
  - **Local technique,**
  - **Câble,**
  - **Patch panel ;**
- **Le réseau:**
  - **Méthode d'accès / topologie,**
  - **Hub et switch,**
  - **Routeur;**
- **Les serveurs;**
- **Les PCs ;**
- **Les imprimantes ;**
- **Le groupware.**

Sans se vouloir exhaustive, cette liste tente de recenser les composants de l'infrastructure les plus importants.

<u>En résumé :</u>

Les principales forces sont :

- **Des postes de travail récents et performants,**
- **Des systèmes d'exploitation « de réseau » (Pas de Win95/98/Me, sauf exceptions),**
- **L'utilisation fréquente de l'agenda partagé,**
- **L'utilisation de Link pour la communication interne et le stockage de documents,**
- **Des serveurs dans un rack qu'il est possible de fermer à clé.**

Les faiblesses identifiées sont:

- **Local technique non sécurisé – climatisé – dédié,**
- **L'utilisation d'un système d'adressage fixe,**
- **Une politique de nommage PC non établie,**
- **Une architecture « Workgroup » alors que tout est prêt pour travailler en « Domaine »,**
- **La présence de données locales sur les PCs (mail et fichiers),**
- **L'absence de centralisation des :**
  - **Fichiers**
  - **Mails**
  - **Impressions**
  - **Gestion users et mots de passe**
  - **Gestion droits d'accès.**

Des recommandations pragmatiques sont données en fin de chapitre.

SPECIMEN

5.2 Rapport détaillé

5.2.1 Analyse du passif

5.2.1.1 Local technique

Le local technique de *SPECIMEN SA* se trouve dans une salle ouverte et accessible par tout le personnel.

Les serveurs (4) sont installés dans un rack 42U installé dans ce local. Il est relativement bien ventilé, si la porte en est ouverte (donne sur le garage).

Des produits d'entretien de piscine et d'étangs sont néanmoins disposés à côté de ce rack.

Le local décrit ne possède pas de système de détection incendie, ni de système de climatisation, quoique ce dernier ait déjà été demandé par certains responsables.

Le rack serveur a d'ailleurs été déplacé dans cette salle après avoir été stocké pendant un moment dans un local trop petit (et donc trop chaud).

Il est à noter également que cette salle renferme une armoire à documents, archives de la société.

5.2.1.2 Câble réseau et Patch Panel

En ce qui concerne le câblage, *SPECIMEN SA* utilise du câble RJ 45 en Ethernet 100 Mbps.

Tous les postes de la société sont reliés à un switch. Les câbles vers la salle serveur sont en câblage direct. Les autres passent par des goulottes le long des murs. Il n'y à pas de patch panel à proprement parler.

Le seul switch de la société se trouve dans un petit local d'entretien, fixé au mur à environ 2m du sol. Il n'est pas dans un rack

5.2.2 Analyse du réseau

5.2.2.1 Méthode d'accès / Topologie

Les postes de travail sont configurés en adresses fixes. Les adresses ainsi configurées ne répondent pas à une technique d'attribution particulière, mais sont gérées au coup par coup, ce qui entraîne des disparités au niveau de l'homogénéité de cet adressage. Le range d'adresses utilisées est le xxx.xxx.x.x

Les 4 serveurs sont également installés sur le même réseau IP, mais 3 seulement d'entre eux communiquent avec le réseau (un serveur vidéo n'est pas connecté).

SPECIMEN

Adresses IP des serveurs

SERVEURNT	xxx.xxx.x.x
SERVEURMAIL	xxx.xxx.x.x
PICK	xxx.xxx.x.x

Adresses IP des stations

PIERRE	xxx.xxx.x.x
GARAGE	xxx.xxx.x.x
PAUL	xxx.xxx.x.x
VERONIQUE	xxx.xxx.x.x
ISABEL	xxx.xxx.x.x
EMMA	xxx.xxx.x.x
CAROLE	xxx.xxx.x.x
SALLE-REUNION	xxx.xxx.x.x
CLAUDE	xxx.xxx.x.x
...	xxx.xxx.x.x
...	xxx.xxx.x.x
...	xxx.xxx.x.x
...	xxx.xxx.x.x
...	xxx.xxx.x.x
...	xxx.xxx.x.x

Le principe est de garder les serveurs en adresse fixes.

Par contre, pour les stations de travail, on peut conseiller un serveur DHCP, qui ne prend que peu de ressources, et qui permet un adressage automatique des stations via le serveur. Cela simplifie l'administration et évite de devoir chercher après des adresses libres sur le réseau. La sécurisation de ce serveur DHCP peut être une option.

3 sites sont interconnectés : *SPECIMEN SA* (XXXXX), Exemple SA (xxxxx) et Exemple2 SA (XXXXXX).

Ces deux derniers sont interconnectés avec *SPECIMEN SA* par des lignes bas débit (ISDN) 256 Kbps et 128 Kbps.

Note : lors de l'évaluation, seule l'entreprise *SPECIMEN SA* de Xxxxxx a été prise en compte.

SPECIMEN

5.2.2.2 Hub et Switch

SPECIMEN SA **utilise du câble RJ 45 en Ethernet 100 Mbps. Le switch utilisé est un switch 3Com Superstack 3 Baseline 50 Ports 100Mbps. Ce switch sert à connecter les serveurs, les stations de travail ainsi que l'imprimante partagée.**

Deux ports Gigabit sont disponibles sur ce switch, mais nous n'avons pas identifié s'ils se connectaient aux serveurs. Si ce n'est pas le cas, la connectique Gigabit sur serveur serait une meilleure solution.

Deux boîtiers wireless avec antenne interconnectent le bâtiment principal avec le garage. Ce sont des boîtiers Buffalo AirStation Pro.
Le poste du garage est connecté en direct sur ce boîtier.
Le boîtier du bâtiment principal est connecté, lui, sur le switch 3Com.

5.2.2.3 Routeur

Le seul router installé (Cisco 800) sert à connecter l'entreprise à Internet. La ligne louée est maintenue par WIN, filiale de Belgacom, opérateur téléphonique belge, situé à Xxxxxx.

Aucun Firewall n'a été détecté sur le serveur lui-même. La société WIN, qui gère les accès externes dispose d'un Firewall.

Un accès VPN est possible depuis l'extérieur, car la société de service peut prendre le contrôle à distance grâce à l'outil VNC.

Le router est la propriété de WIN. Le mot de passe est connu par WIN.

SPECIMEN

5.2.3 Serveurs

Les serveurs de *SPECIMEN SA* sont configurés comme suit :

Nom du serveur	SERVEURNT	SERVEURMAIL
Operating system	Windows 2000 Server	Windows 2000 Server
Service Pack	4	4
Type	Serveur "produit blanc"	Serveur "produit blanc"
CPU	Intel Xeon-A; 2600 MHz	Intel Pentium IIIE; 1000 MHz
RAM	2048 MB	512 MB
Contôleur disque	Adaptec SCSI RAID 2200S	Adaptec AIC-7899
Disques	2 x 18.2 GB RAID1	1 x 3 GB IDE
	2 x 72.8 GB RAID1	1 x 36.4 GB SCSI
Partitions	C:\ : 17437 Mo (4580 Mo libre)	C:\ : 1999 Mo (1092 Mo libre)
	D:\ : 70087 Mo (7879 Mo libre)	D:\ : 35071 Mo (2630 Mo libre)
		E:\ : 1078 Mo (264 Mo libre)
Adresse IP	xxx.xxx.x.x	xxx.xxx.x.x
Subnet mask	xxx.xxx.x.x	xxx.xxx.x.x
Default gateway	xxx.xxx.x.x	xxx.xxx.x.x
Serveurs DNS	xxx.xxx.x.x	xxx.xxx.x.x
	xxx.xxx.x.x	xxx.xxx.x.x
Vitesse réseau	1000 Mbps	100 Mbps
Rôles	Serveur de fichiers	Serveur de mails
	Contrôlleur de domaine	

Nom du serveur	PI	PC
Operating system	Windows 2000 Server	Windows 98 SE
Service Pack	4	N/A
Type	Serveur "produit blanc"	Serveur "produit blanc"
CPU	Intel Pentium IIIE; 1000 MHz	Intel Pentium IIIE; 1000 MHz
RAM	512 MB	128 MB
Contôleur disque	Adaptec AIC-7899	Adaptec AIC-7899
Disques	1 x 80 GB IDE	1 x 6 GB IDE
Partitions	C:\ : 78152 Mo (64721 Mo libre)	C:\ : 6144 Mo (2099 Mo libre)
Adresse IP	xxx.xxx.x.x	xxx.xxx.x.x
Subnet mask	xxx.xxx.x.x	xxx.xxx.x.x
Default gateway	xxx.xxx.x.x	xxx.xxx.x.x
Serveurs DNS	xxx.xxx.x.x	xxx.xxx.x.x
	xxx.xxx.x.x	xxx.xxx.x.x
Vitesse réseau	100 Mbps	100 Mbps
Rôles	Serveur Compta	Serveur Video

5.2.4 PC

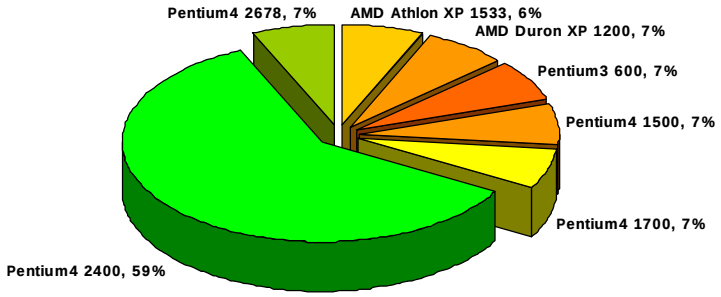
On trouve dans le parc informatique de *SPECIMEN SA* différents types de postes de travail, avec des processeurs différents, des tailles mémoires différentes, des configurations différentes. Les achats des postes « en fonction des besoins » ont fait que les configurations étaient fonction du marché de l'époque. Des upgrades n'ont pas forcément été réalisés.

