CESAG **Centre Africain d'Etudes Supérieures en Gestion**

CESAG BF – CCA

BANQUE, FINANCE, COMPTABILITE, CONTROLE & AUDIT

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 2

(2007-2009)

Mémoire de fin d'étude

THEME

Elaboration de la cartographie des risques liés au réseau informatique : Cas du PNUD Sénégal

Présenté par :

Harold MEDESSOUKOU

Dirigé par :

M. Alain SAWADOGO
Auditeur informatique
Enseignant Associé au CESAG

Octobre 2010

Dédicace

Je dédie ce mémoire :

- ✓ mon *Dieu Tout Puissant,*
- ✓ mon Père Désiré Ayihadji MEDESSOUKOU (Que Dieu ait son âme),
- ✓ ma Mère Sophie Jéronime KISSEZOUNON, qui a éclairé mon chemin et qui m'a encouragé et soutenu tout au long de mes études.
- ✓ ma sœur Abègnonhou Joëlle Bérénice Colombe MEDESSOUKOU,
- ✓ mon frère Prudence DOHOU, pour son soutien,
- ✓ ma chérie Nesly LASSISSI, pour son soutien dans les moments difficiles et surtout pour sa patience.

Remerciement

A la fin d'une formation, il est de tradition d'exprimer ses reconnaissances à l'égard de ceux qui, par leurs apports multiformes, ont contribué à l'aboutissement et à la réussite de ce travail.

Je me dois de remercier très sincèrement M. Yérim FALL, mon maître de stage, pour avoir accepté de me suivre avec tant d'attention sur ce sujet.

Je remercie à double titre M. YAZI Moussa, qui a accepté de recevoir ce mémoire, et m'a encouragé dans la rédaction de celui-ci à travers des conseils très utiles et judicieux.

M. SAWADOGO Alain, ses conseils ont toujours été précieux, et ses encouragements ont su me donner l'énergie nécessaire pour l'écriture de ce mémoire.

Je remercie tous les membres du corps professoral du Centre Africain d'Etudes Supérieures en Gestion.

A tous ceux, qui, d'une manière ou d'une autre, m'ont soutenu au cours de mes études et du stage au PNUD Sénégal et dont les noms n'ont pu être cités. Qu'ils trouvent à travers ce mémoire l'expression de ma gratitude.

Sigles et abréviations

ACC	**A**udit **C**onseil **C**omptabilité
ACL	**A**ccess **C**ontrol **L**ist
AD	**A**ctive **D**irectory
AMDEC	**A**nalyse des **M**odes de **D**éfaillances, de leurs **E**ffets et de leur **C**riticité
BFR	**B**esoin en **F**onds de **R**oulement
CCA	**C**ommon **C**ountry **A**ssessment
CEAO	**C**ommunauté **E**conomique de **l'A**frique de **l'O**uest
CESAG	**C**entre **A**fricain **d'E**tudes **S**upérieures **en G**estion
COBIT	**C**ontrol **O**bjectives for **I**nformation and related **T**echnology
CPAP	**C**ountry **P**rogramme **A**ction **P**lan
CPD	**C**ountry **P**rogramme **D**ocument
DESS	**D**iplôme d'**E**tudes **S**upérieures **S**pécialisées
DMZ	**D**e**M**ilitarized **Z**one
DSI	**D**irection des **S**ervices d'**I**nformations
DSRP II	**D**ocument de **S**tratégie pour la **R**éduction de la **P**auvreté II
FTP	**F**ile **T**ransfer **P**rotocol
GPO	**G**roup **P**olicy **O**bject
IE	**I**ntelligence **E**conomique
IMAP	**I**nternet **M**essage **A**ccess **P**rotocol
ISA	**I**nternet **S**ecurity **A**cceleration
ISO	**I**nternational **S**tandard **O**rganisation
KDC	**K**ey **D**istribution **C**enter
LAN	**L**ocal **A**rea **N**etwork
OLA	**O**perating **L**evel **A**greement
OMD	**O**bjectifs du **M**illénaire pour le **D**éveloppement
OU	**O**rganizational **U**nit
PME	**P**etites et **M**oyennes **E**ntreprises
PMI	**P**etites et **M**oyennes **I**ndustries
PNUD	**P**rogramme des **N**ations **U**nies pour le **D**éveloppement
POP	**P**ost **O**ffice **P**rotocol
RAID	**R**edundant **A**rray of **I**nexpensive **D**isk
RC	**R**esponsabilité **C**ivile
SGSI	**S**ystème de **G**estion de la **S**écurité de l'**I**nformation
SIDA	**S**yndrome de l'**I**mmuno**D**eficience **A**cquise

SMTP	**S**imple **M**ail **T**ransfert **P**rotocol
SNU	**S**ytèmes des **N**ations **U**nies
SQL	**S**tructured **Q**uery **L**anguage
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket
UNDAF	**U**nited **N**ations **D**evelopment **A**ssistance **F**ramework
UPAS	**U**nité de **P**olitique et d'**A**nalyse **S**tratégique
USA	**U**nited **S**tates of **A**merica
VIH	**V**irus de l'**I**mmunodéficience **H**umaine
WLAN	**W**ide **L**ocal **A**rea **N**etwork

Liste des tableaux

Liste des figures

Table des matières

INTRODUCTION GENERALE

Le développement économique de tout organisme repose aujourd'hui sur l'utilisation quasi-systématique d'outils informatiques et bureautiques, généralement interconnectés à différents réseaux de télécommunication et principalement à internet.

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

La sécurité du système d'information est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenu un point primordial dans la mise en place de réseaux informatiques.

La majorité des opérations qu'il s'agisse de conception, de validation, de publication, etc. transitent par les réseaux informatiques. Ainsi l'exploitation des réseaux informatiques est sujette à d'énormes risques notamment les risques opérationnels qu'il convient d'identifier, d'évaluer, d'analyser et de hiérarchiser.

Les différentes revues sur les conseils politiques, sur l'appui technique et le plaidoyer envers les pays en développement sont élaborées, validées et publiées à travers son système d'information. La sensibilité de ces différents rapports a entrainé le PNUD Sénégal à mieux penser aux différents risques opérationnels liés à son réseau informatique.

Nous avons remarqué la persistance certains risques opérationnels qui peut s'expliquer par :

- l'absence d'un risque Manager ;
- l'absence de la cartographie des risques liés au réseau informatique ;

Les conséquences découlant des problèmes cités ci-dessus sont :

- écoute du réseau ;
- vols de fichiers ;
- espionnage ;
- attaques malicieuses ;

- désinformation ;
- erreurs humaines ;

Plusieurs pistes de solutions peuvent être envisagées pour la résolution des ces problèmes :

- la création de poste d'un risk manager ;
- l'élaboration d'une cartographie des risques liés au réseau informatique;

L'élaboration d'une cartographie des risques liés au réseau informatique nous semble plus appropriée dans un contexte où les nouvelles techniques d'audit privilégient l'approche par les risques.

C'est dans cette perspective que nous nous sommes interrogés sur ce qui suit :

Quel est le profil des risques opérationnels liés au réseau informatique du PNUD Sénégal ?

En d'autres termes:

- Quels sont les risques opérationnels liés au réseau informatique d'une institution en général ?
- Quelles sont les bonnes pratiques pour la maîtrise de ces risques ?
- Comment apprécier et évaluer ces risques et les formaliser dans une cartographie ?
- Quelles sont la nature et l'efficacité des dispositifs de contrôle interne mis en place par le PNUD Sénégal pour limiter la survenance et l'impact de ces risques ?
- Quels sont la probabilité de survenance, l'impact et les contre-mesures des risques identifiés ?
- Comment maîtriser et limiter davantage ces risques liés au réseau informatique du PNUD Sénégal ?

C'est pour répondre à ces questions que nous avons structuré notre thème de recherche sur : l'élaboration de la cartographie des risques liés au réseau informatique : Cas du PNUD-Sénégal).

L'objectif principal de notre étude est d'élaborer une cartographie des risques liés au réseau informatique du PNUD-Sénégal, lui permettant d'assurer un contrôle efficient de ses données issues des applications transitant par le réseau informatique pour enfin bénéficier des avantages qui en découlent.

A cet égard, un des objectifs spécifiques de l'étude est d'analyser l'efficacité des techniques d'évaluation des risques employées par le PNUD Sénégal pour assurer la sécurité du réseau informatique. Ensuite il nous sera permis de montrer, par la même occasion, que ces techniques, bien qu'elles soient efficaces, peuvent être vulnérables et qu'il conviendrait de mettre en place un dispositif de contrôle pour réduire l'impact des risques.

Aussi allons-nous:

- identifier tous les risques liés au réseau informatique ;
- étudier les avantages à élaborer une cartographie des risques informatiques ;
- mettre en évidence les différentes approches pratiques, en fonction des objectifs poursuivis et du point de vue de l'utilisateur de la cartographie ;
- évaluer ces risques et les analyser ;
- évaluer le contrôle interne pour en tirer les forces et les faiblesses ;
- proposer une cartographie des risques lies au réseau informatiques ;
- formuler des recommandations au regard des menaces constatées.

Notre étude portera sur le réseau informatique du PNUD Sénégal notamment :

- le réseau interne ;
- la zone démilitarisée ou DMZ ;

La pertinence de cette étude se manifeste par le fait qu'elle nous permettra de nous enquérir de tous les problèmes de sécurité qui existent dans le domaine de l'informatique c'est-à-dire les menaces et les attaques. Elle nous permettra en outre de mettre en pratique les connaissances théoriques acquises à l'école et de nous familiariser aux méthodes d'évaluation des risques opérationnels.

Ce sujet comportera deux parties.

La première partie concernera les aspects théoriques du réseau informatique et comprend trois chapitres repartis ainsi qu'il suit : le premier présentera les risques opérationnels du réseau informatique, le second sera consacré à la méthodologie d'élaboration d'une cartographie des risques et le troisième à la méthodologie de recherche.

La deuxième partie présentera l'aspect pratique du travail et se composera de deux chapitres : le premier concernera la présentation du Programme des Nations Unies pour le Développement Sénégal et le second présentera l'élaboration d'une cartographie des risques du PNUD Sénégal.

PREMIERE PARTIE : CADRE THEORIQUE

L'informatique et les technologies de communication sont devenues des outils performants et indispensables au quotidien. Ils permettent à une entité, qu'il s'agisse d'une entreprise, d'une administration, d'une organisation ou d'un citoyen, de réaliser certains objectifs et de rester concurrentielle. L'atteinte des objectifs définis par l'entité peut aussi bien nécessiter la création d'une vitrine de produits accessible via le Web, que la réalisation d'une base de données clients, la mise en place de services e-gouvernement en ligne ou simplement la connexion à Internet.

Pour pouvoir réaliser ses objectifs, l'entité en question va se doter des moyens nécessaires et implémenter une solution adéquate à ses besoins et à ses moyens. Même si la planification et la réalisation des outils mis en place sont effectuées de façon très consciencieuse, il existe toujours une certaine probabilité que l'entité échoue dans l'atteinte de ses objectifs. Cette probabilité a un nom : le risque informatique.

La gestion des risques informatiques nécessite l'utilisation d'outils adéquats qui permettent à l'entreprise d'atteindre les objectifs qu'elle s'est assignée. L'un des outils utilisés dans ce cadre est la cartographie des risques.

Nous consacrerons donc cette partie aux risques liés au réseau informatique, puis à la méthodologie d'élaboration de la cartographie des risques et nous terminerons par notre méthodologie de recherche.

Chapitre 1 : LES RISQUES LIES AU RESEAU INFORMATIQUE

Aujourd'hui les différentes opérations s'appuient de plus en plus sur le réseau informatique. Avec la libre circulation des informations et la haute disponibilité de nombreuses ressources, les responsables de réseaux d'entreprise doivent connaître toutes les menaces susceptibles de compromettre la sécurité. Celles-ci prennent de nombreuses formes, mais résultent toutes en une compromission de la confidentialité à un certain degré et en une destruction possible de données ou de ressources pouvant conduire à des pertes financières considérables.

La compréhension des risques liés au réseau informatique nécessite la définition de concepts importants. Ainsi nous présenterons le réseau informatique, puis les risques qui y résultent ainsi que leur gestion et nous terminerons par le dispositif de contrôle interne sur lequel doit reposer l'entreprise pour être performante.

1.1. Présentation du réseau informatique

L'ancêtre des réseaux est le réseau Arpanet (de l'Advanced Research Projects Agency), créé en 1968 par le département américain de la Défense, dans un but stratégique, pour relier ses centres de recherche. Le but était de concevoir un réseau qui résiste à des attaques militaires telles que des bombardements. Ainsi, il ne devait pas y avoir de point névralgique dans le réseau, dont l'arrêt aurait provoqué le blocage complet de celui-ci, et les données devaient pouvoir automatiquement prendre un chemin différent en cas de coupure de liaison. D'où l'absence de contrôle centralisé dans l'Internet et un cheminement dynamique des données.

Nous définirons donc le réseau informatique afin d'avoir une vision de sa fonction.

1.1.1. Définition du réseau informatique

Le mot réseau est très souvent employé dans un sens qui le lie aux communications. Ex : le réseau téléphonique, le réseau routier ou réseau de trafiquants d'armes.

PUJOLLE (2011 : 3), définit : Un réseau est un ensemble d'équipements et de liaisons de télécommunications autorisant le transport d'une information, quelle qu'elle soit, d'un point à un autre, où qu'il soit.

Dans son Aide Mémoire des réseaux et télécoms, SERVIN (2012 : 3), affirme qu'en informatique, le terme réseau recouvre un ensemble de moyens technologiques et logiciels mis en œuvre pour permettre l'échange de données entre ordinateurs.

TANENBAUM et WETHERALL (2010 : 2), disent qu'un « Réseau d'ordinateurs » est pour désigner un ensemble d'ordinateurs autonomes interconnectés au moyen d'une seule technologie leur permettant d'échanger des informations.

En informatique deux ordinateurs reliés entre eux par un câble forment déjà un réseau. Deux réseaux reliés entre eux par un quelconque moyen permettant aux informations de circuler (ligne téléphonique, satellite...) forment un nouveau réseau.

Un réseau informatique permet à plusieurs machines (ordinateurs au sens large) de communiquer entre elles afin d'assurer des échanges d'informations: du transfert de fichiers, du partage de ressources (imprimantes et données), de la messagerie ou de l'exécution de programmes à distance.

1.1.2. Types des réseaux informatiques

DORDOIGNE (2005 :14), à travers Réseaux Locaux Et Étendus nous définit les notions fondamentales des LAN, MAN, WAN etc.

- **Les LAN**

Les réseaux LAN (Local Area Network) sont les réseaux locaux. Les ordinateurs sont reliés par l'intermédiaire de câbles dans une petite zone géographique. (La technologie Ethernet est utilisée pour relier les PC). Un réseau local est donc un regroupement de PC étant proches les uns des autres reliés au réseau (soit avec des fils et en utilisant la technologie Ethernet qui permet de monter à plus de 100 Mbits par seconde (et 1Gbit pour le GigaEthernet), soit sans fils avec des technologies comme le WIFI).

- **Les MAN**

Les réseaux métropolitains MAN (Metropolitan Area Network).Ce type de réseau est apparu relativement récemment et peut regrouper un petit nombre de réseaux locaux au niveau d'une ville ou d'une région. Par exemple, une banque peut décider de créer un 'MAN' pour relier ses

agences sur un rayon de quelques kilomètres. La bande-passante peut être de quelques centaines de kbits/s à quelques Mbits/s.

❖ **Les WAN**

Les réseaux distants WAN (Wide Area Network).Ce type de réseau permet l'interconnexion de réseaux locaux et métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville. L'infrastructure est en général publique (Poste, Télécom, Banques etc.) et l'utilisation est facturée en fonction du trafic et/ou en fonction de la bande-passante réservée, pour les lignes louées. Les modems sont un des éléments de base des WANs. La bande passante va de quelques Kbits/s à quelques Mbit/s. Une valeur typique pour une ligne louée est de 64kbits/s (en fonction des services offerts).

1.1.3. Topologies des réseaux informatiques

SERVIN (2013 : 67), dans son ouvrage Réseaux Et Télécoms nous décrit les différents protocoles IP, les architectures réseaux etc.

La topologie décrit comment les machines sont raccordées au réseau, c'est-à-dire la connexion physique entre les machines.

1.1.3.1. La topologie en bus

C'est une ancienne topologie aujourd'hui peu utilisée. Elle consiste à relier chaque ordinateur à un "bus" par l'intermédiaire souvent de câbles coaxiaux.