Cette hétérogénéité est explicitée ci-après

5.2.4.1 Exemple de répartition des processeurs

Les différentes stations de travail (PC et laptops), étant donné leur achat à différentes époques, ont des processeurs différents :

Répartition des processeurs

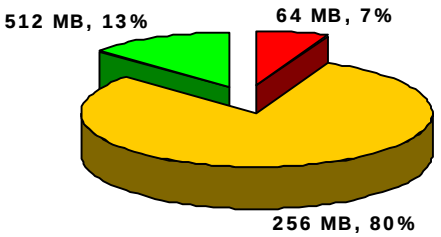


Les disparités processeur sont dues aux périodes d'achat, mais en ce qui concerne le fonctionnement des machines, aucune plainte n'a été formulée.

5.2.4.2 Disparité de la taille de la mémoire RAM

Les différentes stations de travail (PC et laptops), étant donné leur achat à différentes époques, ont des tailles mémoire différentes :

Répartition de la mémoire

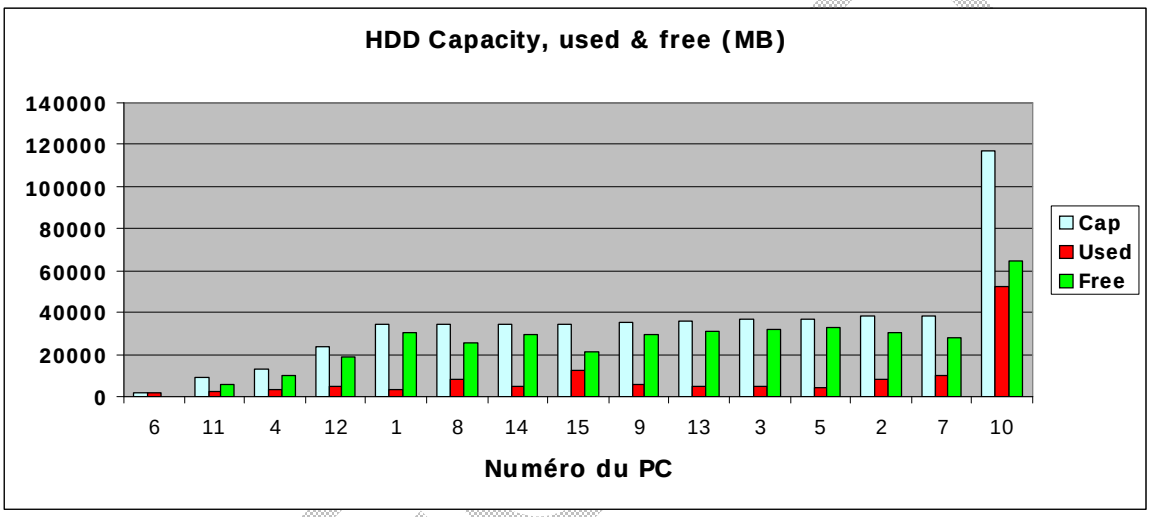


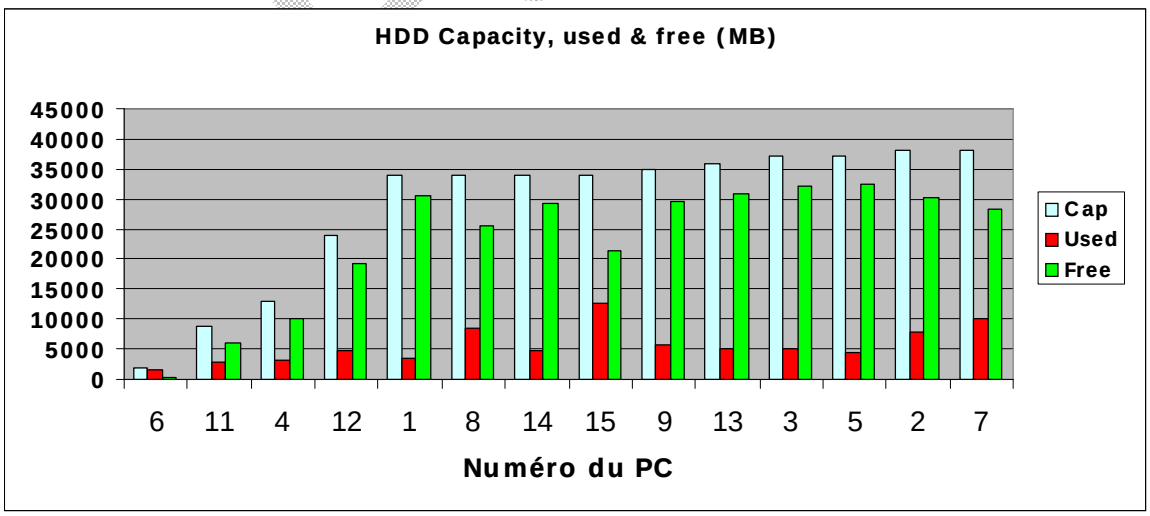
Les disparités mémoire présentent moins d'importance au niveau du fonctionnement et de l'utilisation des stations de travail. Les disparités mémoires, comme celles des processeurs, sont dues aux périodes d'achat, mais en ce qui concerne le fonctionnement des machines, aucune plainte n'a été formulée.

Il faudrait cependant songer à un upgrade mémoire car les applications futures sont gourmandes

5.2.4.3 Stockage de données locales sur le PC et nomenclature

Les différentes stations de travail ont une configuration disque comme suit :





Le premier graphique tient compte du PC 10, qui effectue un backup de certaines données des serveurs.
Le second graphique fait abstraction du PC 10 et montre les espaces utilisés en Rouge.

En regardant ces résultats, et cela a été confirmé par l'analyse, certains postes travaillent avec des données locales (Poste 15 : 12 GB utilisés, poste 7 : 10 GB utilisés). L'utilisation de données locales est un paramètre à prendre en compte lorsqu'on parle de sécurité des données. En effet, le plantage du disque dur pourrait impliquer de recommencer les différents projets en cours, les courriers, les tableaux et les différents documents stockés localement.

C'est pourquoi l'utilisation du serveur de fichiers s'impose.

En ce qui concerne le PC 10, la configuration est un peu particulière étant donné que ce PC réalise un backup synchronisé du serveur de fichiers. C'est donc la bouée de sauvetage de la société et il est normal de retrouver une grande quantité de données locales.

L'analyse des postes montre au total environ 50 GB de données stockées localement sur les des PCs (uniquement dans Mes Documents). La perte de ces données (non-backupées pour rappel) pourrait avoir des conséquences sur le business de la société (dossiers à recréer, contacts à reprendre, documents papier à retrouver, …).

Concernant les noms des postes de travail, ils sont attribués en fonction du nom de la personne l'utilisant, mais sans pour autant avoir une convention de nommage équivalente pour tous. Parfois NOM-PRENOM, ou NOM-INITIALES, ou NOM-DIMINUTIF. Les noms des PC, attribués en fonction de l'utilisateur, permettent de retrouver facilement la machine au niveau du réseau, mais ne permettent pas de la rendre « anonyme » - possibilité pour une personne de changer de poste en cas de problème.

Il est important d'avoir une politique de noms correcte afin de pouvoir identifier rapidement sur le réseau, les différentes stations. Dans le cas de *SPECIMEN SA*, le nommage comme effectué actuellement est suffisant. Néanmoins, si la société venait à grandir, une autre politique serait éventuellement à réfléchir (en fonction de la localisation, avec des numéros d'incréments), de façon à pouvoir intervertir plus facilement les postes et les utilisateurs (PC hors service, par exemple), et de façon à pouvoir les identifier plus rapidement pour le responsable informatique.

SPECIMEN

5.2.5 Imprimantes

Une seule imprimante réseau est installée au sein des bureaux de *SPECIMEN SA* :

Xerox Document Center CS50 PS

L'imprimante est connecté au réseau et a l'adresse IP : xxx.xxx.x.x
a le nom : XXXXX12345

L'imprimante n'est pas déclarée au niveau du serveur, mais est installée sur tous les postes comme une imprimante « locale », grâce au Print Server qui est configuré au sein même de l'imprimante. La configuration doit dès lors être faite sur tous le postes de travail.

La recommandation sera de déclarer cette imprimante sur le serveur afin que tous puissent en profiter et que l'installation soit plus simple

En ce qui concerne les autres imprimantes, nous trouvons 8 imprimantes locales deskjet ou laserjet, noir et blanc ou couleur :

2	HP	Laserjet 1100	B&W
1	HP	Deskjet 1120C	Color
4	HP	Laserjet 1200	B&W
1	HP	Deskjet 895C	Color

Ces imprimantes sont installées localement sur certains postes de travail et sont partagées pour être disponibles pour d'autres postes et/ou d'autres utilisateurs. Cette technique implique que le poste sur lequel l'imprimante est physiquement connectée soit démarré pour que l'imprimante soit accessible.

De surcroît, si une grosse impression est lancée, ce poste précis va réaliser l'opération de spooling (préparation de l'impression) , ce qui va ralentir le poste proprement dit.

Cette contrainte peut être éliminée par l'utilisation de boîtiers réseau qui servent de mini serveur d'impressions pour les imprimantes de type deskjet ou laserjet ne disposant pas de carte réseau. L'installation et la configuration de tels boîtiers rendent disponibles toutes les imprimantes à tous les utilisateurs, ce qui en simplifie la gestion.

Il est également à noter que la multiplication des imprimantes et des types oblige la gestion des différentes cartouches et toners, et détail moins négligeable, leur prix. La centralisation des imprimantes en les partageant pour réduire leur nombre pourra avoir un impact sur les différents consommables.

Comme l'imprimante réseau est utilisée en majeure partie, il sera bon de vérifier les contrats de maintenance relatifs à celle-ci. En cas de non disponibilité, la rapidité de réparation pourra avoir un impact sur la productivité.

SPECIMEN

5.2.6 Infrastructure groupware

Groupware : Définition :

Classe de logiciels prévus pour être exploités par plusieurs utilisateurs en même temps, sur un même projet - logiciel de travail en groupe. Façon de travailler, basée sur les relations entre les membres d'un groupe (reliés par un réseau).

Ensemble d'outils destinés à favoriser le travail en équipe. Comme par exemple des logiciels permettant à un groupe d'utilisateurs de travailler en collaboration sur un même projet sans être nécessairement réunis. Au coeur des logiciels de travail de groupe, on retrouve un serveur de messagerie. Il est généralement complété par des outils de partage de documents, de gestion d'agenda, de gestion de contacts, de workflow, de vidéoconférence, etc…

Une infrastructure Groupware est donc destinée à faciliter le partage et l'accès de l'information pour tous les utilisateurs d'un groupe de travail.

5.2.6.1 Serveurs de fichiers

Bien que tous les noms d'utilisateurs soient définis au niveau du serveur, dans Active Directory Windows 2000, les utilisateurs se connectent à leur poste de travail avec un utilisateur local et pas un utilisateur réseau.

De la même façon, bien que le serveur soit configuré en contrôleur de domaine, les postes de travail sont configurés en mode Workgroup (avec parfois le nom du domaine comme nom de Workgroup).

Ces deux constatations impliquent que les droits d'accès sont gérés exclusivement avec des comptes locaux aux machines et aux utilisateurs.

Ce mode de travail peu pratique a plusieurs conséquences :

- **Gestion non centralisée des utilisateurs et/ou des mots de passe**
- **Gestion non centralisée des accès au réseau par les machines**
- **Complexité de la mise en place de droits d'accès sur le serveur (ce qui implique généralement un accès total pour tous afin de limiter la gestion).**
- **Nécessité de création de tous les utilisateurs partout (il faut avoir une synchronisation utilisateurs et mots de passe sur les différents PCs)**
- **Impossibilité de changer son mot de passe sans devoir le changer à plusieurs places (complexité de gestion)**

En ce qui concerne le système de fichiers et son arborescence actuelle, tous les utilisateurs ont droit d'accès à tout.

SPECIMEN

Ce système de droits a plusieurs implications, reliées aux constatations précédentes :

- **Chaque utilisateur a tous les accès**
  - **è possibilité de corruption malencontreuse de données par un autre utilisateur.**
- **Le fait de devoir se connecter avec un user local implique que les droits d'accès ne « suivent » pas l'utilisateur.**
- **L'indisponibilité des postes implique parfois la connexion d'un utilisateur sur un autre poste que le sien. Les droits ne « suivent » pas.**
- **La gestion des droits file serveur se fait en fonction des utilisateurs et des mots de passe**
  - **è obligation d'avoir le même mot de passe partout où l'utilisateur est défini, et donc au niveau du server.**

Il n'existe pas non plus de zones privées (home directory) par utilisateur au niveau du serveur.

La structure même de l'arborescence du serveur de fichiers, dans l'état actuel, ne satisfait pas forcément tous les utilisateurs (anarchie). Néanmoins, elle n'a que peu d'importance, car l'utilisation de Link comme base de données principale permet de stocker les documents de manière automatique, centralisée par link.

En résumé, même si un file serveur existe chez *SPECIMEN SA*, la façon de l'utiliser n'est pas du tout optimale. La gestion locale des utilisateurs et des mots de passe représente une surcharge d'administration si des modifications sont à effectuer.

Tous les éléments déjà en place sont réunis pour pouvoir centraliser la gestion de ces accès, mais rien n'est réalisé en ce sens. Quelques modifications mineures pourraient améliorer drastiquement la façon de gérer ces accès.

En ce qui concerne l'utilisation du produit Link, aucune plainte n'est ressortie au niveau de l'organisation des documents.

Il va de soi que, si tous les documents sont inclus dans Link, il est nécessaire de s'assurer de la stabilité de la base de données et de la possibilité de récupération de celle-ci (base propriétaire ou base standardisée).

SPECIMEN

5.2.6.2 La messagerie

La messagerie utilisée sur les postes de travail est Outlook (2000, XP ou 2003 en fonction des stations de travail).

Une grosse partie des communications internes de la société passe par LINK, qui permet de gérer l'agenda également.

2 suffixes d'adresse messagerie sont configurés chez *SPECIMEN SA* :
***@specimensa.be* (12 utilisateurs)**
***@specimen2.com* (2 utilisateurs)**

Les adresses *@specimen2.com* sont gérées à l'extérieur par un serveur POP3 et SMTP chez EXEMPLE SA, société de services située à Xxxxxxx.

Les adresses *@specimensa.be*, elles, sont gérées différemment :

Le serveur POP3 est interne (SERVERMAIL) et travaille avec le logiciel ArtiSoft XtraMail.

Le serveur SMTP, lui, est externe et hébergé chez WIN, filiale de Belgacom, opérateur téléphonique belge, situé à Xxxxxx.

Les clients Outlook sont configurés pour utiliser une connexion POP3/SMTP, qu'il soient *@specimensa.be* ou *@specimen2.com*. Cette connexion en POP3 télécharge les mails depuis le serveur, et les stocke dans un fichier (PST) de mail.

Ces fichiers PST sont stockés en local sur les stations de travail. En effet, une lettre du réseau (W) est configurée pour le mail, mais cette lettre est redirigée sur le disque dur local des stations de travail.

La même constatation et les mêmes remarques que pour les fichiers sont émises ici : le serveur de mails n'héberge pas les mailboxes, et suite à une panne de disque dur, les mails des utilisateurs seraient perdus.

En ce qui concerne la communication interne, LINK est le plus souvent utilisé, car il regroupe le système d'agenda et de tâches.

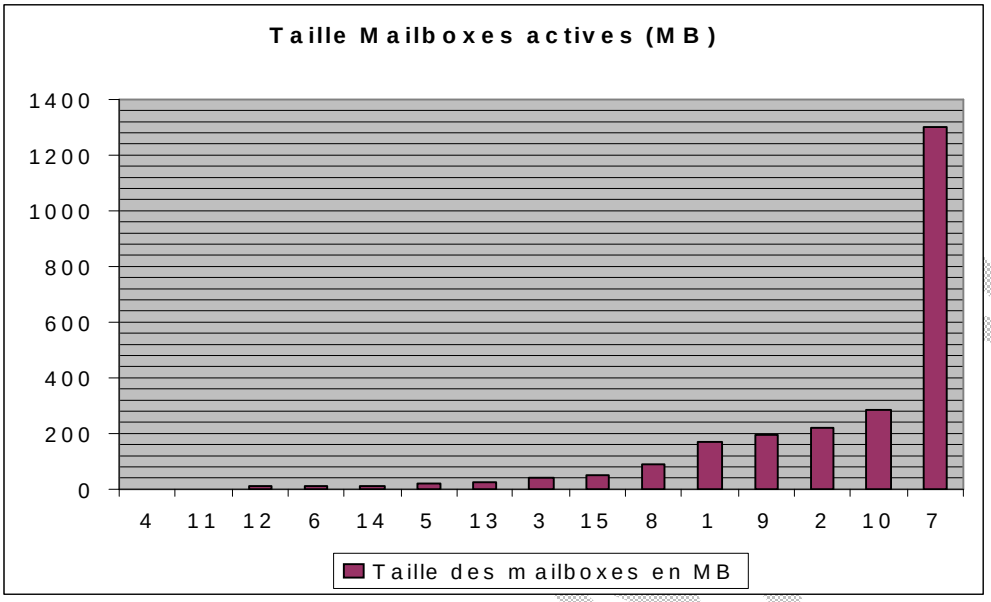
Il conviendra dès lors de reconfigurer le système de mails ainsi que les postes de travail afin de centraliser les mailboxes (et les archives).