Elle a par contre de nombreux défauts :

- Une lenteur assez importante ;
- Une vulnérabilité importante en cas de panne. En effet, si un câble est en panne le réseau ne fonctionne plus ;

Figure 1 : Topologie en bus

Source : Nous même

1.1.3.2. La topologie en étoile

C'est la topologie la plus utilisée aujourd'hui. Les réseaux qui utilisent cette topologie, ont un point central commun auquel sont connectés tous les nœuds du réseau (généralement un concentrateur).

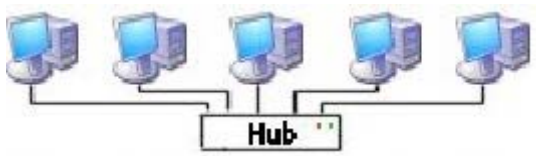
Les avantages principaux :

- Chaque nœud est indépendant, contrairement aux topologies en bus ou en anneau, la défaillance d'un nœud n'affecte pas le reste du réseau ;
- Il est très simple de rajouter ou d'enlever des nœuds au réseau ;

Les principaux désavantages :

- Cette topologie nécessite un câblage bien plus important qu'une topologie en bus, ce qui implique un coût plus élevé ;
- Si le nœud central est victime de défaillance, tout le réseau tombe en panne ;

Figure 2 : Topologie en étoile



Source : Nous même

1.1.3.3. La topologie en en étoile étendue

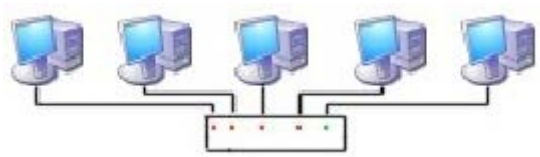
Structure de réseau constituée d'une topologie en étoile principale, et d'autres topologies en étoile secondaires.

L'avantage d'une topologie en étoile étendue est de réduire les longueurs de câble et de limiter le nombre d'unités interconnectées à un nœud central. Son plus grand désavantage est que, si le nœud central connaît une défaillance, tout le réseau est en panne.

1.1.3.4. La topologie en anneau

La topologie en anneau est une structure en cercle où chaque nœud est connecté à 2 autres nœuds. Les trames sont généralement envoyées dans une seule direction. Chaque nœud recevant des informations doit les retransmettre au nœud suivant.

Figure 3 : Topologie en anneau



Source : Nous même

1.1.3.5. La topologie hiérarchique

Topologie de réseau local similaire à une topologie en bus, excepté que les réseaux en arbre peuvent contenir des branches avec plusieurs nœuds. Les émissions d'une station se propagent sur toute la longueur du média et sont reçues par toutes les autres stations.

1.1.3.6. La topologie maillée

Topologie réseau dans laquelle des segments relient les nœuds dans une topologie ne pouvant se réduire à un cas plus simple. Dans un maillage intégral (full mesh), chaque nœud est directement relié à tous les autres. L'usage le plus fréquent des réseaux maillés, sont des réseaux internationaux WAN (Wide Area Network) Réseau pouvant s'étendre au monde entier

1.1.4. Architecture des réseaux informatiques

L'architecture des réseaux informatiques se décomposent en architecture client-serveur et en architecture poste à poste (peer to peer).

1.1.4.1. Architecture client-serveur

❖ **Serveur**

Est une machine qui offre un service sur le réseau. Le serveur accepte des requêtes, les traite et renvoie le résultat au demandeur. Le terme serveur s'applique à la machine sur lequel s'exécute le logiciel serveur.

Client

Est une machine qui utilise le service offert par un serveur. Le client envoie une requête et reçoit la réponse. Le client peut-être raccordé par une liaison temporaire.

❖ **Architecture client/serveur**

C'est la description du fonctionnement coopératif entre le serveur et le client. Les services Internet sont conçus selon cette architecture. Ainsi, chaque application est composée de logiciel serveur et logiciel client. A un logiciel serveur, peut correspondre plusieurs logiciels clients développés dans différents environnements: Unix, Mac, PC...

Exemple :

A titre d'illustration, le réseau local d'un établissement scolaire est organisé autour d'un ordinateur central (le serveur) auquel tous les autres ordinateurs de l'établissement (les clients) sont connectés. Cela signifie que sous une architecture client/serveur, toutes les requêtes envoyées sur le réseau par les élèves ou leurs enseignants sur leur ordinateur sont exécutées par le serveur qui centralise l'envoi et la réception de courrier électronique ou la réception de page web entre autres.

Passage obligé entre les « clients » et l'Internet, le serveur distribue les données reçues et envoyées auprès de chaque ordinateur connecté à lui et destinataire ou expéditeur des données.

Avantages

Un des gros avantages de ce mode client/serveur est sa relative simplicité de fonctionnement. En effet, une fois que vous avez l'information que vous souhaitez partager, vous ouvrez un

serveur, et vous n'avez plus qu'à attendre les clients. Bien sûr, ici, pas question d'attendre que quelqu'un rentre à l'improviste, il faut faire connaître votre serveur.

Ce mode permet surtout une grande simplicité des mises à jour : chaque possesseur d'information la met sur un serveur (on parle alors d'upload d'une information, contrairement au download qui consiste à rapatrier les informations du serveur vers le client), et elle est disponible immédiatement pour tout le monde.

Inconvénient

Le problème de ce mode de fonctionnement est son coût. En effet, si un ordinateur un peu puissant suffit largement à traiter quelques requêtes simultanées, dès que le nombre de requêtes devient grand, les serveurs (ordinateurs utilisés uniquement pour fournir un type de service) doivent se multiplier, et la connexion réseau doit également être augmentée, faute de quoi les performances (temps de réponse du serveur) seront dégradées. Le pire des cas est un crash du serveur : celui-ci n'est plus en mesure de répondre.

1.1.4.2. Architecture Poste à Poste (Peer to Peer)

Le terme P2P, abréviation de “Peer -to- Peer” (“égal à égal”). Il désigne un type d’architecture de réseau informatique, connexion directe entre deux ou plusieurs ordinateurs, où chacun joue à la fois un rôle de client et de serveur, par opposition au simple schéma client/serveur.

1.1.5. Câblage des réseaux informatiques

Le medium de transport correspond aux éléments matériels et immatériels capables de transporter des données binaires (0 et 1), comme les câbles et les ondes radio. Dans le premier cas, ce sont des fils métalliques ou des fibres optiques qui transportent l’information et dans le second cas les ondes hertziennes.

Les deux types de support sont complémentaires. Le hertzien permet la mobilité mais à débit plus faible. De son côté, le câble propose des débits de plus en plus importants. On arrive aujourd’hui à des dizaines de gigabits par seconde sur la fibre optique contre des centaines de mégabits par seconde pour le hertzien. Cette section examine les caractéristiques de ces différents médias de transmission afin de mieux comprendre leurs architectures et leur fonctionnement.

1.1.5.1. Câble coaxial

Ce type de câble est utilisé pour la transmission de signaux numériques ou analogiques à haute ou basse fréquence. Par exemple, vous trouverez un câble coaxial, entre votre antenne TV et votre télévision.

1.1.5.2. Paire torsadée

Le câble à paire torsadée **(Twisted-pair câble)** est un câble réseau dont les fils sont regroupés deux par deux. Il est souvent fabriqué à partir de plusieurs paires torsadées regroupées et placées à l'intérieur d'une gaine protectrice.

1.1.5.3. Fibre optique

La fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

1.1.5.4. Wi-Fi

Le Wifi, pour Wireless Fidelity, est une technologie standard d'accès sans fil à des réseaux locaux. Le principe est d'établir des liaisons radio rapides entre des équipements et des bornes reliées au réseau haut débit. Cette technologie permet en principe une interopérabilité totale des équipements, quelle que soit la marque ou la nature du terminal

Grâce au Wifi, il est possible de créer des réseaux locaux sans fils à haut débit. Il permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres.

1.1.6. Protocole réseaux

L’échange de données nécessite un support physique (au sens large), mais surtout des programmes qui vont assurer la qualité et le contrôle d’échange. En effet un échange d'information, nécessite au moins deux partenaires qui se comprennent. Ainsi, la

communication ne peut avoir lieu que si l'un et l'autre des intervenants respectent les mêmes conventions.

Un protocole réseau est un ensemble de règles et de procédures de communication utilisées de part et d'autre par toutes les stations qui échangent des données sur le réseau.

1.1.6.1. Protocole TCP/IP

Le protocole TCP est défini dans le but de fournir un service de transfert de données de haute fiabilité entre deux ordinateurs raccordés sur un réseau.

Dans le monde des réseaux, les machines sont identifiées par leurs adresses IP.

Une adresse IP est une série unique de nombres (par exemple 41.224.215.143) qui permet d'identifier un ordinateur sur un réseau. C'est l'équivalent de l'adresse postale d'un particulier ou d'une entreprise.

Le rôle du protocole IP, peut être comparé, par le rôle de la poste. En effet, la poste joue un rôle fondamental, dans la distribution des lettres à leurs correspondants. Donc, la poste doit envoyer les lettres suivant les adresses de destinations, pour ce faire, elle doit suivre des règles et des procédures bien précises.

- la priorité de chaque lettre ;
- la distance entre l'émetteur et le destinataire ;
- le chemin que doit parcourir la lettre, pour arriver le plus vite possible ;

Parallèlement, le protocole IP, joue un rôle fondamental dans l'échange des informations sur Internet. Pour cela, il suit un ensemble de règles standard, pour déterminer les chemins de paquets IP, et de parvenir chaque paquet à sa destination.

1.1.6.2. Protocole ARP

ARP (Adress Resolution Protocol) est utilisé dans un LAN pour déterminer l'adresse physique ou l'adresse MAC (Medium Access Card) d'une machine à partir de son adresse IP.

Les adresses MAC sont gravées dans une mémoire (ROM) des cartes réseau. Chaque carte réseau possède une adresse MAC unique dans le monde depuis sa fabrication.

Quand un ordinateur donné doit communiquer avec un autre ordinateur en utilisant son adresse IP, il regarde tout d'abord si le destinataire est répertorié dans son cache ARP. S'il l'est, une trame est associé avec l'adresse MAC du destinataire, puis expédiée sur le réseau : les deux équipements peuvent alors communiquer.

Sinon, une requête ARP est envoyée sur le réseau, dans le but d'obtenir une information indispensable pour l'envoi d'une trame et donc de données : l'adresse MAC du destinataire.

1.1.6.3. Protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est une norme IP conçue pour faciliter l'administration des configurations d'adresses en utilisant un ordinateur serveur pour centraliser la gestion des adresses IP et des autres éléments de configuration associés utilisés sur votre réseau. Le service DHCP permet à l'ordinateur serveur de fonctionner comme un serveur DHCP et de configurer des ordinateurs clients DHCP sur votre réseau.

1.1.6.4. Protocole DNS

Le protocole DNS (Domain Name System) est la corrélation entre les adresses IP et le nom de domaine associé.

L'utilisation d'un serveur DNS simplifie la gestion du réseau car les utilisateurs ont simplement besoin de connaître le nom des machines sans se préoccuper des adresses IP.

1.1.7. Matériels pour le réseau informatique

Les matériels pour le réseau informatique sont : carte réseau, concentrateur, commutateur, passerelles, routeurs.

1.1.7.1. Carte réseau

Une carte réseau est une carte de circuits imprimés qui permet la communication réseau depuis et vers un ordinateur. La carte réseau se connecte à la carte mère et est pourvue d'un port permettant de relier l'ordinateur au réseau.

Chaque carte à besoin d'une adresse MAC (Medium Access Unit) unique stocké dans sa mémoire depuis sa fabrication, cette adresse est nécessaire dans la communication avec les autres ordinateurs.

1.1.7.2. Concentrateur

Elément central d'un réseau, il est utilisé pour recevoir les câbles des divers ordinateurs connectés au réseau. Le concentrateur est ainsi un boîtier possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32). Le concentrateur permet ainsi de connecter plusieurs machines entre elles afin de concentrer un plus grand nombre. Il est utilisé généralement dans les topologies en étoiles avec des câbles RJ45.

1.1.7.3. Commutateur

Equipement réseau permettant l'interconnexion d'équipements informatique en réseau local en optimisant la bande passante. Contrairement au concentrateur, qui transmet chaque trame arrivant d'un port vers tous les autres ports, il ne transmet que le trafic réseau qu'entre les ports impliqués dans la communication.

Dès lors, lorsqu'un équipement connecté sur le port 4 d'un commutateur envoie une trame à destination d'un équipement connecté sur le port 14 de ce même commutateur, seuls ces 2 ports sont interconnectés, tous les autres ports étant préservés de ce trafic réseau.

1.1.7.4. Passerelles

La passerelle (en anglais, Gateway) est un dispositif permettant de relier deux réseaux informatiques différents, comme par exemple un réseau local et l'Internet. Elle permet de faire l'interface entre des protocoles réseau différents. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à l'Internet par l'intermédiaire de la passerelle.

1.1.7.5. Routeurs

Le routeur est un élément principal dans les réseaux. Pour résumer, c'est un guide: vous lui demandez votre route, il vous accompagne vers la bonne destination. Sa fonction principale est de prendre un paquet et de le renvoyer au bon endroit en fonction de la destination finale.

1.1.8. Internet, Intranet et Extranet

Parmi tous les réseaux existants, les trois (3) réseaux les plus importants pour l'entreprise sont : internet, intranet et extranet.

1.1.8.1. Internet

Eric Larcher dans son ouvrage L'Internet Sécurisé définit L'internet comme « est un réseau informatique mondial qui résulte de l'interconnexion d'un grand nombre de réseaux publics ouverts qui utilisent un protocole de communication commun appelé TCP /IP ».

1.1.8.2. Intranet

L'intranet est un réseau informatique utilisé à l'intérieur d'une entreprise ou d'une organisation et qui recourt au même protocole de communication que l'internet (Adressage IP et serveur http). C'est un réseau qui doit être fermé, protégé et utilisable uniquement par les membres de l'entreprise avec un accès contrôlé par mot de passe.

1.1.8.3. Extranet

L'extranet est une ouverture contrôlée et sécurisée d'un intranet à des partenaires extérieurs à l'entreprise (clients, fournisseurs etc.). C'est un réseau privé qui interconnecte plusieurs intranets d'entreprises qui souhaitent communiquer entre elles en utilisant les protocoles internet avec adressage IP et serveur http.

1.1.9. Organisation réseau-SGBD-Sécurité-Sauvegarde

Nous évoquerons l'organisation réseau, le système de gestion des bases de données, la sécurité et enfin la sauvegarde.

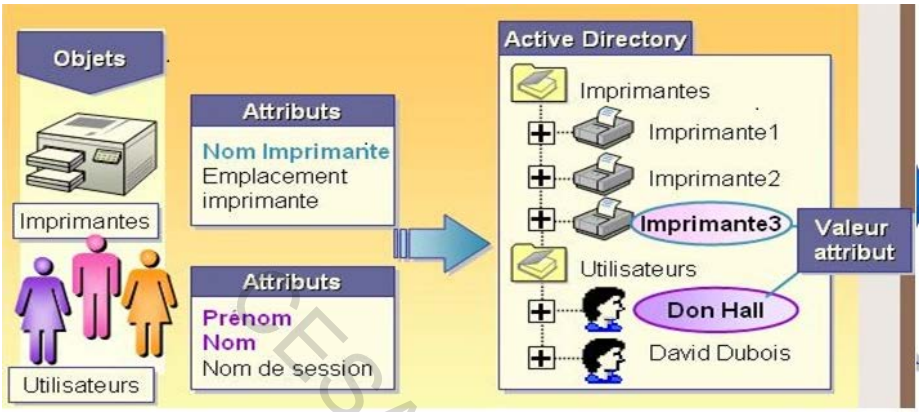
1.1.9.1. Organisation réseau

L'application par excellence qui permet de faire de l'organisation réseau est la plate forme de Microsoft qui se nomme Active Directory.

José Dordoigne dans Réseaux Informatiques, Maîtrisez Les Fondamentaux définit « Active Directory est un annuaire des objets du réseau, il permet de centraliser, de structurer, d'organiser et de contrôler les ressources réseau dans un environnement Windows ».

Stephen A dans son ouvrage Windows NT Security Guide nous renseigne que « Active Directory stocke les informations sur les objets du réseau à savoir les utilisateurs, les ordinateurs, les imprimantes… ».