De plus, certaines plaintes ont été émises par des utilisateurs concernant la vitesse de réaction de système de mails.

Dans ce cadre, l'utilisation d'un serveur de mails interne et externe (pas en POP3, mais en SMTP pur) pourrait s'avérer intéressant.

SPECIMEN

Tableau des tailles des mailboxes (hors archives).



5.2.6.3 L'agenda

L'utilisation de l'agenda est une pratique bien établie chez *SPECIMEN SA*. Tous les utilisateurs utilisent l'utilitaire LINK pour la gestion des calendriers. Chaque utilisateur a le droit de créer des tâches pour un autre, de consulter les agendas de chacun, et ce système est bien mis en place.

Un bémol cependant concernant les agendas : la réplication avec les Palm Pilots ne se fait pas correctement. Le problème est apparemment en cours d'être solutionné.

Quelques soucis ont été remarqués également au niveau de la praticité de l'agenda (il faut le remplir correctement), et de la réservation des salles et des ressources.

SPECIMEN

5.3 Recommandations

Les recommandations sont les suivantes :

- **R.INF.1 : Centraliser les mailboxes**
- **R.INF.2 : Centraliser les fichiers**
- **R.INF.3 : Centraliser la gestion au niveau du serveur et des PCs**
- **R.INF.4 : Centraliser les impressions**
- **R.INF.5 : Revoir du système d'adressage IP des stations**
- **R.INF.6 : Modifier le local technique**

R.INF.1 **Centraliser les mailboxes**	Comme détaillé dans l'analyse, le serveur de mail dans la société n'est utilisé qu'en tant que relais. La configuration du mail est donc à revoir. La recommandation peut s'articuler sur 2 aspects : Le premier vise dans un premier temps à reconfigurer les postes de travail de façon à stocker les mails sur le serveur (déplacement de la mailbox pst vers le réseau), ce qui a pour but de l'intégrer dans les backups. Le second vise à centraliser la réception et l'envoi des mails qui, pour l'instant, sont des fonctions réalisées par les postes et plus particulièrement par Outlook. Le but ici serait de reconfigurer le serveur mail afin qu'il effectue ce travail. La solution optimale serait de combiner les deux aspects (pour autant que cela soit possible).
R.INF.2 **Centraliser les fichiers**	Le stockage local est un élément à prendre en compte lorsqu'on aborde le problème de la sécurité des données de travail. En effet, des données locales sont : • Indisponibles pour d'autres utilisateurs, • Non backupées avec les autres fichiers stockés, eux, sur le serveur, • Plus susceptibles d'être perdues, à cause de la qualité moindre des éléments hardware des PCs par rapport à ceux du serveur • Plus facilement effaçables : o moins de protection au niveau des droits, o dans le cadre d'une réinstallation de poste. Pour toutes ces raisons, le stockage local des données n'est pas recommandé, que la société soit petite ou grande. La perte de données est un facteur de perte de profit pour les entreprises, et le risque est encore plus grand dans le cas de données locales. Il serait également opportun de forcer les fichiers My Documents sur les zones privées et de sécuriser correctement celles-ci.

R.INF.3 **Centraliser la gestion au niveau du serveur et des PCs**	**La société travaille sur un mode de partage de l'information « à l'ancienne mode ». Les postes sont liés au serveur de manière physique, mais pas de manière software. Ils travaillent tous de façon indépendante. Ce mode de travail implique plusieurs contraintes :** • **Gestion non centralisée des utilisateurs et/ou des mots de passe,** • **Gestion non centralisée des accès au réseau par les machines,** • **Complexité de la mise en place de droits d'accès sur le serveur (ce qui implique généralement un accès total pour tous afin de limiter la gestion),** • **Nécessité de création de tous les utilisateurs partout,** • **Impossibilité de changer son mot de passe sans devoir le changer à plusieurs places (complexité de gestion).** ***SPECIMEN SA* gagnerait en simplicité si les différents accès, passwords, et gestion de PC et de noms étaient centralisés. Les droits d'accès pourraient être plus sécurisés.**
R.INF.4 **Centraliser les impressions**	**La mise en place d'une imprimante réseau a été faite de la même manière que pour les postes : elle a été créée sur tous les PCs comme une imprimante locale.** **Une configuration optimale vise à définir les imprimantes au niveau du serveur et de partager celles-ci. De cette façon, seul le serveur travaille pour préparer l'impression, et de plus, il est toujours allumé.** **La mise en place d'une telle solution implique l'achat de boîtiers print servers pour les 8 imprimantes locales.**
R.INF.5 **Revoir du système d'adressage IP des stations**	**Actuellement, le système d'adressage des stations de travail est réalisé à la main, ce qui implique des difficultés de gestion.** **L'utilisation d'un serveur DHCP permet d'allouer automatiquement une adresse IP à une station se connectant sur le réseau.** **Cette bonne solution peut être mise en place de façon simple et sécurisée.**
R.INF.6 **Modifier le local technique**	**Le local technique actuel manque un peu de sécurité. En effet, le local ne ferme pas à clé, les serveurs se trouvent à proximité de produits d'entretien et d'arrivées d'eau, le local n'est pas climatisé et n'est pas dédié aux serveurs.** **Une amélioration viserait à dédier un local ou à cloisonner celui existant.**

6. Evaluation des pratiques en matière de sécurité

La sécurité des données repose sur trois grands points :

- **Confidentialité**
- **Intégrité**
- **Disponibilité**

(CIA en anglais : Confidentiality, Integrity and Availability)
Ces trois points ainsi que les aspects périphériques ont été évalués lors de l'évaluation.

6.1 Synthèse

Ce chapitre s'intéresse aux composants de l'infrastructure informatique suivants :

- **le local technique ;**
- **la sécurité du serveur et sa résilience ;**
- **l'alimentation secourue ;**
- **le back up ;**
- **la protection virale;**
- **l'utilisation du mot de passe et la protection des stations ;**
- **la sécurité des données au niveau des serveurs.**

Sans se vouloir exhaustive, cette liste tente de recenser les éléments de sécurisation les plus nécessaires.

<u>En résumé :</u>

Les principales forces sont :

- **La présence d'un système de backup de qualité et fonctionnel**
- **Le double backup par réplication**
- **La présence d'un antivirus sur quasi tous les PCs**

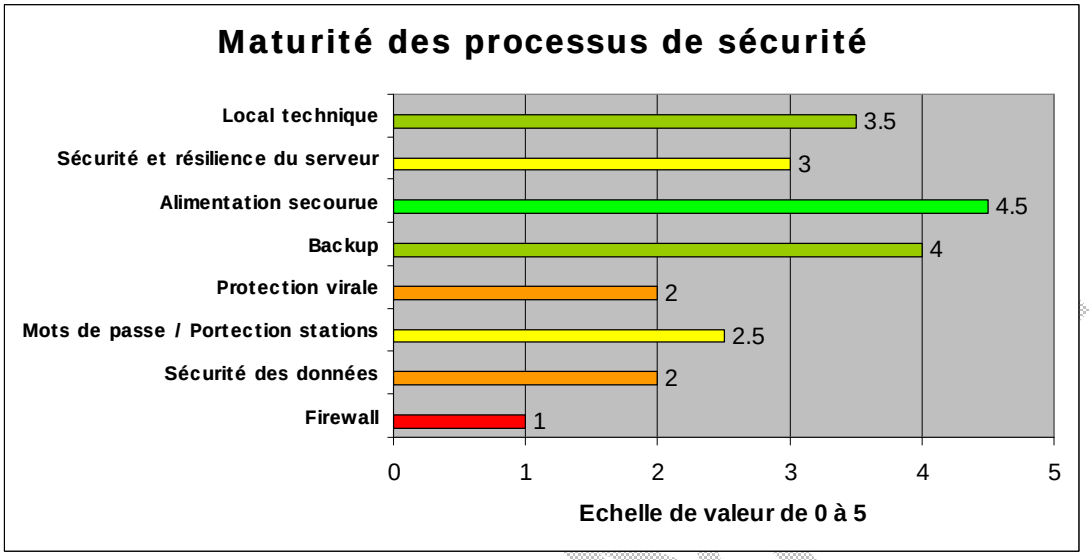
Les faiblesses identifiées sont:

- **La simplicité des mots de passe**
- **La présence de données locales et donc non backupées**
- **Le non suivi des antivirus**
- **L'absence d'un antivirus au niveau de 3 des 4 serveurs**
- **Les versions différentes d'antivirus (4 éditeurs différents pour 15 postes)**
- **La non-externalisation de certaines bandes de backup**
- **Le clavier non adapté à une console serveur**

Des recommandations pragmatiques sont données en fin de chapitre.

Le graphique suivant illustre les niveaux de maturité des différents processus de sécurisation du système d'information analysé lors de l'évaluation.

SPECIMEN



Echelle : 0 mauvais et 5 excellent

SPECIMEN

6.2 Rapport Détaillé

6.2.1 Le local technique

Les serveurs utilisés par *SPECIMEN SA* se trouvent installés dans un rack 42 U, situé dans une des pièces du bâtiment principal de l'entreprise.

Cette pièce est dédiée aux serveurs, à l'ups, à l'alarme du bâtiment, aux connectiques vers l'extérieur (lignes SDSL, router, modem, etc…), mais renferme également quelques fournitures et archives, une arrivée d'eau et des produits chimiques d'entretien de piscine et de bassin.

La ventilation des serveurs ne pose pas de problèmes, mais la climatisation de la salle devrait être mise en place. C'est d'ailleurs une demande de la part des personnes en charge de l'informatique ou d'une partie de celle-ci.

La salle est ouverte en permanence et tout le monde peut y avoir accès.

Il convient donc de remédier à 3 soucis « potentiels » :

L'absence de climatisation dans la salle
La sécurité de l'accès au local et au rack
La présence d'éléments dangereux à proximité (produits chimiques, conduites d'eau).

6.2.2 La sécurité du serveur et sa résilience

Les serveurs utilisés chez *SPECIMEN SA* sont tous des « produits blancs ».

Seul le serveur utilisé comme serveur de fichier et serveur de backup dispose d'une carte RAID de type Adaptec SCSI RAID 2200S. Les disques contrôlés par cette carte sont des disques externes, hot-swap.

L'utilisation de cette carte apporte un élément de résilience au niveau du disque dur du server. En effet, si un des 2 disques vient à être défectueux, les données sont disponibles sur un disque miroir de celui-ci. Encore faut-il être au courant de la défaillance d'un des disques. C'est pour cette raison que des outils d'avertissement peuvent être mis en place (avec notification à l'extérieur : SMS, par exemple).
Les disques utilisés sont hotplug, ce qui évite l'arrêt du serveur en cas de remplacement.

En ce qui concerne l'alimentation, deux arrivées de courant sont disponibles sur le serveur de fichiers, une seule sur les 3 autres. Par contre, si l'alimentation est fournie à la seule alimentation des 3 serveurs, le serveur de fichiers n'est alimenté que par 1 seul câble, ce qui signifie que, si l'alimentation est défectueuse, le serveur est indisponible le temps du remplacement de cette alimentation ou le temps de rebranchement du câble sur la second alimentation.

SPECIMEN

Deux cartes réseaux sont disponibles sur chaque serveur, mais la configuration qui en est faite est à optimiser (mise des cartes en teaming pour de la redondance, installation de cartes de drivers identiques).

Aucun contrat de maintenance ou d'intervention ou de garantie n'est relatif à ces serveurs, ce qui signifie qu'aucune intervention d'urgence ni aucune disponibilité de pièces n'est envisagée. Certaines données sont néanmoins répliquées sur un portable tous les soirs, en complément du backup, ce qui rendrait celles-ci disponibles en cas de désastre. Par contre, le mail serait indisponible.

La vitesse des attaques depuis l'Internet, même dans les petites sociétés, n'est pas à négliger. Les attaques peuvent être de nature virale ou encore être dues à des hackers.
Aucun Firewall n'est installé que ce soit au niveau du serveur ou au niveau des stations de travail. Il faut savoir que les phénomènes d'intrusion les plus fréquents se passent au niveau accès vers l'extérieur, et donc au niveau de l'Internet. Le serveur lui-même étant connecté directement sur l'Internet, il est indispensable de prévoir une protection à ce niveau.
La société qui gère les connexions vers l'extérieur (WIN) dispose d'un firewall. Cette protection est-elle dédiée à *SPECIMEN SA* ou est-ce un firewall général qui est utilisé pour plusieurs société, auquel cas les règles de passages ne sont peut-être pas adaptées à l'activité de *SPECIMEN SA*.
Les règles de sécurité du Firewall n'ont pas pu être étudiées.

6.2.3 Alimentation secourue

L'arrivée de puissance électrique dans le rack passe par une UPS de type MGE Pulsar Extreme 3000.

Cet onduleur alimente les 4 serveurs, et sert de relais pour alimenter tous les postes de la société, ainsi que le switch réseau. En cas de coupure de courant, les postes restent allumés et continuent de fonctionner.

Le courant peut, le cas échéant, être fourni par une génératrice (60 KVA) qui peut prendre le relais dans le cas d'une coupure générale du courant de la ville.

La protection de l'alimentation est bien réalisée, et la durée approximative de l'alimentation secourue est de 30 à 40 minutes.

Cependant, si le courant venait à tomber aussi bien à l'UPS qu'à la génératrice, les serveurs s'éteindraient violemment, car ils ne sont pas gérés par l'UPS.

Il faut également vérifier la bonne calibration de l'UPS, bien que, dans le cas de *SPECIMEN SA*, la génératrice soit là en secours deuxième niveau.

SPECIMEN

6.2.4 Back up

Le système de backup utilisé est Veritas Backup Exec version 9.1, avec un lecteur de bandes BENCHMARK DLT1 (DLT 40/80 GB).

Les backups sont réalisés chaque soir à 23h00, et la quantité de données est d'environ 52 GB.

En parallèle, une synchronisation des données du serveur est effectuée sur un poste de travail (Poste 1).

En plus, une copie de sécurité de la base LINK est réalisée par Xxxxxx Xxxxxx sur son poste.

Au niveau de la stratégie de rotation, 10 cassettes sont utilisées (LU, MA, ME, JE, VE, plus rotation sur 2 semaines) et réutilisées la semaine d'après. Les cassettes sont stockées dans un coffre ignifugé et fermé à clé, dans les bureaux. Il n'y a pas de système d'externalisation des cassettes. Les cassettes ont été toutes remplacées il y a 2 ans environ.

Les backups se passent correctement presque tous les soirs (9 fois sur 10). Le problème des plantages de backup a été énoncé lors des interviews. Une politique de gestion des incidents de backup n'est pas mise en place autrement que par le fichier des interventions de EXEMPLE SA.

Les soucis de backup sont généralement dus au non chargement des cassettes (absence du responsable) ou à des fichiers ouverts (et donc non accessibles par le backup).

La notification du job de backup est réalisée soit par mail, soit par impression, mais est réalisée. Les messages sortent si le backup est OK ou NOK, ce qui est une source pratique de diagnostic.

4 remarques cependant :

- **Aucune procédure de backup n'est présente, ce qui signifie que si la personne gérant les backups n'est pas présente, la cassette n'est pas forcément changée.**
- **Si l'on veut retrouver un fichier dans une version antérieure à 10 jours, cela n'est pas possible (rotation sur 10 jours et pas par semaine).**
- **Un souci de configuration oblige la personne qui change de cassette à réponde à 4 questions tous les matins. Point à régler.**
- **La personne responsable des backups n'a pas de procédure de restauration de fichiers et n'a jamais eu à en faire un. En cas de gros pépin, il faut faire appel à EXEMPLE SA.**

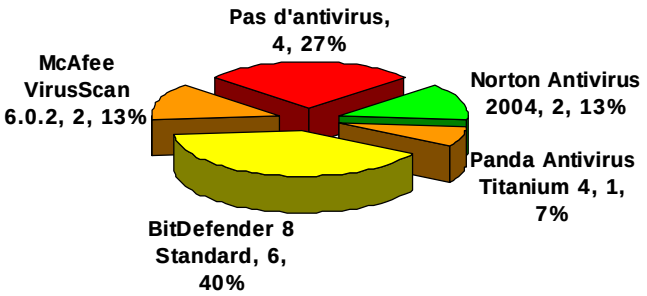
SPECIMEN

6.2.5 Protection virale

Les stations de travail sont quasi toutes équipées d'un antivirus. Malheureusement, ces antivirus ne sont pas tous identiques (4 éditeurs pour 15 postes de travail). On y retrouve :

- **Norton Antivirus 2004**
- **McAfee VirusScan 6.0.2**
- **Panda Antivirus Titanium 4**
- **Bit Defender 8 Standard**

Répartition des types d'antivirus



Les signatures sont en théorie mises à jour via la connexion Internet, et ce régulièrement. Certaines signatures datent de 2003 et de 2004, ce qui revient à remettre en cause la politique de gestion des mises à jour.