Figure 4 : Active Directory illustration



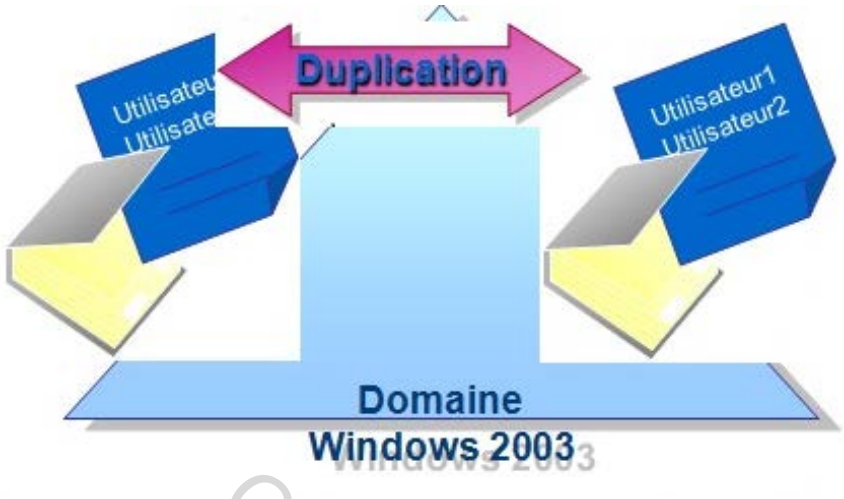
Dan Holme, Nelson Ruest, Danielle Ruest dans leur ouvrage Configuration d'une infrastructure Active Directory avec Windows Server 2008 définit les différents composants de AD.

Les composants logiques d'Active Directory sont les sites, domaines et unités organisationnelles.

Un site est une combinaison d'un ou de plusieurs sous-réseaux connectés entre eux par une liaison à haut débit fiable.

Un domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données. L'administrateur d'un domaine ne peut qu'administrer son domaine.

Figure 5 : Domaine d'Active Directory illustration

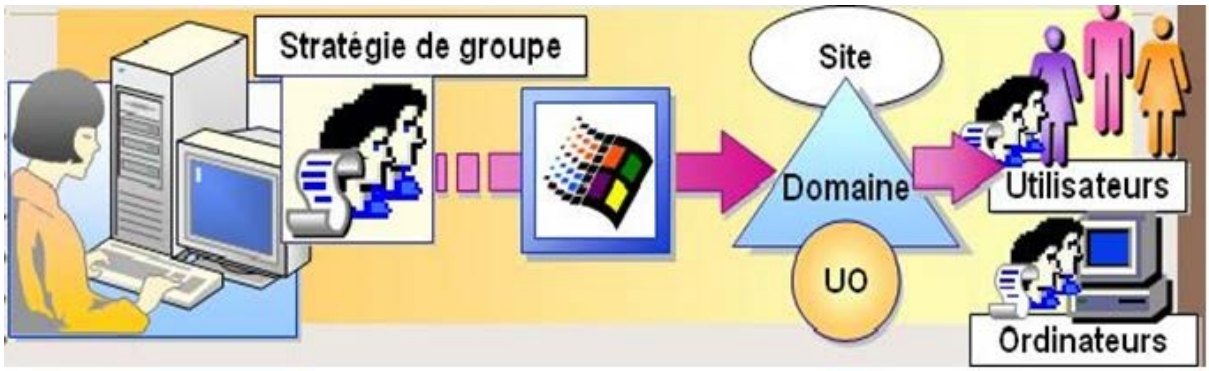


Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.

Figure 6 : Unité d'organisation -Active Directory illustration

Une stratégie de groupe est un objet d'AD qui va contenir un ensemble de paramètres. Ces paramètres vont agir sur l'environnement d'un utilisateur ou d'un ordinateur. Il est aussi appelé Group Policy Object.

Figure 7 : Stratégie de groupe -Active Directory illustration



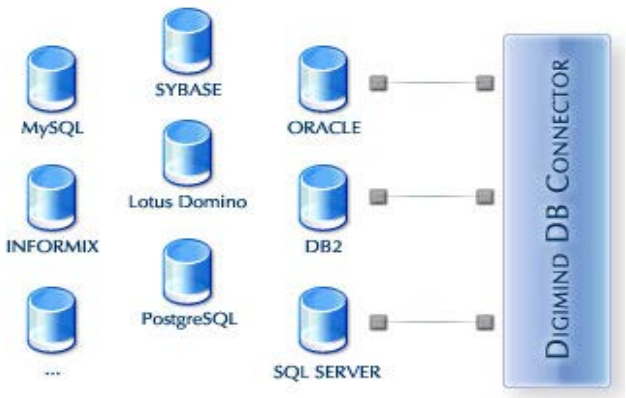
1.1.9.2. Système de Gestion de la Base de Données

Un système de gestion de base de données est un ensemble de logiciels qui sert à la manipulation des bases de données. Il sert à effectuer des opérations ordinaires telles que consulter, modifier, construire, organiser, transformer, copier, sauvegarder ou restaurer des bases de données. Il est souvent utilisé par d'autres logiciels ainsi que les administrateurs ou les développeurs.

L'ensemble, dont le composant central est le moteur de base de données, peut être sous forme de composant logiciel, de serveur, de logiciel applicatif ou d'environnement de programmation. Il permet généralement à plusieurs utilisateurs et plusieurs logiciels de manipuler plusieurs bases de données en même temps et ceci quel que soit le contenu et l'organisation des bases de données.

Les principales bases de données sont : Oracle, Mysql, Microsoft Access

Figure 8 : Principales bases de données illustration



Source : Digimind Inc

1.1.9.3. Sécurité informatique

IFACI dans son ouvrage Les Principes De La Sécurité Informatique nous décrit La sécurité du réseau informatique comme « est un vaste domaine qui regroupe tous les équipements (matériel et logiciel) ainsi que les bonnes pratiques chargées d'assurer la conservation, l'intégrité et la fiabilité des informations traitées ».

Nous avons la sécurité matérielle qui est constituée des différents équipements tels que les portes badgés, les protections des prises anti foudre, l'onduleur, système antivol, système anti-incendie qui permettent de lutter contre les incendies, le dégât des eaux, le vol des matériels, les microcoupures, surtensions, baisses de tensions et les coupures momentanées et également les intrusions.

La sécurité logicielle qui est constituée à la fois des pare feux matériels (ISA Firewall, Firewall ASA, Serveur SUS, Serveur d'Antivirus, Serveur AAA) et logiciels (les logiciels d'antivirus et anti spywares, les logiciels de mises à jour, le système d'authentification via les certificats ou le LDAP) qui permettent de lutter contre les attaques informatiques, les virus, les spywares etc.

Solange Ghernaouti-Hélie dans son ouvrage Sécurité Informatique Et Réseaux nous renseigne que la sécurité du réseau informatique se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

- élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de conseiller les décideurs sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en terme de sécurité.

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- une procédure de management des mises à jour ;
- une stratégie de sauvegarde correctement planifiée ;
- un plan de reprise après incident ;
- un système documenté à jour ;

1.1.9.4. Sauvegarde informatique

En informatique, la sauvegarde (backup en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

Ce terme est à distinguer de deux notions proches :

- l'enregistrement des données, qui consiste à écrire des données sur un périphérique, tel qu'un disque dur, une clé USB, des bandes magnétiques, où les informations demeureront même après l'extinction de la machine, contrairement à la mémoire vive.
- l'archivage, qui consiste à enregistrer des données de manière à garantir sur le long terme leur conformité à un état donné, en général leur état au moment où elles ont été validées par leurs auteurs.

La sauvegarde passe forcément par un enregistrement des données, mais pas nécessairement dans un but d'archivage.

❖ **La sauvegarde complète**

Les fichiers sont sauvegardés sans tenir compte d'une éventuelle sauvegarde antérieure. Inutile de dire que cette sauvegarde est celle qui occupe le plus d'espace. Pour cette raison, il est préférable de n'utiliser ce type de sauvegarde qu'épisodiquement.

Pour restaurer sa sauvegarde, il suffit d'utiliser uniquement les fichiers créés par sauvegarde complète.

❖ **La sauvegarde incrémentale**

Cette sauvegarde examine le contenu de la dernière sauvegarde en date (peu importe son type). Elle compare cette sauvegarde avec l'état actuel du système et ne sauvegarde que ce qui a changé. Évidemment, la taille occupée par cette sauvegarde est réduite étant donné qu'elle ne s'occupe que des modifications récentes du système. C'est le type de sauvegarde qu'il faut appliquer journalièrement, du moins, régulièrement.

Pour restaurer son système, il faut restaurer la dernière sauvegarde complète puis toutes les sauvegardes incrémentales effectuées depuis, et dans l'ordre !

❖ **La sauvegarde différentielle**

Fort semblable à la sauvegarde incrémentale, cette sauvegarde ne s'occupe que de ce qui a changé depuis la dernière sauvegarde **complète**.

Ici, pour restaurer le système, il suffit de restaurer la sauvegarde complète puis la dernière différentielle.

❖ **Stratégie de sauvegarde**

Selon vos besoins, plusieurs stratégies me paraissent envisageables.

Il est nécessaire d'effectuer des sauvegardes complètes périodiquement, mais avec une fréquence assez réduite (une fois par mois, par exemple).

On doit combiner cela avec des sauvegardes incrémentales et différentielles plus fréquentes.

1.2. Risques liés au réseau informatique

Le risque est inhérent à l'entreprise et constitue même son essence. Nous définirons donc la notion de risque ainsi que celle de risque opérationnel.

1.2.1. Notion de risque

L'utilisation au quotidien des applications (base de données, intranet, internet etc.) liés au réseau informatique peuvent se révéler être source de risques. Les risques doivent donc être identifiés, mesurés et maîtrisés pour éviter à l'entreprise une perte financière, une affectation de l'image de marque, et enfin une perte de crédibilité, etc.

1.2.1.1. Définition du risque

Nombreux auteurs ont apporté une définition du risque,

Selon l'IFACI (RENARD 2006 : 115), « le risque est un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ».

Selon HAMZAOUI (2005 : 37), « le risque est un concept selon lequel la direction exprime ses inquiétudes concernant les effets probables d'un évènement sur les objectifs de l'entité dans un environnement incertain ».

Pour une meilleure compréhension de la notion de risque, il existe une équation reine (applicable également à d'autres domaines que l'informatique)

RISQUE = MENACE * IMPACT * VULNERABILITE

Les «menaces» désignent l'ensemble des éléments (généralement externes) pouvant atteindre les ressources informatiques d'une organisation ;

Les «vulnérabilités» expriment toutes les faiblesses des ressources informatiques qui pourraient être exploitées par des menaces, dans le but de les compromettre ;

L'«impact» est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, perte de crédibilité, etc.

La combinaison des ces trois facteurs fonde le «risque», qui permet notamment de mesurer l'impact financier et/ou la probabilité de survenance d'un événement indésirable.

1.2.1.2. Types de risques

Les risques liés au réseau informatique peuvent être classées en deux groupes :

- les risques financiers ;
- les risques opérationnels.

1.2.1.2.1. Les risques financiers

Nous ne nous attarderons pas sur ce risque car il n'entre pas dans le cadre des risques que nous étudions.

Le risque financier est celui qui paraît le plus évident, dans la mesure où tout dommage s'accompagne en principe d'une perte et d'une réparation (pour certains, les entreprises ne connaissent qu'un risque, celui de perdre de l'argent).Il se définit comme l'événement aléatoire

pouvant avoir un impact sur le résultat de l'entreprise et pouvant affecter son patrimoine. Le risque financier est un risque initial pouvant entrainer à son tour l'occurrence d'autres risques.

1.2.2. Les risques opérationnels

Nous définirons les risques opérationnels et les recenserons.

SENFT (2008 : 230), dans son ouvrage Information Technology Control and Audit nous définit les différents risques liés au réseau informatique.

1.2.2.1. Définition des risques opérationnels

Les risques trouvent leurs origines dans :

- les causes accidentelles ;
- les erreurs ;
- la malveillance ;

1.2.2.2. Les risques accidentels

Les risques accidentels se déclinent en risques matériels, pannes et dysfonctionnement.

1.2.2.2.1. Les risques matériels

C'est la destruction totale ou partielle d'un ou plusieurs composants d'un système d'information (matériel informatique ou de communication, supports de données, environnement tels que locaux, conditionnement d'air, alimentation électrique, installation téléphonique, …) suite à des événements comme un choc, la coupure de câbles électriques ou téléphoniques, l'incendie, l'inondation, la foudre, la tempête, etc.

1.2.2.2.2. Pannes et dysfonctionnement de matériel ou de logiciel de base

Généralement, les interruptions de service consécutives à des pannes sont de courte durée mais ce n'est pas toujours le cas. Des défaillances de matériel ou de logiciels de base ont provoqué des arrêts de fonctionnement de serveurs importants s'étendant sur plusieurs jours ouvrables.

Les interruptions peuvent aussi résulter de pannes dont l'origine est externe à l'entreprise (réseau téléphonique, alimentation électrique, …).

L'impossibilité d'accéder au réseau Internet peut empêcher une organisation de recevoir ou d'émettre du courrier électronique ou faire en sorte qu'un site de commerce électronique ne puisse plus recevoir de commandes.

A ce niveau également, les CEO, les CIO et les CISO seront bien avisés de jauger régulièrement leur dépendance de la continuité du « réseau des réseaux » et d'envisager des solutions de continuité alternatives pour leurs processus les plus critiques, dans la mesure du possible bien entendu.

1.2.2.3. Les risques liés aux erreurs

Les risques liés aux erreurs s'articulent autour des risques liés aux erreurs de saisie, de transmission et d'utilisation de l'information, aux erreurs d'exploitation, aux erreurs de conception et de réalisation

1.2.2.3.1. Les risques liés aux erreurs de saisie, de transmission et d'utilisation de l'information

On a tendance à sous-estimer les erreurs de saisie de données. Même après vérification, elles atteignent couramment un taux de 0,5 %. A tort, on les considère comme une conséquence inéluctable de l'activité humaine, alors qu'elles sont à l'origine d'un nombre élevé de problèmes et de pertes pouvant être importantes. De bons contrôles de vraisemblance des données saisies sont une mesure indispensable.

La transmission de données, qu'elle se fasse par transport de supports ou par télécommunications, est sujette à altération de données ou détournements, sans compter les transmissions des mauvais fichiers.

D'une manière générale, les erreurs humaines de tous types sont une grande source de préoccupation. Des défauts organisationnels ou de communication interne, tels que la non-suppression d'un mot de passe attribué à une personne licenciée, peuvent être lourds de conséquences.

1.2.2.3.2. Les risques liés aux erreurs d'exploitation

Ces erreurs prennent des formes variées : effacement accidentel de fichiers, supports ou copies de sauvegarde, chargement d'une version incorrecte de logiciel ou de copie de sauvegarde, lancement d'un programme inapproprié, …

II est souvent difficile d'identifier la cause exacte de ces problèmes : faute professionnelle, malveillance, erreur, négligence, laxisme, … Une analyse pointue des processus et des éléments endogènes ou exogènes, qui ont provoqué l'erreur, prendra du temps et risque d'être coûteuse pour l'entreprise.

1.2.2.3.3. Les risques liés aux erreurs de conception et de réalisation

Alors que le nombre d'erreurs des deux catégories précédentes a tendance à se stabiliser et même à diminuer, les erreurs de conception et de réalisation sont en forte augmentation. Il suffit pour s'en convaincre de consulter les publications internationales qui recensent des dizaines de nouvelles vulnérabilités chaque semaine.

D'une part, des logiciels conçus et réalisés il y a bon nombre d'années sont toujours utilisés de manière opérationnelle. Leur documentation est souvent inexistante, incomplète ou mauvaise et n'est plus à jour. Leurs auteurs ne sont plus disponibles pour assurer la maintenance. La qualité de la programmation est généralement médiocre. Toute évolution, adaptation ou correction de ces logiciels devient dès lors une gageure, qui entraîne fréquemment des dysfonctionnements graves et imprévisibles.

D'autre part, on développe chaque jour de nouveaux logiciels de grande taille et d'une complexité sans cesse croissante. Les ambitions dépassent quelquefois l'état de l'art ou la compétence de leurs auteurs. Les développements s'appuient souvent sur des bibliothèques de composants ou des logiciels de base eux-mêmes truffés d'erreurs.

1.2.2.4. Les risques liés à la malveillance

Les risques liés à la surveillance s'identifient aux risques liés au vol et sabotage de matériel, aux fraudes, au sabotage immatériel, aux indiscrétions et détournements d'informations et de logiciels.

1.2.2.4.1. Les risques liés au vol et sabotage de matériel

Les vols portent principalement sur les petits matériels, tels que les ordinateurs portables et les supports informatiques (disques de serveurs, …). La disparition d'un PC ou d'un serveur peut être lourde de conséquences au cas où celui-ci n'a pas fait l'objet d'une copie de sauvegarde récente et complète ou encore lorsque celui-ci contient des données ou programmes confidentiels.