Le serveur de fichiers, lui, dispose d'une protection antivirus grâce à Norton Antivirus. Par contre, les signatures de celui-ci datent de Janvier 2004, ce qui est un point critique. En effet, la connexion vers Internet est aussi disponible sur les serveurs, et cette non protection laisse la porte grande ouverte pour les éléments viraux. Les 3 autres serveurs ne disposent pas de protection Antivirus du tout. Ici encore, nous identifions une faille potentielle de sécurité.

De par la constatation précédente, les signatures d'antivirus ne sont pas récoltées via un point central, mais chaque station effectue ses mises à jour régulièrement (les versions des AV des stations sont d'ailleurs des versions standalone).

En ce qui concerne les intrusions virales éventuelles, aucun virus n'a jamais été remarqué chez *SPECIMEN SA*. Certains mails arrivent vides dans les mailboxes de certains utilisateurs, mais on n'en connaît pas la cause. Une bonne pratique déjà mise en place : si on ne connaît pas l'expéditeur, on n'ouvre pas.

L'utilisation d'un système centralisé est néanmoins à recommander :

- **Gain de disponibilité de la ligne SDSL**
- **Synchronisation**
- **Rapidité de mise à jour**
- **Suivi dans un endroit unique de toutes les versions de signatures.**

6.2.6 Utilisation des mots de passe

La politique de *SPECIMEN SA* n'est pas très complexe, et les mots de passe sont aisément identifiables grâce aux informations de l'utilisateur. Cette configuration pourrait s'expliquer par :

- **Le nombre limité d'utilisateurs**
- **La confiance entre les utilisateurs**
- **Le partage des informations géré localement et pas de manière centralisée**

Cette configuration peut être très pratique (pas besoin de se souvenir), mais est également dangereuse dans le cas où une personne extérieure entre dans les bureaux. Cette dernière a TOUS les accès PARTOUT. Ceci est manifestement une lacune au niveau de la sécurité.
Cette situation est également dangereuse en cas de départ d'un collègue (qui ne se passe pas toujours bien) et qui voudrait, sous forme de représailles, mettre son grain de sable dans l'engrenage.
A noter que les mots de passe locaux sont parfois changés, mais pas sur toutes les stations. Ils sont communiqués par EXEMPLE SA, mais il n'y a pas de logique.

6.2.7 La sécurité des données au niveau des serveurs

L'accès aux données du serveur n'est pas réellement sécurisé, en ce sens que les mots de passe sont relativement simples, et que tous les utilisateurs ont accès à tout.
Il n'y a des zones d'utilisation privée pour chaque utilisateur et ses données personnelles, mais ces espaces ne sont pas sécurisés spécifiquement (ce que pensent croire certains utilisateurs). Cet espace n'est pas forcément nécessaire d'après les utilisateurs.
Aucun groupe d'utilisateurs n'a été créé non plus. Les droits d'accès sur les répertoires et fichiers ne sont donc pas « gérés » par groupe.
Il serait bon de créer plusieurs groupes d'utilisateurs, correspondant au département par exemple, afin de simplifier la gestion des droits sur les serveurs. En effet, l'utilisation de groupes :

- **Diminue la liste des comptes auxquels on attribue les droits,**
- **Facilite le changement de département d'un utilisateur (il change de groupe, on ne doit pas l'ajouter au niveau des droits car il récupère les droits du groupe),**
- **Simplifie la mise à disposition des données pour un nouvel utilisateur,**
- **Simplifie la restriction pour un utilisateur sortant,**
- **Permet de hiérarchiser plus simplement.**

Certains programmes enregistrent en dur les identifiants utilisés pour leurs services et stockent également la correspondance avec le mot de passe. Si le mot de passe de l'administrateur est modifié, il se peut que ces services ne puissent plus démarrer. Il est donc recommandé de créer un utilisateur spécifique pour les services critiques, et de lui confier un mot de passe que l'on ne changera qu'avec un maximum de précautions.
En ce qui concerne les utilisateurs spéciaux, un seul compte spécial est défini : Service LINKERVEUR. Aucun utilisateur spécifique pour les services backup et mail n'a été défini.

SPECIMEN

6.2.8 La sécurisation des stations

La sécurité au niveau des stations de travail est très limitée de par l'utilisation des comptes locaux (équivalents administrateurs) avec des mots de passe simplistes. Il va de soi qu'une personne extérieure à la société a par le fait tous les accès au niveau des postes locaux, s'il essaie un minimum de mots de passe.

En regardant ces résultats, et cela a été confirmé par l'analyse, certains postes travaillent avec des données locales (Poste 15 : 12 GB utilisés, poste 7 : 10 GB utilisés). L'utilisation de données locales est un paramètre à prendre en compte lorsqu'on parle de sécurité des données. En effet, le plantage du disque dur pourrait impliquer de recommencer les différents projets en cours, les courriers, les tableaux et les différents documents stockés localement, c'est-à-dire des pertes de productivité non négligeables

6.2.9 Les logonscripts

Les connections des disques au niveau des accès serveurs sont réalisées à la main et pas par un login script.
Les lettres attribuées sont différentes en fonction des postes de travail. Un utilisateur changeant de poste doit donc recréer ses lettres de connexion, reconnecter son imprimante réseau.

Grâce à l'utilisation de login scripts, et moyennant une reconfiguration de la structure des fichiers et de l'architecture globale du réseau, l'anonymisation des postes peut être réalisée de manière simple.
Ceci est une opération très simple, donnant des résultats rapides, mais implique une documentation écrite et quelques explications afin que l'utilisateur ne se sente pas perdu

SPECIMEN

6.3 Recommandations

Les recommandations sont les suivantes :

- **R.SEC.1 : Sécuriser/Modifier le local technique**
- **R.SEC.2 : Augmenter la résilience des serveurs**
- **R.SEC.3 : Gérer l'alimentation secourue**
- **R.SEC.4 : Modifier la politique de backup**
- **R.SEC.5 : Simplifier la protection virale**
- **R.SEC.6 : Protéger les données et les stations. Avoir une politique de mots de passe**
- **R.SEC.7 : Sécuriser les données au niveau des serveurs**
- **R.SEC.8 : Mettre en place un Firewall**

R.SEC.1 **Sécuriser/Modifier le local technique**	**Le local technique est moyennement approprié. Le fait d'avoir des serveurs se trouvant dans un rack est déjà une bonne solution. Par contre, il conviendra d'isoler ce rack aussi bien au niveau de l'accessibilité que par rapport aux arrivées d'eau et des produits d'entretien.** • **La mise en place d'une climatisation est également vivement recommandée.** • **Il est fortement recommandé de changer le clavier (Touches Power, Standby et Resume sur le clavier è attention aux mauvaises manipulations)**
R.SEC.2 **Augmenter la résilience des serveurs**	**Un seul des serveurs actuels dispose d'une carte RAID, ce qui le protège contre une défaillance d'un des disques durs.** **Les 3 autres serveurs n'ont pas d'un tel dispositif. En fonction de la criticité de ceux-ci, la résilience pourrait être améliorée** **Cette protection peut néanmoins être mise en place/renforcée par :** • **L'utilisation de cartes réseau couplées (teaming)** • **L'utilisation de la double alimentation sur le serveur.** • **L'utilisation de cartes RAID et de disques Hotplug**
R.SEC.3 **Gérer l'alimentation secourue.**	**Il suffirait de reconfigurer la connectique série sur le serveur principal afin de communiquer avec l'UPS, et ainsi permettre d'éteindre proprement le serveur lorsque les batteries de l'onduleur et de la génératrice arrivent à bout de souffle (en cas de panne électrique).**
R.SEC.4 **Modifier la politique de backup**	**Le système de backup en place actuellement fonctionne correctement et apparemment sans trop de problèmes.** **Néanmoins, aucune procédure n'est définie, aucun test de restauration n'est réalisé, les cassettes demeurent à l'intérieur du bâtiment, et les cassettes tournent de 2 semaines en 2 semaines.**