Le sabotage va de l'endommagement d'un appareil isolé aux attentats terroristes détruisant toute une infrastructure.

L'utilisation de matériels hors standards du marché aggrave les conséquences d'un vol ou d'un sabotage dans la mesure où l'obtention de matériels de remplacement peut s'avérer plus difficile. Cette dimension du risque (diminution de sa capacité à réagir) devrait être prise en compte par le CIO dans ses choix technologiques.

1.2.2.4.2. Les risques liés aux fraudes

Kenneth Lindup dans son ouvrage The Computer Security And Fraud Prevention Audit nous décrit les différents risques liés aux fraudes dans un réseau informatique.

La pratique des fraudes est aussi vieille que le monde. L'informatique y a cependant ajouté de nouvelles dimensions :

- le montant moyen des fraudes informatiques est sensiblement plus élevé que celui des fraudes traditionnelles ;
- le manque d'enregistrements visibles réduit les chances de détection par observation fortuite ;
- programmes et données peuvent dans bien des cas être modifiés sans laisser de traces et être effacés avec une rapidité extrême. Il n'est pas rare qu'un fraudeur efface les fichiers comportant les traces de ses méfaits, ainsi que toutes ses copies de sauvegarde ;
- la sécurité est souvent sacrifiée au profit de l'efficience ;
- la complexité de certains systèmes est telle que les utilisateurs ne disposent plus de la compétence requise pour vérifier l'exactitude des résultats produits ;

- les contrôles organisationnels classiques (séparation de fonctions et de connaissances, doubles contrôles, …) ont été négligés lors de l'introduction des nouveaux systèmes ;
- de nombreux systèmes informatiques ont été réalisés sans prendre la sécurité en compte lors de leur conception ;
- le personnel technique peut contourner des contrôles essentiels ;

Les fraudes informatiques conduisent à des détournements de biens et de fonds. Elles peuvent également avoir pour conséquence le sabotage du fonctionnement :

- des exécutants, que l'on induit en erreur (p.ex. livraison à des clients dont l'insolvabilité a été masquée, acceptation de risques tarés dans une compagnie d'assurances par manipulation de l'historique des sinistres, …) ;
- des gestionnaires, en basant le contrôle de gestion sur des états incorrects, ce qui peut conduire à ne pas prendre des décisions qui s'imposeraient ou à prendre des décisions inappropriées qui pourraient avoir des conséquences désastreuses (p.ex. rentabilité des départements et produits, situations de trésorerie, …) ;

1.2.2.4.3. Les risques liés au sabotage immatériel

Le sabotage immatériel concerne l'altération ou la destruction, totale ou partielle, des données, des programmes ou de leurs sauvegardes. Ses conséquences peuvent être aussi graves et parfois même davantage que celles d'un sinistre matériel, car il peut provoquer des destructions en profondeur et avoir pour effet de neutraliser pendant un temps long le fonctionnement du système informatique.

Le sabotage immatériel recouvre diverses notions :

- la modification non autorisée de programmes ;
- le cheval de Troie qui est une partie de programme pernicieuse ajoutée à un autre programme dont le comportement externe paraît normal ;
- les bombes logiques, qui sortent leurs effets destructeurs de données ou de programmes lors de la réalisation d'un événement (p.ex. survenance d'une date particulière, destruction de fichiers lorsque le matricule de l'auteur licencié disparaît du fichier du personnel,…). Une forme particulièrement dommageable de bombe logique consiste à altérer graduellement un nombre limité d'enregistrements d'une grande base de données. Lorsque le problème est découvert, parfois au terme de

nombreux mois, il y a fort à parier que l'entreprise ne disposera plus d'aucune copie de sauvegarde fiable et devra procéder à un contrôle exhaustif et coûteux de l'entièreté de la base de données ;

- les virus et vers, fortement médiatisés, qui agissent comme des bombes logiques mais qui ont, en outre, la faculté de se reproduire et faire perdurer les infections. L'Internet et le courrier électronique leur ont fourni des voies royales de propagation ;
- les logiciels espions (« spyware »). Lorsqu'un utilisateur consulte licitement des sites Internet, il peut lire une page intéressante, mais qui cache des parties malveillantes permettant à ces dangereux logiciels espions de s'installer dans le poste de travail et de migrer sur le réseau interne tout en communiquant des informations-clés vers l'extérieur. Techniquement, ces pages dangereuses sont beaucoup plus difficiles à détecter que les virus dans les mails ;

Le recours intensif à l'Internet a fait apparaître de nouvelles formes d'actes malveillants, dont voici quelques exemples :

- le déni de service, qui se traduit par l'indisponibilité d'un site web. Il se provoque en inondant et en saturant le serveur ou le réseau par une masse énorme de messages rendant impossible l'accès normal aux ressources. Ces messages proviennent le plus souvent de réseaux de PC mal protégés, encore appelés « botnets ». Il s'agit de réseaux de PC « zombies », dont l'auteur malveillant a pris le contrôle. Ces réseaux peuvent comporter des dizaines de milliers de PC, appartenant bien souvent à des propriétaires, qui n'ont pas installé les mesures de sécurité élémentaires que sont des logiciels « firewall » et des logiciels anti-virus ;
- le remplacement de la page d'accueil d'un site web par un renvoi automatique sur le site d'un concurrent ou sur un site à caractère pornographique ;
- le renvoi de la page d'accueil vers celle d'un site qui y ressemble très fortement, mais qui est en fait celui d'une organisation malveillante, qui tentera ainsi de voler des données personnelles (données d'identité de l'utilisateur, données relatives à des comptes bancaires ou à des cartes de crédit, mots de passe, etc.) ;
- la modification des prix du catalogue d'une entreprise de vente exclusivement par Internet ;
- la modification de l'adresse e-mail pour les commandes sur Internet et son remplacement par l'adresse du concurrent ;

- le dépôt, dans la boîte d'envoi du système de messagerie d'un service Relations publiques d'un message annonçant l'ouverture d'une instruction judiciaire à l'encontre de l'entreprise. Le message devait être envoyé aux agences de presse ;
- le blocage du central téléphonique (ordinateur) empêchant toutes les communications téléphoniques intérieures et extérieures. Les techniques de téléphonie par Internet (VoIP) devront faire l'objet de mesures de protection adéquates ;

1.2.2.4.4. Les risques liés aux indiscrétions, détournements d'informations

II s'agit d'actes qui ont pour effet que des personnes non autorisées ont accès aux informations maintenues par le système informatique. Ces informations peuvent être des données ou des programmes (correspondances, contrats, secrets industriels, plans commerciaux, calculs de prix de revient, offres, données personnelles, financières, médicales, …). Au fur et à mesure que des données de plus en plus confidentielles sont confiées à des ordinateurs, ceux-ci deviennent les cibles privilégiées de cette forme actuelle d'espionnage industriel.

Les systèmes-experts font l'objet d'une convoitise particulière car ils contiennent une part essentielle du savoir-faire et de la politique suivie par une organisation.

Ces accès non autorisés aux données confidentielles de l'entreprise peuvent être perpétrés par des tiers qui font une intrusion dans le réseau de l'entreprise. Toutefois, le propre personnel de l'entreprise est souvent à l'origine de ces méfaits. Il devient courant qu'un employé quitte une entreprise pour se faire engager par un concurrent ou pour démarrer une activité concurrente, non sans avoir pris soin de copier les fichiers essentiels qui lui procureront un avantage concurrentiel et déloyal. La multiplication de supports amovibles de petite taille mais de grande capacité de stockage, tels que les sticks mémoire ou les disques portables à interface USB, a grandement facilité la mise en œuvre de ces actes de copiage. Parfois, les fichiers sont même exportés en annexe à des courriers électroniques transmis par le propre système de messagerie de l'entreprise victime.

1.2.2.4.5. Les risques liés aux détournements de logiciels

La copie de logiciels pour PC est une activité qui bat toujours son plein nonobstant les succès récents de poursuites judiciaires engagées contre les pirates et la diminution de l'attrait du copiage résultant des baisses de prix consenties par les éditeurs de logiciels.

La responsabilité de l'entreprise est engagée si elle permet le copiage ou l'utilisation de logiciels copiés et ce, en vertu de la loi sur les droits d'auteur des programmes du 30 juin 1994.

Les conséquences pour les entreprises prises en flagrant délit de détention de programmes illicites sont lourdes. Elles devront en effet s'acquitter de :

- l'acquisition des licences manquantes ;
- le paiement d'indemnités pouvant s'élever à 200 % du prix des licences ;
- le défraiement des frais de la procédure (frais de justice, d'huissier, d'expert judiciaire, etc.) ;

1.2.3. Gestion des risques opérationnels

Alain Desroches, Alain Leroy, Frédérique Vallée dans leur ouvrage La gestion des risques Principes et pratiques nous décrit les différentes étapes pour une bonne identification et un meilleur suivi des risques.

La définition et l'identification des risques opérationnels doivent être suivies d'une gestion de ces derniers.

1.2.3.1. Définition de la gestion des risques

Les mesures de sécurité informatique se construisent au départ d'une gestion des risques, pour laquelle il existe plusieurs approches possibles. Elles se résument toutes à quelques aspects essentiels.

Un risque est la potentialité d'une menace donnée d'exploiter une vulnérabilité d'une entité et donc d'occasionner un dommage à l'entreprise.

La gestion des risques consiste :

- à identifier les risques (menaces, potentialité, probabilité de survenance) ;
- à les évaluer selon des critères propres à chaque entreprise, tenant compte tant des faiblesses des protections (exposition aux risques, vulnérabilités) ainsi que des conséquences potentielles pour l'entreprise (impact, enjeu) ;

Cet examen tiendra compte de la capacité de l'entreprise à réagir en cas d'impact, capacité qu'il faudra qualifier avec la plus grande objectivité.

Il faut ensuite définir les moyens de protection adéquats, modulés selon une analyse coûts/bénéfices. Certains risques peuvent être transférés en les couvrant par exemple par des assurances ou en sous-traitant certaines applications.

En toutes circonstances, il est essentiel que toutes les parties concernées par les risques contribuent activement à l'évaluation de ces derniers, notamment par l'identification des menaces potentielles ou en évaluant les conséquences possibles. En particulier, chaque constat de faiblesse en sécurité informatique doit être signalé en vue de l'étudier de manière adéquate et de prendre les éventuelles mesures nécessaires.

La gestion des risques doit être un processus permanent. La réévaluation des risques doit intervenir en temps opportun : de manière périodique ou lors d'événements tels que le lancement d'une nouvelle application, la modification dans la configuration des réseaux, la réorganisation d'un département, la mutation de responsables, etc. Tout ceci va donc requérir une méthode de « gestion du changement » adéquate.

1.2.3.2. Risques majeurs et risques mineurs

Le risque informatique n'est qu'un des nombreux dangers que court l'entreprise. Aussi, il doit être maîtrisé et géré comme ces autres risques par une approche méthodologique rigoureuse. Des mesures adéquates et cohérentes doivent être prises

Un arbitrage doit être fait entre les conséquences financières des sinistres et le montant des investissements de sécurité à consentir. La sous-sécurité est dangereuse. La sur-sécurité est un gaspillage.

Une saine gestion des risques implique que l'on établisse la distinction entre risques majeurs et mineurs.

Les **risques majeurs** sont des risques de vie ou de mort pour l'organisation. Ils ont généralement un taux de fréquence extrêmement bas mais leurs conséquences sont catastrophiques. S'ils se matérialisent, l'entreprise ne survivra pas car les conséquences dépassent sa capacité financière ou sont telles que l'entreprise n'atteindra plus ses objectifs

généraux. Ils sont totalement INACCEPTABLES. L'assurance est inadéquate pour se protéger contre pareils risques. Plus de la moitié des entreprises dont les bâtiments ont été totalement détruits par un incendie n'existent plus trois ans après le sinistre. Elles sont tout simplement "out of business". Ceci n'est pas dû au fait qu'elles n'étaient pas ou mal assurées mais bien parce qu'elles ne disposaient pas d'un plan de survie. L'assureur donne une indemnisation mais il ne peut restituer à l'entreprise les données et programmes perdus. Que faire lorsque les programmes et données indispensables au fonctionnement de l'organisation ont été détruits ? Comment reconstituer la situation comptable, les fichiers clients, fournisseurs et articles, les prix de revient, les modèles ou gammes opératoires de la production, ...? Plusieurs entreprises belges ont perdu l'entièreté de leurs données, suite à la conjugaison de sinistres et de systèmes de sauvegarde de données défectueux à l'insu de leurs utilisateurs.

La seule réponse aux risques majeurs est la mise en œuvre d'un plan de survie, qui permettra à l'entreprise de restaurer, dans des délais acceptables, la situation qui prévalait avant le sinistre et de poursuivre ses activités. Ce plan doit être périodiquement testé pour valider son bon fonctionnement. L'expérience a montré que même dans des environnements où ces plans sont régulièrement testés, il subsiste toujours des imprévus et des difficultés lorsqu'il faut mettre le plan en exécution suite à un sinistre réel et non simulé.

Les **risques mineurs** ont le plus souvent une probabilité de survenance plus élevée mais leurs conséquences sont moindres et temporairement acceptables. Ces risques peuvent être traités par des mesures de prévention et le recours aux assurances. L'amortissement économique de ces mesures sera évalué par rapport à la probabilité et la gravité des sinistres. Les très nombreux incidents que l'on rencontre au quotidien sans même qu'ils ne soient répertoriés dans les statistiques vu leur fréquence élevée sont à ranger dans cette catégorie.

1.2.3.3. Le dispositif de maîtrise des risques opérationnels du réseau informatique

Les risques opérationnels du réseau informatique précédemment décrits doivent être maîtrisés à travers un dispositif.

1.2.3.3.1. Le dispositif de maîtrise des risques accidentels

Le dispositif de maîtrise des risques accidentels se fait à travers :

- une mise en place d'un système de redondance ;
- une sécurisation de la configuration informatique ;
- une mise en place d'un système d'accès performant.

1.2.3.3.2. Le dispositif de maîtrise des risques liés aux erreurs

Le dispositif de maîtrise des risques liés aux erreurs se fait à travers:

- des contrôles de robustesse (limite d'un champ de saisie évitant un débordement dans les champs suivants) ;
- des filets de sécurité (« une date d'expiration » qui suspend automatiquement un utilisateur dont le contrat se termine à une date précise) ;
- le recours à des systèmes automatisés de gestion des applications permet de réduire le rôle joué par les opérateurs humains et de faire baisser le nombre de ces erreurs ;
- l'application de méthodologies rigoureuses supportées par des outils performants et une approche systématique de contrôle de la qualité ;

1.2.3.3.3. Le dispositif de maîtrise des risques liés à la malveillance

Le dispositif de maîtrise des risques liés à la malveillance se fait à travers:

- mise en place d'un système d'antivol pour les ordinateurs portables et les serveurs ;
- acheter les matériels standards pour faciliter l'acquisition ;
- séparation de fonctions et de connaissances ;
- mise en place d'un système de double contrôle ;
- mise en place d'un système de filtrage et de pare feu ;
- mise en place des systèmes d'authentification en se basant sur les niveaux d'accès de chaque utilisateur ;
- mise en place d'un système de détection d'utilisation de licences frauduleuses ;

Conclusion

Le réseau informatique est donc sensible et nécessite une gestion efficace de ses risques. Une bonne gestion des risques est un gage de succès de performance pour l'entreprise, elle doit donc ainsi couvrir toute l'entreprise et être accompagnée d'un bon dispositif de maitrise des risques et une forte culture du risque.

Chapitre 2 : METHODOLOGIE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES

La transparence recherchée par les entreprises dans leur fonctionnement est due à la complexité et l'incertitude qui constituent les principales caractéristiques de l'environnement économique aujourd'hui. Ainsi plusieurs instruments et outils sont à la disposition des entreprises tout comme les réponses des pouvoirs publics (loi SCADA aux Etats Unis d'Amérique, la loi du 6/1/78 en France et la loi Computer Misuse Act 1990 en UK) pour une bonne et meilleure utilisation du réseau informatique.

Selon **JACOB & SARDI** (2001 : 221) le processus de management des risques comporte de nombreuses étapes. Nous pouvons citer entre autres :

- l'identification des risques ;
- l'évaluation ou quantification des risques ;
- la hiérarchisation des risques ;
- la mesure de contrôle des risques ;
- la surveillance et le reporting des risques.

La cartographie des risques constitue ainsi un instrument privilégié de ce dispositif car permettant d'exécuter les étapes d'un bon système de risk management, et puis les meilleures pratiques de maîtrise des risques recommandent son utilisation selon **MATTE** (2003 : 39). Comment élaborer une cartographie des risques ? Telle est la question à laquelle nous apporterons une réponse.

2.1. Notions sur la cartographie des risques

Tout au long de cette section nous procéderons à la définition de la cartographie des risques, ses objectifs, les acteurs concernés, les motivations conduisant à l'élaboration d'une cartographie des risques, les principaux facteurs de réussite contribuant à son succès, les facteurs internes de spécificité, et enfin les types de cartographie.

2.1.1. Définition, objectifs et acteurs de la cartographie des risques

Nous définissons la cartographie des risques selon les points de vue de différents auteurs, ensuite nous déclinerons les objectifs assignés à la cartographie des risques et nous terminerons en montrant les différents acteurs concernés par la cartographie des risques.

2.1.1.1. Définition de la cartographie des risques

Selon **l'IFACI** (in RENARD, 2005 : 221), « une cartographie des risques est une représentation graphique de la probabilité d'occurrence et de l'impact d'un ou de plusieurs risques. Les risques sont représentés de manière à identifier les plus significatifs (probabilité et/ou impact le plus élevé) et les moins significatifs (probabilité et/ou l'impact le plus faible) ». Selon l'objectif assigné, l'analyse est réalisée de manière plus ou moins détaillée et approfondie. La cartographie des risques peut soit représenter la probabilité ou l'impact global, soit intégrer un élément venant modifier la probabilité ou l'impact.

Pour **l'AMRAE** (2002 : 3) la cartographie des risques est un moyen permettant de classer, de comparer et de hiérarchiser les risques entre eux, et de mettre en place des plans d'action pour les traiter en fonction des ressources disponibles.

La cartographie des risques ou « risk mapping » n'est que le résultat du processus général de la gestion des risques. Cette cartographie, permet en fonction de l'évolution du contexte et des activités de l'entreprise, d'appliquer les actions de transformation du profil des risques qui s'imposent. Il s'agit également de pouvoir mesurer la performance de la gestion des risques et veiller au respect des attentes des parties prenantes en terme de profil de risque et des règles de gestion des risques. C'est aussi un outil, un moyen de suivi et de communication affinée (BAPST, 2002 : 4).

Selon SANIGO & al. (2001 :4), la cartographie des risques est un outil qui permet :

- de classer, de comparer, de hiérarchiser les risques entre eux ;
- de mettre en place des plans d'action pour les gérer en fonction des ressources disponibles ;
- d'en assurer le suivi ;
- de communiquer les informations sur les risques dans l'organisation.

Pour POULIOT (2002 : 37) la cartographie des risques est un outil de gestion des ressources humaines, financières, matérielles puisqu'elle permet l'affectation des ressources aux risques prioritaires et susceptibles d'empêcher l'atteinte des objectifs.

D'après INGRAM (2004 : 1), la cartographie des risques peut être la première étape du processus de management des risques pour une entreprise n'ayant pas de culture d'entreprise Risk Management.

Et enfin pour MOREAU (2002 : 162) et MATTE (2003 : 39), la cartographie des risques, de la même manière que les états financiers présentent l'image fidèle d'une entité, présente les risques d'une organisation.

La synthèse des définitions des différents auteurs fait de la cartographie des risques un outil d'aide à la décision permettant :

- l'identification et la hiérarchisation des risques, point de départ de toute cartographie ;
- le choix de deux axes (probabilité et gravité ou impact) en vue d'une représentation graphique des risques ;
- la mise en place de plans en vue de la maîtrise de ces risques et/ou de la réduction de leurs impacts ;

2.1.1.2. Objectifs de la cartographie des risques

La clarté des objectifs constitue un élément essentiel de la gestion du profil de risque dans l'entreprise et est par conséquent nécessaire dans l'élaboration d'une cartographie des risques. Véritable inventaire des risques de l'organisation, la cartographie des risques permet d'atteindre les objectifs suivants (RENARD, 2008 : 140-141 ; BERGERET, 2002 : 32 ; LECLERC & al, 2003 : 6) :

- inventorier, évaluer et classer les risques de l'entreprise ;
- informer les responsables afin que chacun soit en mesure d'adapter le management de ses activités ;
- permettre à la Direction Générale, et avec l'assistance du Risk Manager d'élaborer une politique de risque qui va s'imposer à tous ;
- l'établissement du plan d'audit : la norme 2010 d'audit interne (in RENARD, 2008 : 217) exige au département d'audit interne d'établir un planning de ses interventions ; la cartographie des risques sert ainsi de base à la programmation des missions qui tient compte de l'identification des zones à risques et des domaines prioritaires ;
- l'établissement de plan d'action de gestion : évaluation de l'impact final des décisions d'action, formalisation des actions sur une fiche d'action, document qui trace le type

d'actions correspondant à quelques risques : qui prend la responsabilité ? quand cette action doit être entreprise ? Une fois les risques majeurs déterminés dans l'entreprise, il revient aux responsables la charge de définir la stratégie en vue de les prévenir ou de les atténuer ;

- répondre aux dispositions réglementaires ;

Les objectifs définis, nous allons voir par la suite quels sont les acteurs à qui s'adresse la cartographie des risques.

2.1.1.3. Les acteurs de la cartographie des risques

L'élaboration d'une cartographie des risques fait intervenir tous les agents de l'organisation mais à des degrés différents. Selon RENARD (2008 : 139-140), les acteurs les plus impliqués sont :

- le risk manager : il identifie les risques, en dessine la cartographie, les mesure et, à partir de là, définit la politique qui sera appliquée dans le double domaine de la prévention et de la protection ;
- le management opérationnel : il applique cette politique et met en place les moyens pour maîtriser les risques inacceptables et limiter les risques acceptables (contrôle interne) ;
- l'auditeur interne : il apprécie la qualité de la cartographie et les moyens mis en place, il en détecte les lacunes et les insuffisances et formule des recommandations pour y mettre fin ;

A ces acteurs identifiés par RENARD il convient d'ajouter la participation de la Direction Générale qui définit les objectifs de l'organisation, les politiques et les moyens à mettre œuvre pour les atteindre. Ces acteurs pourraient se faire aider par un cabinet de consultants ou expert thématique plus spécialisé.

Les acteurs de la cartographie des risques définis, le paragraphe suivant sera consacré aux motivations à l'élaboration d'une cartographie des risques.

2.1.2. Les motivations d'élaboration d'une cartographie des risques

Plusieurs facteurs peuvent conduire une entreprise à envisager l'élaboration d'une cartographie des risques, qui est un outil de pilotage de gestion des risques. Différents éléments peuvent conduire à l'élaboration d'une cartographie des risques.

Selon BELLUZ (2002 : 2), DE MARESCHALL (2003 : 34), DESCAPENTRIES & BAPST (2003 : 2), ce sont :

- le référentiel d'analyse : la cartographie des risques permet aux dirigeants de l'entreprise de savoir quelle démarche adopter et d'avoir un référentiel en matière de risques ;
- la communication : la cartographie des risques permet d'améliorer la communication sur les risques au sein de l'organisation et notamment à destination de la Direction Générale ;
- les évènements de la restructuration de l'entité : la gestion des risques permet de minimiser les pertes et d'augmenter les effets positifs des décisions lors des restructurations. La cartographie des risques aidera, dans ce cas, les acteurs dans leur prise de décision ;
- les pressions internes et externes : les pressions externes sont assurées en majeure partie par la bonne gouvernance qui nécessite la mise en place de système de contrôle et de contre pouvoir au sein des sociétés afin d'assurer en toute transparence la qualité de pilotage et de gestion des entreprises ; tandis que les pressions internes se résument à la qualité de l'information et du reporting ;
- l'effet de la mode : la mise en pratique d'outil performant et récent montre que l'entreprise est en phase avec l'évolution, s'adapte et est informée des meilleures pratiques ;

2.1.3. Les facteurs clés de succès de la cartographie des risques

Le type d'organisation influe sur les critères de réussite d'une cartographie des risques. Toutefois, un certain nombre de facteurs généralisables peut être dégagé selon les auteurs suivants : MOREAU (2003 : 134) ; DE MARESCHAL (2003 : 44) ; RENARD (2003 : 100) ; BAPST (2004 : 9) ; IFACI (2005 : 160). Il s'agit de :

- une définition claire, précise et partagée par les intervenants des objectifs de l'organisation, détermine l'approche utilisée, permet de savoir ce que l'on recherche et doit être comprise par l'équipe afin d'avoir une vision cohérente de la démarche à adopter ;
- un sponsor (de préférence membre de la Direction Générale), et des alliés pour réaliser une phase pilote ;
- la désignation d'un responsable selon l'entreprise, il peut être un risk manager, un responsable de l'audit interne ou une personne émanant de la direction ;
- un soutien motivé et une implication de la part de la Direction Générale. Il est fondamental que les membres s'impliquent et que les opérationnels se sentent obligés d'y participer. En tant qu'axe stratégique la Direction Générale a une obligation d'appropriation des outils ;
- une méthode robuste et simple ;
- la mesure du coûts/temps à passer par les opérationnels : besoin d'optimiser l'organisation, planning et méthodologie du risk mapping ;
- la mise en place d'une équipe de qualité : il faut y retrouver aussi bien les opérationnels susceptibles de connaitre les risques que les spécialistes outillés dans le domaine. L'équipe sera chargée de piloter et de coordonner la démarche de la cartographie des risques, mais aussi l'intervention d'un cabinet de conseil peut être d'une grande utilité afin de faciliter les décisions (FONTUGNE et al. 2001 : 9);
- les moyens : toutes ces décisions n'auront aucun sens si les moyens adéquats ne sont pas réunis. Les ressources suffisantes pour un bouclage rapide, la mise à disposition d'un capital humain compétent et expérimenté est nécessaire en plus des fonds suffisants pour sa réalisation.

Les démarches conduisant à l'élaboration d'une cartographie des risques diffèrent d'une organisation à une autre. Les risques identifiés diffèrent d'une entité à une autre (BAPST, 2003 : 2), ainsi chaque organisation à sa propre cartographie (BELLUZ, 2002 : 4). Ceci nous amène à présenter les différents types de cartographie des risques qui pourraient être envisagés dans une organisation.

2.1.4. Les types de cartographie des risques

Le type de cartographie du risque à mettre en œuvre dans une organisation est fonction du risque étudié. Selon DE MARESCHALL (2003 : 17), deux grandes options peuvent être envisagées :

- la cartographie globale ou l'étude de l'ensemble des risques qui menacent l'organisation concernée ;
- la cartographie thématique ou l'étude des risques spécifiques liés à un domaine particulier.

2.1.4.1. La cartographie globale

La cartographie globale vise à recenser l'ensemble des risques qui pèsent sur une entité (service, entreprise, groupe). Cette démarche permet, pour une entité, de réunir et surtout de hiérarchiser et de comparer des risques très différents les uns des autres, dans une perspective de bonne gouvernance (DE MARESCHAL, 2003 : 23).

2.1.4.2. La cartographie thématique

Pour DE MARESCHALL (2003 : 23), la cartographie thématique s'attache à recenser et hiérarchiser les risques liés à un thème précis. Son principal intérêt est de pouvoir réunir et comparer sur un même thème factuel :

- soit différentes organisations pour un même type de risques ;
- soit différents domaines de risques liés au thème étudié pour une même organisation.

L'accent sera mis sur ce deuxième type de cartographie car nous intéressant le plus. Ce type de cartographie peut se présenter sous la forme d'un polygone, d'un spectre, d'une matrice ou tout simplement d'un tableau. De manière standard, les risques sont représentés selon deux composantes : la fréquence (probabilité) et la gravité.

2.1.5. Démarche d'élaboration d'une cartographie des risques

Le choix des méthodes et d'outils nécessaires à la mise en place d'une cartographie des risques demeure une épreuve difficile, car la cartographie des risques est propre à chaque entreprise et dépend du cycle de management mis en œuvre dans l'entreprise.

La diversité des domaines explorés qui vont de l'entreprise, du niveau local au niveau global, nécessite des approches d'élaboration de la cartographie des risques différentes. Pour RENARD (2002 : 100) et LECLERC & al. (2003 : 6), il existe trois démarches à savoir le bottom up, le top down et l'approche combinée. Pour l'AMRAE (2002 : 4), cinq autres méthodes s'ajoutent aux trois précitées qui sont : l'approche par le benchmarking, l'approche par l'auto-évaluation, l'approche par analyse et synthèse rationnelle des risques, les points d'entrée et la macro cartographie. La synthèse de ces différents auteurs permet d'avoir huit approches qui sont : le bottom up, le top down, l'approche combinée, l'approche par le benchmarking, l'approche par l'auto-évaluation, l'approche par analyse et synthèse rationnelle des risques, les points d'entrée et la macro cartographie.

2.1.5.1. Le bottom up

L'identification des risques est effectuée de manière relativement libre et ouverte par les personnes les plus proches possibles de l'activité. Il s'agit d'effectuer une remontée des risques du terrain aux personnes en charge de l'élaboration de la cartographie. Ce type d'identification se fait généralement par l'intermédiaire d'interview. Selon DE MARESCHAL (2003 : 15), le bottom up est une approche utilisée pour une démarche de cartographie globale.

2.1.5.2. Le top down

Selon MANIVIT (2002 :4), l'approche « top down » s'appuie sur les pertes historiques, lesquelles constituent une bonne mesure des pertes futures. L'identification des risques est dans ce cas effectuée de manière plus fermée, c'est-à-dire à l'aide d'un questionnaire à choix multiples. Souvent utilisée pour une démarche de cartographie thématique, elle peut se faire par questionnaire. En effet, le sujet ciblé peut permettre l'élaboration de questionnaires relativement exhaustifs par les personnes en charge de la cartographie. Ce processus permet donc de descendre chercher l'information (DE MARESCHAL, 2003 : 16).

2.1.5.3. L'approche combinée

Dans cette démarche les risques sont identifiés tant par la hiérarchie que par les opérationnels. Les approches bottom up et top down deviennent particulièrement complémentaires pour assurer une mesure pragmatique des risques opérationnels. Pour RENARD (2003 : 101), la meilleure méthode est celle qui concilie les deux approches et qui consiste pour chaque

responsable de se faire assister soit par le risk manager soit par l'audit interne dans la définition des risques de son activité.

2.1.5.4. L'approche par le benchmarking

Elle consiste à mener une campagne de collecte des meilleures pratiques en matière de gestion des risques. Elle permet de se faire une idée générale quant aux risques à prendre en compte et la façon de les considérer.

2.1.5.5. L'approche par l'autoévaluation

La mise en œuvre de cette approche consiste à confier la responsabilité du contrôle interne aux opérationnels en les chargeant de l'autoévaluation de la qualité du dispositif de contrôle interne mis en place. Selon COLATRELLA (2006 : 7), la valeur ajoutée de l'autoévaluation est, en terme de contrôle interne, l'appropriation de la démarche de contrôle interne par les opérationnels.

2.1.5.6. L'approche par analyse et synthèse rationnelle des risques

Elle consiste à partir de l'existant et des données chiffrées de chercher les meilleures pratiques (benchmarking), et à faire des comparaisons (DHERS & al, 2004 : 11).

2.1.5.7. Les points d'entrée

Cette approche consiste à l'analyse des objectifs de l'entreprise, des pôles de valeur et des différents processus (DHERS & al, 2004 : 11).

2.1.5.8. La macro cartographie

Elle est effectuée à l'échelle de l'entreprise et tend à recenser, quantifier et cartographier l'ensemble des risques d'une organisation, tous sujets confondus.

2.2. Les différentes étapes d'élaboration d'une cartographie des risques

La présentation de la synthèse des points de vue et des démarches proposés par différents auteurs permettra à travers une synthèse de bâtir notre propre démarche référentielle. Ainsi nous avons choisi un échantillon de cinq auteurs (FONTUGNE, BELLUZ, ERNST & YOUNG, KPMG France, RENARD) dans divers domaines et nous présenterons la synthèse sous la forme du tableau suivant.