	Des recommandations sont : • Ecrire une procédure de backup claire, avec un maximum de détail, pour pallier aux absences des « responsables » du backup. • Faire régulièrement des tests de restauration de fichiers. • Diminuer la fréquence d'utilisation des cassettes en optant pour un roulement plus large (Lu-Ma-Me-Je / Ve1-Ve2-Ve3-Ve4/ Mois , par ex.) • Externaliser de temps en temps une cassette (autre part que dans les bureaux).
R.SEC.5 Simplifier la protection virale	Installer un système d'antivirus centralisé simplifierait la gestion des postes de travail. Installer un antivirus sur les serveurs est fortement recommandé, car eux aussi ont accès à Internet. • Protéger les serveurs avec un antivirus • Centraliser les mises à jour antivirus • Uniformiser les versions d'antivirus
R.SEC.6 Protéger les données et les stations. Avoir une politique de mots de passe	Les mots de passe sont simples au niveau des accès aux stations de travail. Afin de protéger les données et les postes, une politique de mots de passe un peu plus compliquée est vivement recommandée. • Mettre les PCs en mode Domaine • Centraliser les utilisateurs • Créer une politique de mots de passe
R.SEC.7 Sécurisation des données au niveau des serveurs	Le fait d'avoir la configuration de la société en mode Workgroup « oblige » presque à donner tous les droits à tout le monde au niveau des accès aux données. Le passage en mode Domaine aura pour effet de pouvoir mettre en place une politique simple d'accès aux données, grâce à la création de comptes utilisateurs centralisés, à qui on donnera des droits d'accès. Il convient alors de revoir la politique d'accès aux données du serveur.
R.SEC.8 Mettre en place un Firewall interne.	Le fait d'empêcher certains accès depuis l'extérieur de la société devient obligatoire. Cette protection peut se mettre en place avec un Firewall, un filtre entre les entrées-sorties des lignes de connexion de la société. Installation d'un Firewall interne

7. Evaluation en matière de gestion documentaire

7.1 Synthèse

Les principales forces sont :

- **Un minimum de suivi des interventions grâce au fichier de Mr Xxxxx,**
- **Le classement automatique et la facilité de gestion des documents via LINK,**
- **La présence d'un système de codification de fichiers.**

Les faiblesses identifiées sont:

- **Le peu ou l'absence de documentation technique,**
- **Le peu ou l'absence de procédures (bakup, installation, redémarrage serveur, …).**

Des recommandations pragmatiques sont données en fin de chapitre.

7.2 Rapport détaillé

7.2.1 Ce qu'un document devrait contenir : généralités

La procédure d'inspection de document est basée sur la lecture et un examen approfondi effectué sur base des critères liés au contenu du document, tels que la structure, la complétude, la cohérence et la clarté.

L'inspection vérifie la conformité du document par rapport aux standards de documents à utiliser pour la mise en place, la gestion et le suivi de projet. Cette inspection analyse les aspects suivants des documents :

- **Identification**
- **Stockage**
- **Utilité, complétude et exactitude.**

Pour chaque document analysé, les informations suivantes devraient être reprises:

- **Identification**
- **Nom du document**
- **Auteur**
- **Statut (draft/définitif)**
- **Date d'émission**
- **Version**
- **Nombre de pages**
- **Identification de chaque page (en-tête ou pied de page)**
- **Nombre de copies/liste de diffusion**
- **Stockage**
- **Détenteur du document**
- **Format du document (papier ou électronique)**
- **Utilité du document**
- **Utilité pour l'entreprise**

SPECIMEN

Des instructions de travail relatives à l'utilisation des ressources partagées, la mise en jour des anti-virus, etc… devraient être disponibles.

Idéalement, toutes ces documentations devraient comporter un nombre important de copies d'écran de façon à guider l'utilisateur le plus doucement possible.

Une procédure sur la nomenclature des noms de fichiers est très demandée par les collaborateurs afin d'être plus efficace dans leur travail sur des documents créés par d'autres.

Enfin, si une procédure existe, elle doit aussi être suivie. Pour ce faire, il est nécessaire de vérifier l'adhésion des personnes à la dite procédure et de prendre les mesures adéquates en cas de non respect.

Sans se vouloir exhaustive, cette liste tente de recenser les éléments de sécurisation les plus nécessaires.

En résumé :

7.2.2 Documentation à disposition des utilisateurs

Très peu de documentation est disponible chez *SPECIMEN SA*, les utilisateurs se référant beaucoup à leurs collègues lors de problèmes techniques ou de questions.

Au niveau des documentations disponibles, certains guides d'utilisation (Office) sont disponibles, mais cela se limite à la documentation fournie par les éditeurs de programmes.

Il n'y a pas non plus de procédure d'encodage, de procédure d'exécution aussi bien au niveau du travail journalier que des tâches informatiques.

Un manuel utilisateur reprenant toutes les informations fournies gagnerait à être produit et diffusé.

Ceci permettrait aussi d'améliorer les connaissances de chacun.
Une évaluation régulière de la réalité par rapport aux bonnes pratiques pourrait être menée afin de repérer les récalcitrants et les former plus en détails.

Exemple de procédures (générales) à mettre en place :

- **Procédure liée à la gestion documentaire, documents informatiques et non informatiques,**
- **Procédure à suivre en matière de sécurité des données,**
- **Procédure à suivre concernant le stockage de données et les sauvegardes,**
- **Procédure concernant l'utilisation des imprimantes.**

SPECIMEN

7.3 Recommandations

Les recommandations sont les suivantes :

- **R.DOC.1 : Améliorer la gestion documentaire**

R.DOC.1 **Améliorer la gestion documentaire**	**Des politiques de documentation et de création de procédure technique et autre devraient être mises en place, notamment pour pallier aux absences de certaines personnes ou pour éviter les pertes de connaissances.** **Une procédure de nommage des fichiers du réseau, aussi bien dans LINK que dans Windows gagnerait à être mise en place.**

7.3.1 Recommandation relative au stockage des documents

Tout document devrait être stocké sous forme électronique, dans une structure d'accueil propre à tout ce qui concerne l'informatique. Une arborescence de répertoires avec autorisations d'accès pour les personnes concernées doit exister. La structure suivante est proposée :

- **Administration** — **Tout document administratif et contractuel (contrats, offres, budgets).**
- **Bibliothèque** — **Tout document bibliographique pouvant contribuer d'une manière ou d'une autre à toute activité informatique.**
- **Courrier** — **Tout envoi de lettre, fax, mémo concernant l'informatique.**
- **Gestion de projet** — **Tout ce qui concerne la gestion et le suivi de projet ou des activités régulières relatives à la fonction informatique dans l'entreprise (planning, suivi des modifications, état d'avancement, contrôle qualité).**
- **Besoins** — **Tout ce qui concerne l'expression des besoins des utilisateurs (cela peut se décliner dans un document dénommé « cahier des charges »).**
- **Analyse fonctionnelle** — **Tout document de description fonctionnelle du point de vue de l'informaticien.**
- **Analyse technique** — **Tout document préparant la programmation.**
- **Programmation** — **Tout document décrivant le code (cela peut se trouver à l'intérieur des programmes sources).**
- **Support** — **Tout document relatif à l'utilisation du logiciel, à des formations.**

SPECIMEN

Tout dossier papier doit également être ordonné et peut suivre la même organisation que la structure électronique des répertoires.

La classification actuelle des documents (électroniques et papier) peut s'inspirer de la structure proposée ci-dessus de manière à la compléter, l'améliorer.

7.3.2 Recommandation relative à la gestion des versions

La gestion des documents et de leurs versions est une pratique très peu utilisée chez *SPECIMEN SA*, ce qui résulte en un file system relativement anarchique. LINK a son propre système de gestion (base de donnée) qui est largement utilisé par tout le monde, préférentielle à Windows. Un système de codification des documents est à mettre en place, celui-ci en fonction de la date de création ou/et d'édition du document.
Une technique de codification possible est donnée ci-dessous :

- **La version d'un document peut être codifiée : *Vxx_yy***
  - **Où xx constitue la version majeure,**
  - **Et yy constitue la version mineure.**

Les versions mineures représentent des documents ayant évolué en interne sur le projet, ou de toute manière à l'intérieur de l'entreprise (pas de diffusion externe). Dès qu'un document est stabilisé et est prêt à être diffusé pour approbation de façon externe, le document est figé avec une nouvelle version majeure. Par exemple, si un document a pour dernière version mineure V01_07, la nouvelle version majeure devient V02_00

Tout changement de version correspond à des évolutions par rapport à une version antérieure et doit être documenté dans un historique des modifications.

7.3.3 Recommandations relatives aux documents contractuels

Un ensemble d'éléments doivent figurer sur les documents contractuels : les limites et responsabilités du fournisseur, les limites et responsabilités de l'entreprise, les clauses de garantie, la partie couverte par la maintenance, les délais d'intervention en cas de maintenance, les signatures des parties, les versions…

7.3.4 Recommandations relatives aux documents d'expression des besoins

Ce type de document pourrait correspondre à un « cahier de doléances » ou une « boîte à suggestions » qui serait disponible pour les utilisateurs.

SPECIMEN

7.3.5 Recommandations relatives aux documents d'analyse fonctionnelle

Ce type de document doit être rédigé par un informaticien et validé par un ou des utilisateur(s). On doit y trouver : les fonctions du logiciel, un schéma conceptuel des données, une description des postes de travail, des règles de gestion et d'organisation, des schémas d'écrans et d'éditions, etc.

7.3.6 Recommandations relatives aux documents d'analyse technique

Ces documents préparent la phase de programmation.