Tableau 1 : Synthèse des idées de différents auteurs

Auteurs / Phases	Etapes	FONTUGNE (2001 :1-19)	BELLUZ (2002 :1)	ERNST & YOUNG (2004 : 12)	KPMG France (2006 : 1)	RENARD (2008 : 141-143)
Cadre	Analyse du contexte	✓				
Préparation	Conception et mise en place de la démarche					✓
Planification	Identification et analyse des risques	✓	✓	✓	✓	✓
	Evaluation des risques	✓	✓	✓	✓	✓
	Hiérarchisation et mesure des risques	✓	✓	✓	✓	✓
	Identification et évaluation du contrôle interne	✓	✓			✓
	Matrice des risques (cartographie)	✓	✓	✓	✓	✓
Action	Etablissement des plans d'actions	✓	✓	✓		✓
Reporting	Reporting sur les risques résiduels	✓		✓		
Suivi évaluation	Vérification de l'efficacité du plan d'action		✓		✓	
Actualisation	Amélioration et mise à jour de la démarche				✓	

Source : A partir des travaux des auteurs sus mentionnés

2.3. Analyse du tableau de synthèse

Nous analyserons le tableau en indiquant les différentes phases et étapes

2.3.1. Cadre méthodologique

L'analyse du contexte de l'étude est le principal élément constitutif de cette phase. Elle consiste à mettre en valeur les points forts et faibles ainsi que les menaces et opportunités de l'environnement interne et externe, et des objectifs stratégiques. Elle est orientée par un business plan lorsque celui-ci existe. Pour FONTUGNE (2001 : 6), il est primordial de définir les indicateurs de création de richesse, à savoir la croissance, l'efficacité et les variables externes dans le cadre de référence. Le succès des autres phases dépend de la réussite de celle-ci.

2.3.2. La phase de préparation

Pour RENARD (2006 : 217), cette phase nécessite une bonne compréhension de l'entité car il faut savoir où trouver la bonne information et à qui la demander. Les travaux préparatoires ainsi que la conception et la mise en place des fondements de la démarche sont réalisés au cours de cette phase avant de passer à l'action. Le risk manager doit faire preuve de qualité de synthèse et d'imagination.

2.3.3. La phase de planification

Elle est la phase la plus importante d'où son apparition chez les différents auteurs. Elle permet aux dirigeants de prendre des décisions en matière de gestion des risques et également prendre en compte les priorités du management. Cette phase se déroule en plusieurs étapes à savoir :

- identification et analyse des risques ;
- évaluation des risques ;
- hiérarchisation et mesure des risques ;
- identification et évaluation du contrôle interne existant ;
- matrice des risques.

2.3.3.1. Identification et analyse des risques

Cette phase permet de lister l'ensemble des risques inhérents qui pèsent sur l'organisation et identifier les zones où les risques préjudiciables sont susceptibles de se produire. Elle

constitue une phase primordiale à tout processus d'élaboration de la cartographie des risques. L'entreprise doit avoir des compétences spécifiques et une bonne compréhension des activités. La méthodologie d'identification des risques inclue une combinaison de techniques et d'outils. Nous exposerons les techniques tandis que les outils feront l'objet du chapitre suivant. Selon OHANESSIAN (2004 :27), l'identification des risques requière une connaissance appropriée et une compréhension des activités de l'entreprise.

Les techniques d'identification des risques se présentent ainsi :

- exposure analysis ou identification des risques qui affectent les actifs. Elle consiste à la mise en évidence des risques qui pèsent sur les actifs constitutifs de la valeur de l'entreprise. Ce sont les risques qui pèsent sur les biens (MC NAMEE, 1998 : 13) ;
- the environmental analysis ou identification des risques qui affectent les opérations. C'est une technique dans laquelle la détermination des risques se fait en fonction des variétés que peut subir l'environnement dans lequel se trouve l'entreprise. (MC NAMEE, 1998 : 13) ;
- threat scenarios ou identification basée sur les scénarios, qui consistent à mener des enquêtes systématiques auprès d'experts de chaque ligne de métier et de spécialistes de gestion des risques. (MC NAMEE, 1998 : 13) ;
- identification par l'analyse historique : cette approche consiste à remonter les risques qui ont menacé le domaine à l'étude, par le passé, et d'en tenir compte lors de la mise à jour de la conception de la carte des risques (MC NAMEE, 1998 : 13) ;
- identification basée sur l'atteinte des objectifs : elle consiste à identifier d'abord les objectifs de l'activité ou de l'organisation pour ensuite leur affecter la menace correspondante. L'efficacité de cette approche repose sur une identification claire et partagée des objectifs en amont. Cependant, cette identification est un exercice assez complexe (BAPST, 2003 : 3) ;
- identification par les tâches élémentaires : c'est une démarche que l'auditeur connait bien. C'est elle qu'il utilise pour construire son questionnaire de contrôle interne selon RENARD (2005 : 184) ;
- identification basée sur les check-lists : elle consiste à lister l'ensemble des risques possibles en se basant sur les activités ou les évènements. Elle permet de s'assurer qu'aucun risque n'a été omis et complète les autres techniques. Elle doit être utilisée avec discernement (ROUFF, 2001 : 14) .

L'identification des risques terminée, il va falloir évaluer les risques afin de maintenir un degré acceptable de ces derniers.

2.3.3.2. Evaluation des risques

De part leur activité les entreprises sont confrontées à un ensemble de risques qui peuvent être soient internes, soient externes. Ces risques doivent être évalués en vue de déterminer de quelle manière ils seront gérés afin d'amoindrir leur impact sur l'atteinte des objectifs préalablement définis par l'organisation. L'évaluation se fait à deux niveaux : d'abord au niveau du risque brut sans tenir compte du dispositif de contrôle interne puis au regard de la façon dont le contrôle interne va atténuer le risque de l'entreprise. Cela présuppose que le risque ait déjà été identifié dans l'entreprise et qu'il soit déjà géré.

Compte tenu de l'évolution permanente de l'environnement micro et macro économique du contexte réglementaire et des conditions d'exploitation, il convient d'évaluer et de maîtriser les risques spécifiques liés au changement. La méthodologie d'évaluation des risques d'une entité s'appuie sur un ensemble de techniques quantitatives et qualitatives (IFACI in COSO 2, 2006 : 78)

- **La méthode quantitative**

Selon l'IFACI (in COSO 2, 2006 : 78), les techniques quantitatives sont habituellement plus précises et sont utilisées dans des activités plus complexes afin d'apporter un complément aux techniques qualitatives. Cette méthode traite de la probabilité d'occurrence et de la mesure de la gravité des risques caractérisant un évènement redouté. La diversité des risques rend cette méthode un peu difficile or tous les risques ne sont pas évalués sur un impact financier. Selon BERGERET (2002 : 11), il existe des risques, comme les risques intangibles ou immatériels, pour lesquels il est extrêmement difficile d'avoir une idée de l'impact financier, mais la démarche permet de réfléchir sur l'impact que pourrait avoir le risque s'il venait à se réaliser. Leur but est de :

- hiérarchiser les risques ;
- évaluer le niveau de sécurité du système ou du sous système dans la phase considérée ;
- construire la sécurité du système de façon efficace et cohérente (DESROCHES & al, 2003 : 59).

La collecte de données objectives et inhérentes à chaque processus, provenant de sources diverses, est nécessaire pour la mise en œuvre de cette méthode. La complexité de cette méthode est due à la diversité des risques, en effet tous ne peuvent être appréciés sur une échelle commune. Sur chaque période des coefficients sont calculés et combinés aux tendances des risques afin d'obtenir un indicateur statistique final pour chaque catégorie de risque.

Après pondération, ces indicateurs sont eux-mêmes regroupés pour donner un facteur de risque quantitatif global unique ; selon COLATRELLA (2006 : 6), il existe une méthode d'évaluation selon deux critères : d'une part, la probabilité de survenance et d'autre part, la gravité ou impact financier. La probabilité peut résulter d'une estimation de la loi statistique ou d'une modélisation plus complexe fondée sur une description des processus représentée par un graphique (BARROIN & al, 2002 : 2). Cette méthode est utilisée par les actuaires et demeure compliquée pour les auditeurs qui, selon RENARD (2002 : 10), n'ont pas à rentrer dans les calculs de savants. Ce qui explique, selon lui, un recours inéluctable aux méthodes qualitatives.

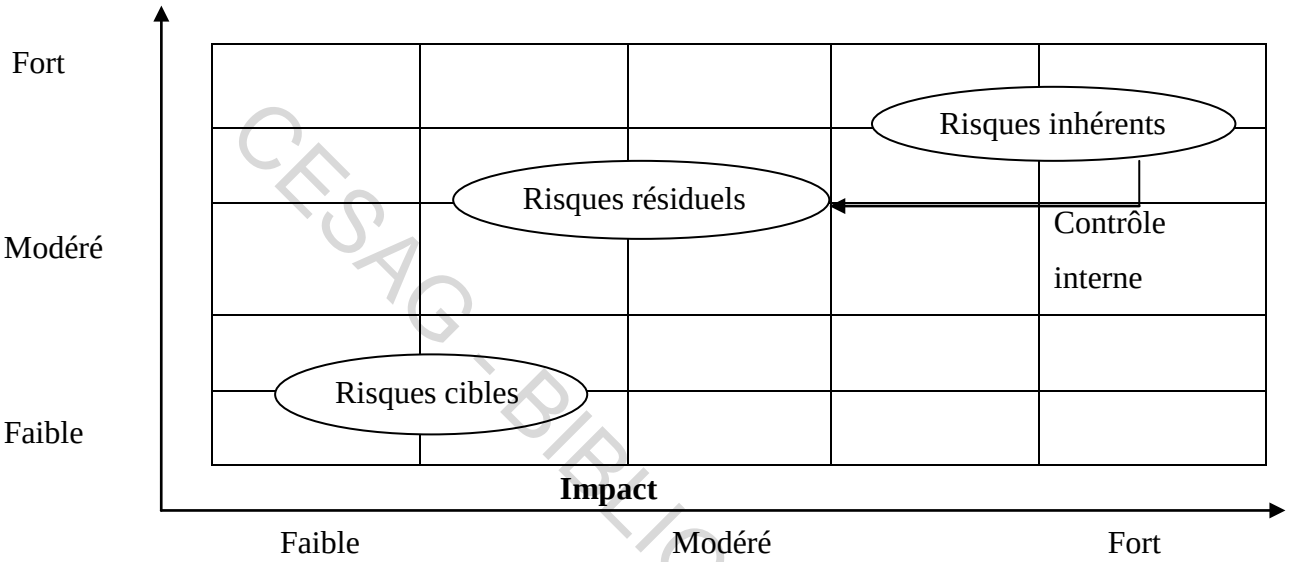
- **La méthode qualitative**

Les techniques qualitatives sont utilisées très souvent lorsque les risques n'offrent pas de possibilité de quantification ou lorsqu'il n'existe pas suffisamment de données fiables donnant droit à une évaluation quantitative ou encore le coût de collecte et d'analyse de ces données s'avère très élevé. L'évaluation qualitative est inversement liée à la qualité du contrôle interne. Pour COOPERS & al. (2000 : 61), des appréciations du type « faible », « moyen » et « élevé » sont attribuées aux risques. Selon OHANASSIAN (2006 : 17), ces appréciations sont établies, pour ce qui est de la probabilité, au regard des forces et faiblesses potentielles de l'organisation. Son but consiste à identifier :

- les évènements à risque apparaissant suite à la défaillance d'éléments du système ;
- les causes des évènements ;
- les conséquences des évènements sur le système à travers des scénarios ;
- les actions en diminution des risques qui peuvent être prises (DESROCHES & al, 2003 : 58) ;

L'évaluation impact probabilité, qui peut être réalisé en deux temps, découle du poids du risque. L'évaluation du risque inhérent avant la mise en place du dispositif de contrôle interne est opérée dans un premier temps avant de procéder à celle de l'efficacité du contrôle interne, autrement dit la manière dont ce contrôle interne va transformer le risque inhérent en risque résiduel (voir la matrice ci-dessus).

Figure 9 : Matrice d'évaluation des risques



Source : Nous même adopté de FONTUGNE (2001 : 10)

Dans un second temps on procède à la quantification des risques associés à chaque évènement redouté susceptible de freiner l'entreprise dans l'atteinte de ses objectifs. Ce qui permet de les classer en fonction de leur acceptabilité, c'est-à-dire cibler ceux qui méritent une attention particulière ou dont la priorité est moindre. L'élaboration d'une matrice de risque est utile pour mesurer le risque posé par divers dangers.

2.3.3.3. Hiérarchisation et mesure des risques

A ce niveau, il s'agit de procéder à la hiérarchisation et à la mesure des risques.

- **Hiérarchisation des risques**

La quantification des risques associés à chaque évènement redouté susceptible de freiner l'entreprise dans l'atteinte de ses objectifs, permet de les hiérarchiser en fonction de leur acceptabilité.

MCNAMEE (1998 : 13) classe les risques selon :

- the absolute ranking ou classement des risqué en fonction du score;
- the relative ranking ou classement des risques suivant trois niveaux : faible, moyen, élevé ;
- the matrice ranking ou regroupement des risques suivants les opérations dans une matrice en leur attribuant des appréciations faible, moyen ou élevé ;

Le classement des risques en fonction de leur score est obtenu par la combinaison de tous les paramètres. Cette hiérarchisation est obtenue par le biais des échelles définies à l'étape précédente, c'est-à-dire au niveau de l'évaluation tout en faisant attention au seuil de tolérance aux risques de l'organisation ainsi que le risque intrinsèque (WALKER & al, 2003 : 3 ; RENARD, 2004 : 150). Elle doit en effet, être affinée par l'appréciation des contrôles internes ayant déjà été mis en œuvre pour la réduction des effets de ces différents risques.

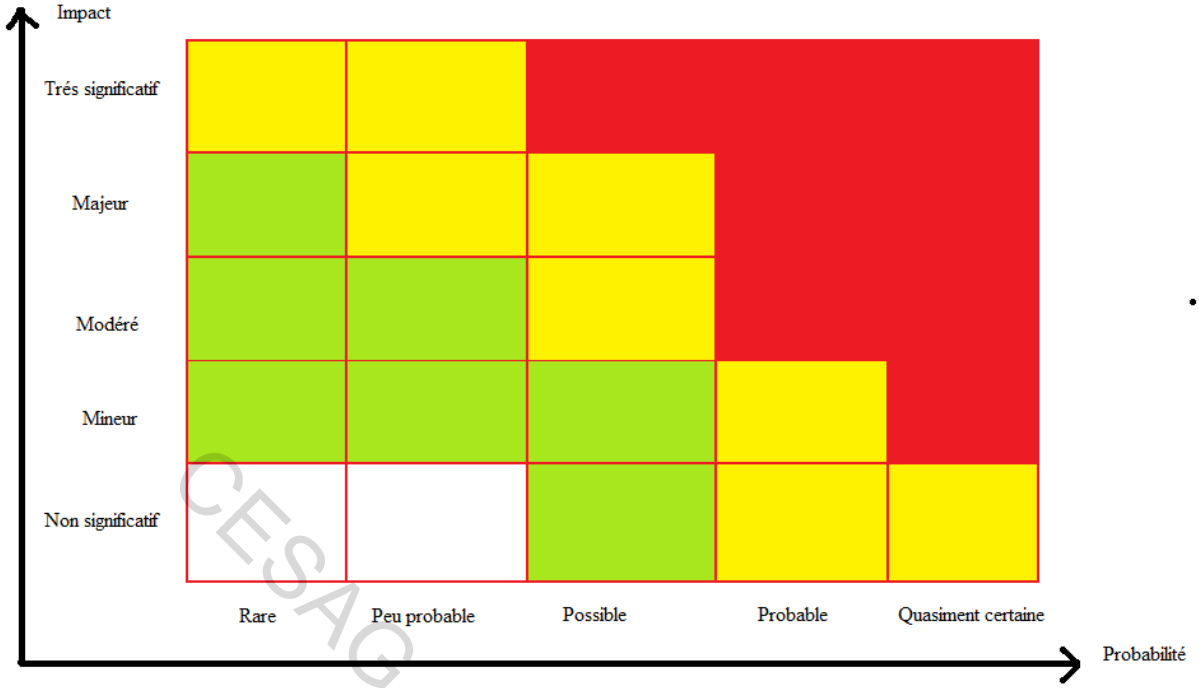
- **Mesure des risques**

Le management, une fois les risques évalués, doit déterminer quel traitement appliquer à chacun de ces risques. Selon BODINE (2001 : 5) et WALKER & al. (2003 : 5), les solutions possibles peuvent être envisagées :

- soit l'évitement signifiant « cesser les activités à l'origine du risque ». Eviter le risque au cas où le risque ne s'est pas encore matérialisé, sinon éliminer complètement le risque par des actions correctives ;
- soit la réduction, c'est-à -dire prendre des mesures afin de réduire la probabilité d'occurrence ou l'impact du risque, ou les deux à la fois ;
- soit le partage, autrement dit diminuer la probabilité ou l'impact du risque en transformant ou en partageant le risque ;
- soit l'acceptation du risque, ne prendre aucune mesure pour modifier la probabilité d'occurrence du risque et de son impact. L'acceptation laisse à penser que le risque inhérent se situe dans la fourchette de tolérance au risque

Le risque est classiquement évalué sous la forme d'une combinaison des facteurs de probabilité et de gravité (DE MARESCHALL, 2003 : 9). D'où **Risque = Probabilité (f) * Gravité (g)**.

Figure 10 : Hiérarchisation des risques opérationnels



Source : KPMG France (2005 : 1)

L'espérance mathématique de la gravité est donnée par le produit f*g. c'est un indicateur de l'acuité du risque aussi appelé criticité. Dans la démarche quantitative la criticité du risque est obtenue par le produit de sa probabilité et de son impact soit : **Criticité = Impact * probabilité**

❖ **Identification et évaluation du contrôle interne existant**

L'identification du contrôle interne existant au sein d'une entité revient à relever tous les contrôles possibles avant l'élaboration de la cartographie. Il s'agit d'évaluer la manière par laquelle les éléments, les concepts et principes de management des risques sont appliqués à l'échelle de l'entreprise et d'avoir une liste exhaustive des contrôles. Pour cela le travail se concentre sur les préventions, les détections ou corrections, les couvertures des risques bruts, leur mode de fonctionnement, les responsables en charge de leur application et de leur suivi, les indicateurs de performance et les facteurs clés de succès. La gestion des risques évalués par l'élaboration et la mise en œuvre de mesures propres à améliorer les systèmes de contrôle interne, permettra d'atténuer et d'éliminer les risques, et de tirer parti des opportunités.

La complexité réside dans le fait de rapprocher ce qui est fait et ce qui doit être fait c'est-à-dire évaluer le contrôle interne. Malgré la multitude de critères proposés par les auteurs pour

l'évaluation du contrôle interne, tous sont unanimes sur la pertinence de l'utilisation de la méthode qualitative. Selon BELLUZ (2002 :1) et FONTUGNE (2001 : 12), les critères retenus sont l'efficacité, la fiabilité, la qualité de la conception et la mise en œuvre. Le contrôle interne est évalué sur une échelle allant de 1 (inexistant) à 5 (efficace) et entre ces deux extrêmes nous avons l'échelle 3 (acceptable).

- **Matrice des risques**

C'est la représentation des risques et de leurs causes sous la forme d'un tableau. Les risques sont représentés en fonction de leurs niveaux, de leurs catégories et de leurs domaines d'influence. Cette matrice ne constitue que la représentation de la hiérarchisation des risques résiduels. En fonction des zones à risques, elle revêt des choix à opérer en matière de gestion des risques. La matrice étant une fois élaborée, les risques sont mis en exergue et cela facilite la prise de décision.

2.3.4. La phase d'action

L'identification, l'évaluation et la hiérarchisation des risques ainsi que l'identification du contrôle interne existant faits, les dirigeants de l'entreprise sont amenés à concevoir des plans d'actions en vue d'évaluer le dispositif de contrôle interne pour réduire les risques résiduels ou les transformer en risques cibles. L'objectif du plan d'action est de créer une plate-forme opérationnelle de progrès (LAURENT & al, 1991 : 1). La plate-forme doit préciser le planning des opérations, les responsables et les moyens de mise en œuvre.

2.3.5. La phase de reporting sur les risques résiduels

Pour PIGE (2003 : 15), le reporting est l'ensemble des informations de gestion qu'un responsable rend disponible à un niveau supérieur pour mesurer sa performance. Outil d'aide à la décision, le reporting permet le suivi des risques et présentera le tableau d'évaluation des risques inhérents et résiduels. Un système de reporting doit permettre de disposer d'informations fiables dans les délais réduits en vue d'une meilleure appréciation des risques de l'entreprise.

2.3.6. La phase de vérification de l'efficacité du plan d'action

Le plan fait l'objet d'une mise à jour permanente afin de faciliter l'évaluation des risques, ou les activités de déploiement complémentaire. La phase de vérification de l'efficacité au plan d'action permet de mettre à la disposition des dirigeants, les informations par l'évolution des risques résiduels, en dépit du contrôle interne existant, et d'éviter la survenance de nouveaux risques.

2.3.7. Amélioration et mise à jour de la démarche

Le suivi et la perpétuelle amélioration d'un système mis en place est nécessaire afin de perfectionner l'existant et de prévenir l'apparition de nouveaux facteurs qui peuvent nuire à la bonne marche de l'entité. L'évolution de l'environnement fait que la démarche doit être mise à jour afin d'être sur la même longueur d'onde de nouvelles pratiques et des dernières apparitions.

Conclusion

L'élaboration d'une cartographie des risques permet à l'organisation de se fixer des objectifs quant à la gestion des risques, de mettre en œuvre les moyens nécessaires à l'atteinte de ces objectifs. Ceci lui permettra d'élaborer sa stratégie de gestion des risques et d'élaborer son plan de communication, aussi bien interne qu'externe, des risques. Nous avons mis en relief la démarche d'élaboration d'une cartographie des risques ainsi que le processus de mise en place d'une cartographie des risques selon diverses approches. Un référentiel en matière de cartographie des risques peut être envisagé, le chapitre suivant sera ainsi consacré à l'élaboration d'une démarche référentielle de cartographie des risques adaptés à l'entreprise.

Chapitre 3 : METHODOLOGIE DE L'ETUDE

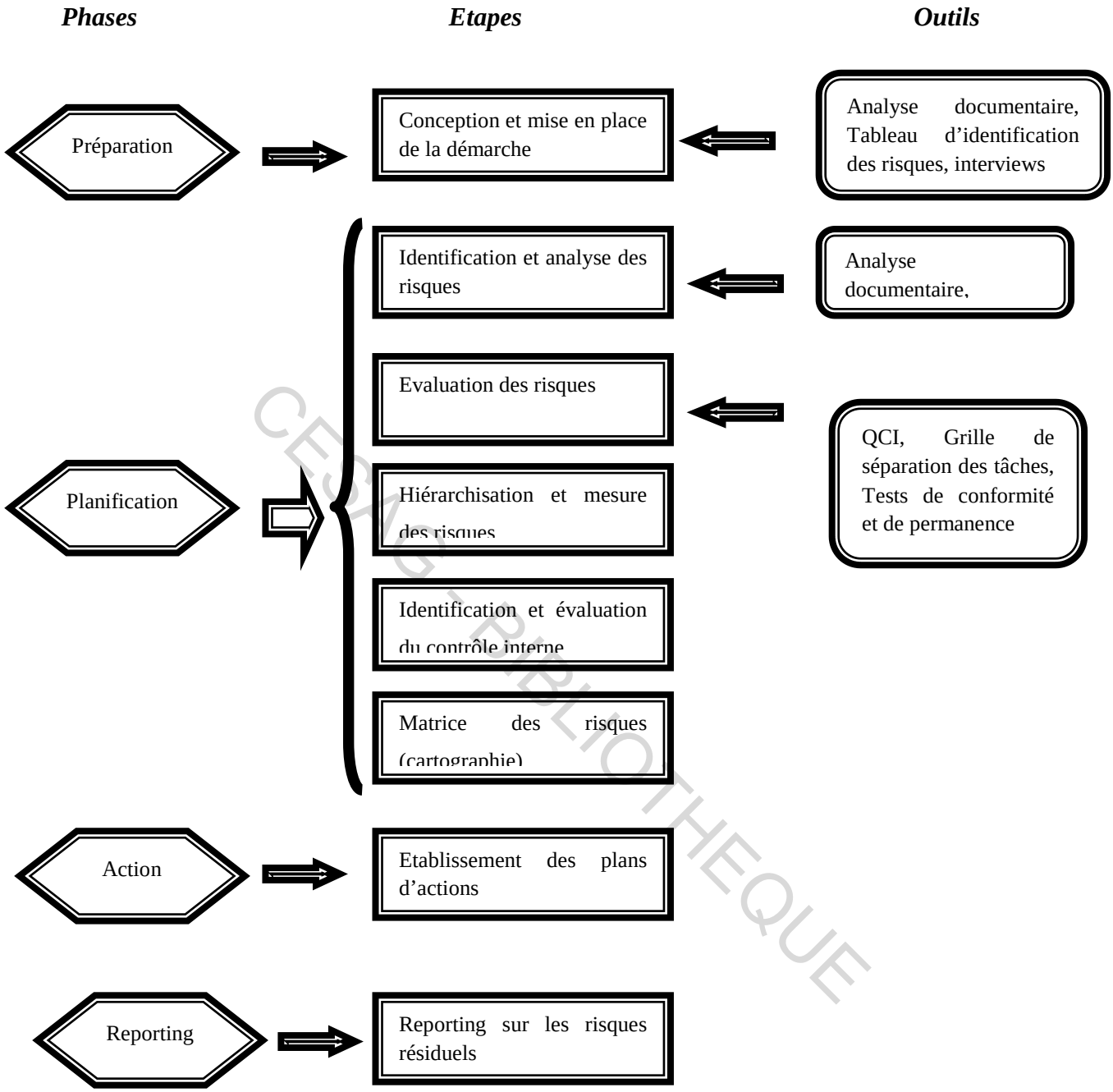
La revue de littérature nous a permis de présenter le réseau informatique ainsi que la cartographie des risques, nous passons donc à la présentation de notre modèle d'analyse qui nous permettra de mener à bien la partie pratique de notre travail.

L'objet de ce chapitre est l'élaboration d'une démarche référentielle de cartographie des risques ; pour cela le travail sera divisé en deux parties. La première partie consistera à la présentation de notre démarche référentielle et la seconde mentionnera les outils de collecte des données nécessaires à l'élaboration de la cartographie.

3.1. Notre démarche référentielle

Le référentiel proposé est composé de quatre phases et huit étapes et se présente comme suit :

Figure 11 : Modèle d'analyse



Source : Nous même

3.2. Outils de collecte des données

Notre objectif est d'avoir le maximum d'informations sur le réseau informatique, nous nous adresserons au responsable du réseau informatique et aux utilisateurs pour la collecte des données.

3.2.1. Collecte de données

L'évaluation du dispositif de contrôle interne se réalise grâce aux divers outils de collecte des données dont dispose l'entreprise. Ces outils peuvent être soit des outils de collecte d'information, soit des outils d'analyse des données.

Nous distinguons ici l'entretien et l'analyse documentaire

- **L'entretien**

L'objectif de l'entretien est d'obtenir une description des processus du domaine sous l'angle de ses risques et de son dispositif de contrôle interne.

Il a pour but d'une part de connaitre et comprendre l'architecture et le fonctionnement du réseau informatique au sein de l'entreprise et d'autre part d'avoir une idée sur les risques liés à son fonctionnement.

Nous avons effectué l'entretien avec le responsable du réseau informatique, les utilisateurs et les partenaires.

Tableau 2 : Récapitulatif des personnes interrogées et de leur responsabilité

Services	Responsabilité	Echantillon	Effectif total
IT	Responsable IT	1	1
Finance, Généraux, Direction etc.	Divers Responsables	3	6
Utilisateurs		25	50
Partenaires		4	10

Source : Nous même

- **L'analyse documentaire**

Elle consiste en l'exploitation des documents de l'organisation faisant l'objet de l'étude. Cela s'est imposé pour permettre d'avoir un aperçu de l'architecture du réseau informatique du PNUD Sénégal.

3.2.2. Outils d'analyse de données

Comme outils d'analyse nous allons utiliser le questionnaire de contrôle interne, la grille de séparation des taches,…

- **Le questionnaire de contrôle interne (QCI)**

Le QCI est une grille d'analyse qui permet de porter un diagnostique sur le dispositif de contrôle interne de l'entité, d'apprécier le niveau de contrôle et aussi de détecter les dysfonctionnements et d'en discerner les réelles causes.

Le questionnaire nous a permis d'apprécier les mesures de contrôles interne existant, de constater les points forts, les points faibles du dispositif mis en place par la caisse.

Les questions sont de types « fermées » et le questionnaire est conçu de sorte qu'un « non » équivaut à une lacune ou une faiblesse. Ce questionnaire a été rempli par les différents chefs des services et validé par le Responsable IT.

- **La grille des taches**

La grille des tâches est un outil permettant d'évaluer le dispositif de contrôle interne mis en place au sein de l'entreprise. Il présente une spécificité, qui est celle de mettre en exergue le cumul des fonctions incompatibles à un même poste de responsabilité.

- **Le tableau des risques**

Il sert à l'identification des risques. Il permet d'associer à chaque tâche, les risques susceptibles de se produire si son objectif n'est pas réalisé. Devant chaque tâche, nous exposerons l'objectif fixé, les risques encourus, et les pratiques d'organisation communément admises (POCA). Selon RENARD (2004 : 226) le tableau de risque prend en compte l'exposition, l'environnement et la menace. Ce tableau est également constitué à l'aide des pistes d'audit que sont les tests de conformité et les tests de permanence.

Conclusion :

Ce chapitre nous a permis de montrer la démarche référentielle que nous utiliserons lors de notre travail. Il a également permis le passage en revue des différents outils qui nous serons

nécessaires pour l'élaboration de la cartographie des risques liés au réseau informatique du PNUD Sénégal. Il marque l'achèvement de la revue de littérature et le passage à la partie pratique de notre étude.

Conclusion de la première partie

L'inhérence du risque nécessite de lui accorder une attention particulière. Toutes les organisations sont concernées par cette assertion ; le réseau informatique du PNUD Sénégal est particulièrement concerné par les risques informatiques.

Le PNUD Sénégal se doit être performant dans son rôle d'appui aux pays dans leur développement. Et cette assistance passe par la maîtrise des risques liés au réseau informatique.

Le support le plus adéquat à la maîtrise de ses risques est la cartographie des risques car elle attirera l'attention des dirigeants et des auditeurs sur les menaces qui pèsent sur la performance de la l'organisation.

DEUXIEME PARTIE : CADRE PRATIQUE

La reddition des comptes envers les donateurs et les partenaires obligent les organisations à être plus regardant que par le passé. Cela passe par la maîtrise des risques et des outils permettant d'y arriver en l'occurrence la cartographie des risques.

La gestion des risques consistera à donner l'assurance que les activités sont sous contrôle. En d'autres termes que les risques pouvant affecter l'atteinte des objectifs, voir entrainer la faillite de l'organisation sont maîtrisés ou minimisés.

Le PNUD Sénégal à travers ses aides multiformes envers les pays doit veiller à minimiser les risques dans tous les domaines. Il convient donc de mettre en place une cartographie des risques qui constituera un plan efficace de maîtrise des risques liés au réseau informatique. Elle constituera donc l'objet de cette seconde partie.

Nous présenterons donc dans cette partie le PNUD Sénégal, l'architecture existante du réseau informatique puis l'élaboration de la cartographie des risques liés au réseau informatique.

Chapitre 4 : PRESENTATION DU PROGRAMME DES NATIONS UNIES POUR LE DEVELOPPEMENT SENEGAL

Le Programme des Nations Unies pour le Développement Sénégal est une organisation internationale vieille de plus de 40 ans, Pour une meilleure appréhension du PNUD Sénégal, il paraît opportun de le présenter de façon générale et plus spécifiquement de présenter l'entité et l'architecture du réseau informatique qui fait l'objet de notre étude.

4.1. Présentation de la structure

Le PNUD Sénégal est une agence des Nations Unies spécialisée dans les Objectifs du Millénaire pour le Développement. Cette section présentera le PNUD Sénégal à travers son historique, ses missions, les objectifs qui lui sont assignés, son organisation, ses activités et ses ressources.

4.1.1. Historique du PNUD Sénégal

Le Programme des Nations Unies pour le développement (PNUD) est né en novembre 1965 de la fusion du Fonds spécial des Nations Unies et du Programme élargi d'assistance technique. Ce mariage conférait au PNUD dès sa création près de 50 ans d'expérience dans le secteur de la coopération.

Le Programme Pays (CPD) du PNUD tire son fondement du DSRP II/OMD, du Bilan Commun de Pays (CCA) et des domaines de coopération retenus dans le Plan Cadre des Nations Unies pour l'Assistance au Sénégal (UNDAF, 2007-2011). Il vise à renforcer la coopération du PNUD avec le gouvernement du Sénégal dans deux domaines prioritaires : la lutte contre la pauvreté et la création de richesse conçue dans la perspective d'une croissance pro-pauvre et durable (promotion des moyens d'existence durables liés à la préservation de l'environnement) et le renforcement de la gouvernance et du développement décentralisé et participatif.

4.1.2. Missions du PNUD Sénégal

Les missions dévolues au PNUD Sénégal sont principalement :

- promouvoir la gouvernance démocratique ;
- réduire la pauvreté ;

- prévenir les crises (catastrophes, guerres…) ;
- aider à la gestion durable des ressources (énergie, environnement …) ;
- empêcher la propagation du VIH/SIDA ;
- de manière globale, promouvoir le développement humain.