Ils doivent inclure une architecture des programmes, le schéma physique de la base de données, des descriptifs relatifs à l'environnement technique (dénomination des fichiers, modules non propriétaires utilisés), l'enchaînement des écrans.

7.3.7 Recommandations relatives aux documents de support et d'exploitation

Plusieurs types de documents sont à considérer :

- **Les guides d'utilisation pour les progiciels**
- **Les documents techniques tels que les documents techniques des serveurs, les documents relatifs aux applications**
- **Les procédures relatives aux activités liées à la fonction informatique dans l'entreprise**

Les deux premiers types de documents sont fournis par les éditeurs de matériel informatique et de logiciels. Concernant les procédures relatives aux activités liées à la fonction informatique dans l'entreprise, il serait souhaitable d'éditer des documents techniques de configuration, d'éditer des procédures de réalisation d'opérations (backup, scan antivirus, redémarrage de serveur), et ceci pour pallier à l'absence des personnes responsables (congés, maladie).

Un point positif ici est la bonne pratique de conservation des fiches techniques et d'un peu de suivi de documents de support par le responsable informatique en interne, documents stockés dans un classeur dans une armoire (factures d'achat, licences, …)

La diffusion auprès des utilisateurs sera à prévoir

7.3.8 Recommandations relatives aux documents de gestion de projet informatique

Aucun document de gestion de projet informatique proprement dit n'existe (par exemple : plan de travail, planning, rapport d'activités, suivi de l'avancement,…).

SPECIMEN

8. Synthèse finale

8.1 Forces et faiblesses

Le rapport ci-dessous reprend les forces et faiblesses des 5 domaines de l'évaluation telles qu'elles ont été mises en évidence dans les différents chapitres du présent rapport.

Domaine évalué	Principales forces	Principales faiblesses
Management	• L'évaluation des besoins (demandes au personnel ou suggestions) et l'écoute • La fidélité vis-à-vis des fournisseurs	• L'absence d'élaboration d'un budget informatique o Le manque de visibilité à long terme o La gestion des besoins au coup par coup • L'absence de contrats de maintenance sur certains éléments vitaux • L'absence de techniques de gestion de projet
Service Support	• Les connaissances informatiques internes pour le helpdesk direct, • Les versions récentes des systèmes d'exploitation et des versions Office, • La disponibilité des personnes de contact de la société de service actuelle.	• Les soucis quant à la compétence technique, et donc un impact sur la qualité de travail, • Le manque de suivi dans les incidents et/ou les problèmes.
Infrastructure	• Des postes de travail récents et performants, • Des systèmes d'exploitation « de réseau » (Pas de Win95/98/Me, sauf exceptions), • L'utilisation fréquente de l'agenda partagé, • L'utilisation de Link pour la communication interne et le stockage de documents, • Des serveurs dans un rack qu'il est possible de fermer à clé.	• Local technique non sécurisé – climatisé – dédié, • L'utilisation d'un système d'adressage fixe, • Une politique de nommage PC non établie, • Une architecture « Workgroup » alors que tout est prêt pour travailler en « Domaine », • La présence de données locales sur les PCs (mail et fichiers), • L'absence de centralisation des : o Fichiers o Mails o Impressions o Gestion users et mots de passe o Gestion droits d'accès.

SPECIMEN

Sécurité	• La présence d'un système de backup de qualité et fonctionnel • Le double backup par réplication • La présence d'un antivirus sur quasi tous les PCs	• La simplicité des mots de passe • La présence de données locales et donc non backupées • Le non suivi des antivirus • L'absence d'un antivirus au niveau de 3 des 4 serveurs • Les versions différentes d'antivirus (4 éditeurs différents pour 15 postes) • La non-externalisation de certaines bandes de backup • Le clavier non adapté à une console serveur
Documentation	• Un minimum de suivi des interventions grâce au fichier d'Olivier Senger • Le classement automatique et la facilité de gestion des documents via LINK. • La présence d'un système de codification de fichiers	• Le peu ou l'absence de documentation technique • Le peu ou l'absence de procédures (bakup, installation, redémarrage serveur, …)

SPECIMEN

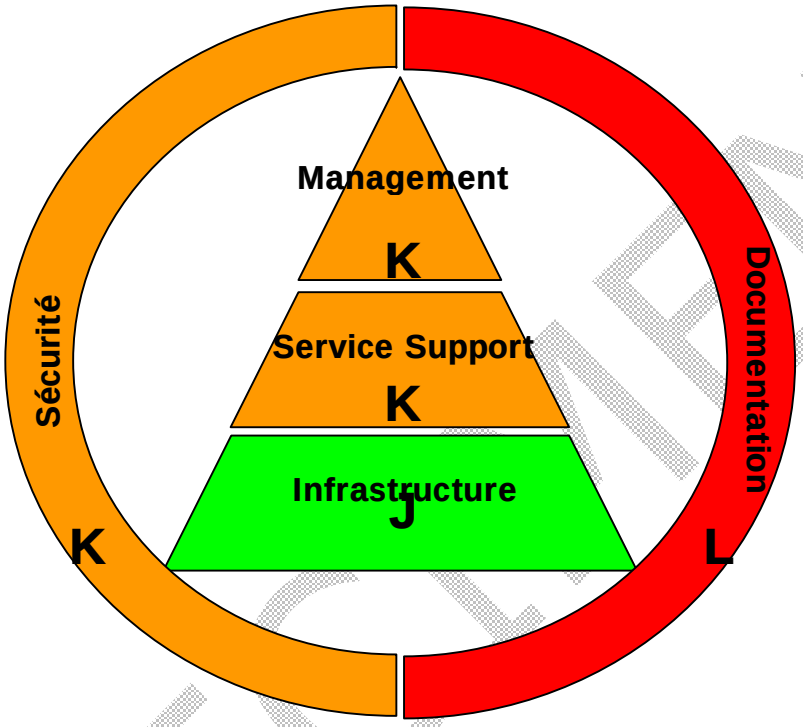
8.2 Niveaux de maturité

Afin d'évaluer la maturité de chacun des processus, il est possible de définir les références suivantes :

Maturité	Description	Code couleur	Code symbole
Stratégique	Les activités d'un domaine de maturité stratégique sont développées, mise en oeuvre et gérées d'une manière satisfaisante dans sa globalité. Les notions de proactivité et de moyen terme y sont généralement présentes. En terme de valeur ajoutée, un domaine de maturité stratégique offre à l'entreprise un avantage compétitif.	Vert	J
Tactique	L'entreprise réalise des efforts importants pour développer et établir les activités d'un domaine de maturité tactique. Les notions de réactivité et de court terme y sont généralement présentes. Toutefois, un domaine de maturité tactique n'est pas à même d'offrir à l'entreprise tous les bénéfices qu'elle pourrait en attendre.	Orange	K
Critique	Les activités d'un domaine de maturité critique ne sont que très partiellement mises en oeuvre, suivent suite à des besoins ponctuels. De nombreux pré-requis manquent. Les apports positifs d'un domaine de maturité critique sont globalement contre-balancés par des manques d'efficacité, de productivité au sein de l'entreprise. En outre, le domaine peut présenter un risque potentiel pour l'entreprise.	Rouge	L

SPECIMEN

Sur base de l'analyse des forces et faiblesses (page précédente) et des bonnes pratiques relatives à ces domaines, les niveaux de maturité de la société sont présentés dans le graphique ci-dessous. Le tableau ci-dessous liste les actions à prendre qui sont classés selon l'importance et l'urgence de la mise en oeuvre.



SPECIMEN

Les recommandations élaborées ci avant pour les 5 domaines de l'évaluation sont la base du programme d'amélioration. Dans cette optique, le synopsis suivant propose une classification des recommandations en fonction de leur importance et de leur urgence.

Urgence

R.SUP.2 : Adopter une politique de gestion des problèmes

R.INF.4 : Centraliser des impressions

R.MGT.2 : Souscrire à un contrat de maintenance

R.SUP.1 : Adopter une politique de gestion des versions antivirus

R.INF.3 : Centraliser la gestion au niveau du serveur et des PCs

R.SEC.5 : Simplifier la protection virale

R.SEC.6 : Protéger les données et les stations. Avoir une politique de mots de passe
R.SEC.7 : Sécuriser des données au niveau des serveurs
R.SEC.8 : Mettre en place un Firewall interne.

Importance

R.MGT.1 : Améliorer la gestion financière

R.MGT.3 : Mettre en place un suivi de projets

R.INF.6 : Modifier le local technique

R.SEC.1 : Sécuriser/Modifier le local technique
R.SEC.2 : Augmenter la résilience des serveurs

R.SUP.3 : Mettre à niveau des différentes versions

R.INF.1 : Centraliser les mailboxes
R.INF.2 : Centraliser les fichiers
R.INF.5 : Revoir du système d'adressage IP des stations

R.SEC.3 : Gérer l'alimentation secourue
R.SEC.4 : Modifier la politique de backup

R.DOC.1 : Améliorer la gestion documentaire