4.1.3. Objectifs assignés au PNUD Sénégal

Les objectifs du PNUD Sénégal se confondent aux Objectifs du Millénaire pour le Développement à savoir :

1. réduction de l'extrême pauvreté et de la faim ;
2. assurer l'éducation primaire pour tous ;
3. promouvoir l'égalité des sexes et l'autonomisation des femmes ;
4. réduire la mortalité infantile ;
5. améliorer la santé maternelle ;
6. combattre le VIH/SIDA, le paludisme et d'autres maladies ;
7. assurer un environnement durable ;
8. mettre en place un partenariat mondial pour le développement.

4.1.4. Organisation du PNUD Sénégal

Le PNUD Sénégal est dirigé par un Représentant Résident nommé par le Secrétaire Général des Nations Unies

Le PNUD Sénégal est subdivisé en trois entités bien distinctes à savoir :

- de la division Unité de Politique et d'Analyse Stratégique est coordonnée par l'Economiste Principal ;
- de la division Programme est coordonnée par les conseillers aux programmes ;
- de la division Operations est coordonnée par le Représentant Résident Adjoint et dispose d'un Assistant au Représentant Résident chargé des Opérations, et des unités opérationnelles suivantes (Unité de gestion des ressources humaines, une unité des finances et trésorerie, une unité des services généraux, approvisionnement et logistique, une unité de développement informatique et de la gestion des réseaux).

Le management ci-dessus cité est représenté par un organigramme (annexe 1).

4.1.5. Activités du PNUD Sénégal

Dans le cadre de l'exécution de son mandat, et pour permettre la réalisation des OMD, le PNUD Sénégal déploie des efforts constants pour accroître la capacité des pays couverts à faire face aux défis auxquels ils sont confrontés, dans les domaines prioritaires que le Programme s'est assignés.

Nous pouvons donc citer :

- réduction de la pauvreté ;
- gouvernance ;
- environnement et développement durable ;
- prévention des risques et catastrophes & relèvements post crise.

4.1.6. Ressources disponibles

Le PNUD Sénégal dispose de ressources humaines et financières. Les ressources humaines constituées d'un effectif de plus de 150 membres en 2008 jouent un rôle important dans la mise en œuvre des OMD. En effet quelque soit le niveau d'investissement le PNUD Sénégal ne peut remplir efficacement les missions qui lui sont assignées sans un personnel apte, qualifié et motivé dans l'accomplissement de ses tâches quotidiennes. Pour y parvenir les organes dirigeants du PNUD Sénégal ont mis en place un système de gestion et de développement des ressources humaines.

4.2. L'unité de développement informatique et de la gestion des réseaux du PNUD Sénégal

Il est dirigé par un analyste informatique placé sous l'autorité de l'Assistant au Représentant Résident chargé des Opérations. Il est secondé dans ses tâches par un assistant.

Cette unité a comme missions :

- administrer et exploiter les serveurs administratifs et communs ;
- maintenir le parc informatique, planifier les interventions d'installation, de configuration et de dépannage de matériels mis à la disposition de l'administration et des enseignants (hors laboratoires), et gérer les priorités ;

- établir l'inventaire du parc informatique et des logiciels en service dans tout l'établissement ;
- gérer le réseau informatique et faire évoluer l'infrastructure matérielle dans tous les bâtiments ;
- établir les schémas du réseau informatique et de téléphonie ;
- gérer les serveurs d'annuaires et fournir des services numériques aux usagers (messagerie électronique, réseau sans fil, ...) ;
- gérer le site Internet institutionnel et mettre à jour les informations qui s'y trouvent ;
- gérer les équipements audiovisuels et les systèmes de visioconférence (IP et RNIS) ;
- mettre en place les mécanismes concernant la sécurité informatique, et assurer la veille sur l'évolution des risques ;
- mettre en place une politique de sauvegarde et d'archivage des données ;
- maintenir et faire évoluer le système d'information ;
- conseiller et informer les utilisateurs dans tout ce qui touche à l'informatique au sens large.

Conclusion :

Ce chapitre a permis de faire, une présentation générale du PNUD Sénégal à travers son historique, ses missions, ses objectifs, son organisation, ses activités et ses ressources ainsi qu'une présentation de l'unité chargé du réseau informatique et de ses missions. Cette présentation achevée, nous ferons une description de l'architecture du réseau informatique existant ainsi que les tests de conformité et de permanence relatifs au réseau informatique

Chapitre 5 : DESCRIPTION DU RESEAU INFORMATIQUE EXISTANT

Dans ce chapitre consacré à la description du réseau informatique existant du PNUD Sénégal, nous verrons l'organisation du réseau, le système de gestion de bases de données, la sécurité et enfin la politique de sauvegarde.

5.1. Description de l'organisation du réseau

Nous présenterons la structure d'Active Directory à savoir le site, le domaine, l'unité organisationnelle et enfin la stratégie de groupe.

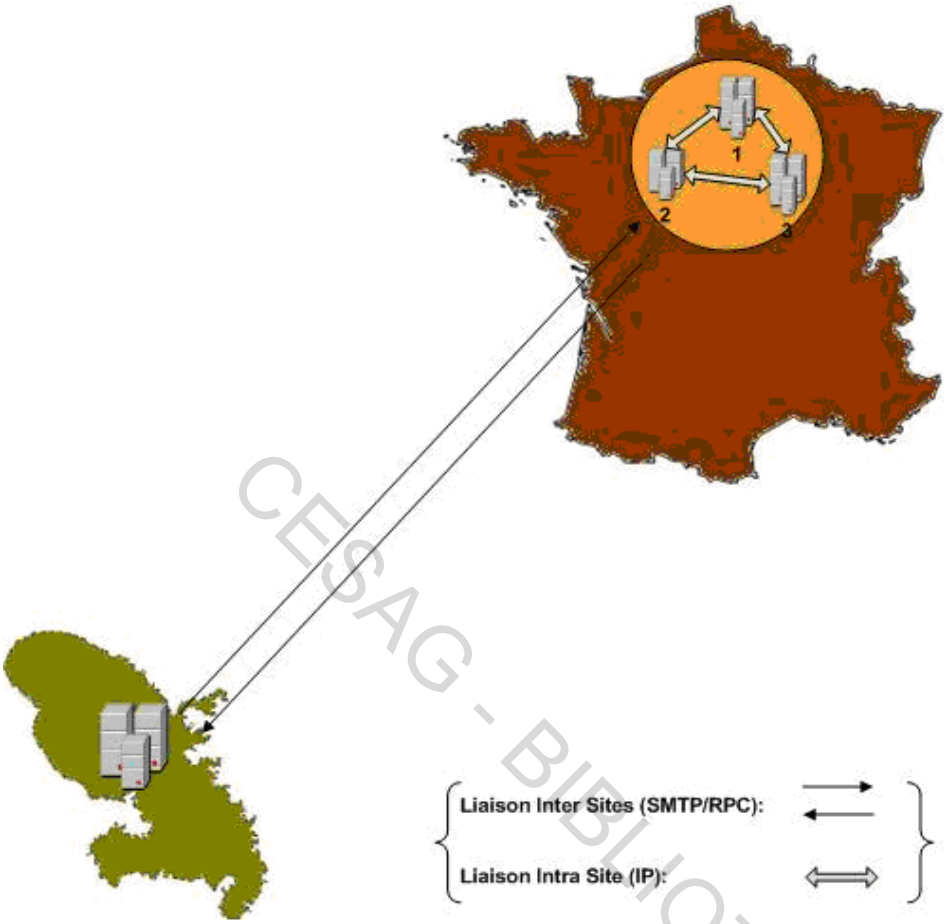
5.1.1. Présentation générale d'Active Directory

La structure d'Active Directory du PNUD Sénégal permet de gérer de façon centralisée des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites. Les règles (autorisation, interdiction...) sont appliquées aux utilisateurs et/ou aux ordinateurs, elles sont appelées « stratégie de groupe ». Elles sont appliquées au niveau du site UNDP, du domaine undp.local ou de l'unité d'organisation Ordinateurs ou utilisateurs.

5.1.2. Description du site UNDP

Le site UNDP est un ensemble de sous réseaux connectés entre eux par une liaison haut débit fiable (LAN). Il est également connecté au PNUD Siège situé à New York par le biais du réseau (WAN).

Figure 12 : Architecture de l'intégration entre AD de Dakar et AD de New York



Source : PNUD

Le protocole utilisé pour la connexion à l'intérieur d'un site utilisée est TCP/IP, entre les sites RPC et SMTP (en renvoi de bas de page).

5.1.3. Description du domaine undp.local

Le domaine du PNUD Sénégal est constitué d'un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Ce domaine a un nom unique sur le réseau qui est undp.local.

5.1.4. Description de l'unité d'organisation

L'unité d'organisation (OU) au sein du PNUD Sénégal est un objet conteneur permettant d'organiser les objets au sein du domaine. Elle contient des comptes d'utilisateurs, des

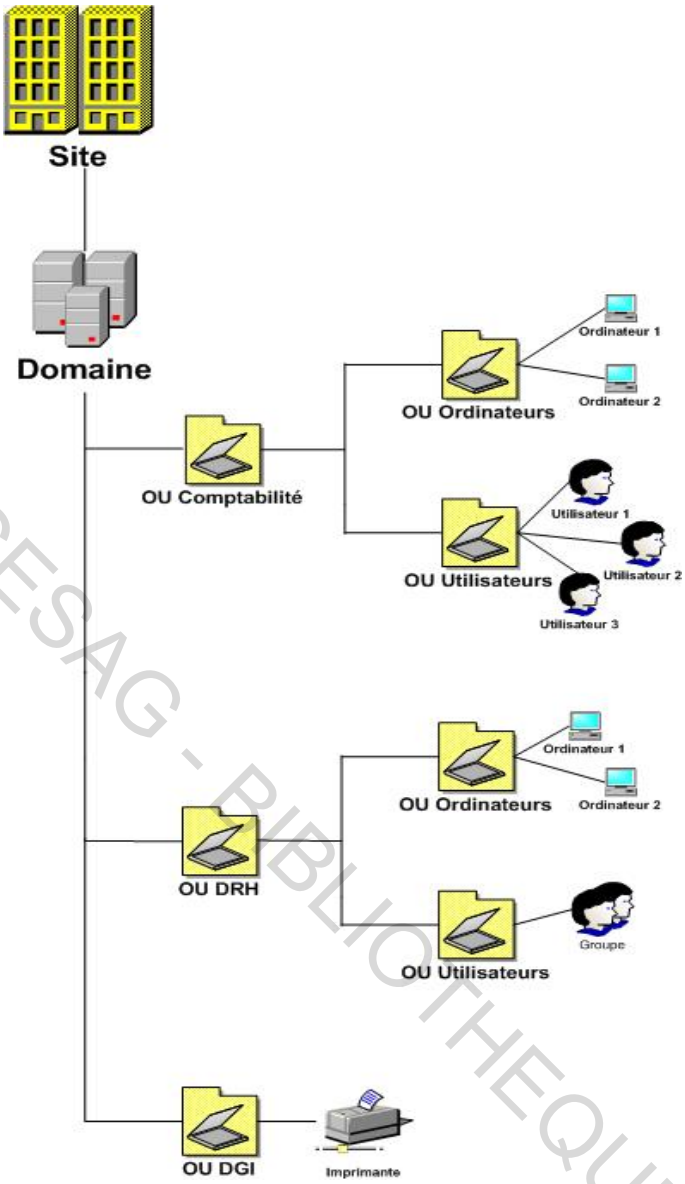
groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation du PNUD Sénégal.

5.1.5. Description de la stratégie de groupe

L'utilisation de la stratégie de groupe (GPO- Objet stratégie de groupe) permet de gérer de façon centralisée les utilisateurs et les ordinateurs au sein du PNUD Sénégal. La centralisation des stratégies de groupe permet de définir une GPO pour toute l'organisation PNUD Sénégal au niveau du site, du domaine ou au niveau de l'unité d'organisation.

Avec les GPO, chaque utilisateur dispose de l'environnement utilisateur dont il a besoin pour travailler, tout en appliquant les stratégies de l'organisation, notamment les règles, les objectifs et les besoins en matière de sécurité. Les objets stratégie de groupe sont appliqués aux ordinateurs et/ou utilisateurs à l'ouverture ou la fermeture d'une session, au démarrage ou à la fermeture du système d'exploitation.

Figure 13 : Partie de l'Active Directory du PNUD Sénégal



Source : Nous Même

5.2. Système de gestion de base de données

La nécessité pour le PNUD Sénégal d'archiver ses données (contacts, courrier, salaires…), lui impose d'utiliser des bases de données pour enregistrer toutes les informations qu'elle souhaite garder dans la mémoire institutionnelle.

Il existe 2 types de bases de données au sein du PNUD Sénégal. Ce choix est dicté par la quantité d'information à stocker, la fiabilité, le coût.

5.2.1. Description du SGBD SQL Server

SQL Server au sein du PNUD Sénégal est un système de gestion de bases de données relationnel de Microsoft. Il possède toutes les fonctionnalités nécessaires nous permettant de créer, de modifier et d'administrer des bases de données.

Le Transact-SQL est le langage dédié à l'accès aux données sous SQL Server. Il est d'ailleurs nécessaire de connaître ce langage pour l'utilisation de SQL Server. Le Transact-SQL est une extension de SQL.

Le système de gestion de base de données SQL Server est basé sur une architecture Client-serveur.

Cette base de données nous permet de créer des utilisateurs, des groupes d'utilisateurs, des groupes de machines etc.

5.2.2. Description du SGBD Access

Microsoft Access est un système de gestion de base de données produit par Microsoft qui permet au sein du PNUD Sénégal de stocker des informations sur les courriers entrants, en attente de départ et sortants. Il est disponible dans la suite Microsoft Office.

Faisant partie d'une suite bureautique, Access n'a pas été conçu pour supporter de grandes bases de données. La taille maximale d'une base Access est de 2Go.

Il est cependant possible d'utiliser un frontal Access connecté à une base de données SQL Server. Il s'agit de créer un formulaire sous Access et de faire la liaison avec SQL Server grâce à une connexion ODBC.

5.3. Sécurité via l'authentification et les pare-feux

Le réseau informatique devient de nos jours un outil indispensable, le PNUD Sénégal comme toutes les autres organisations doivent faire face à l'augmentation d'actes de malveillance de toutes sortes (intrusions, virus, spyware...) qui évoluent sans cesse. Il est donc primordial de gérer la sécurité et l'accès du réseau informatique afin de protéger l'intégrité des données.

La politique de sécurité au sein du PNUD Sénégal est dirigée par le département de sécurité qui se trouve à New York.

Ces informations sur la politique de sécurité au PNUD sont strictement confidentielles et ne peuvent figurer dans ce mémoire.

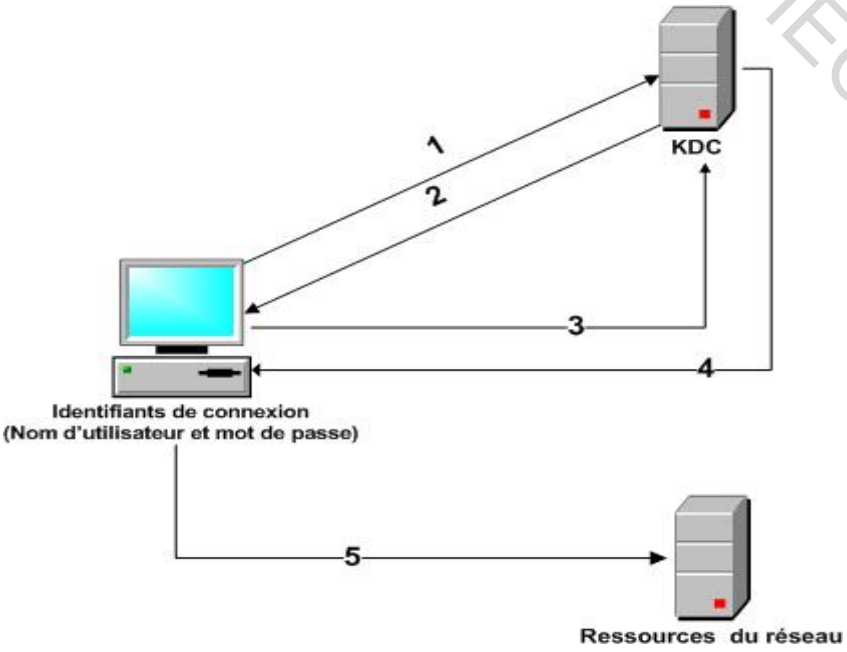
5.3.1. Description du système d'authentification

L'authentification étant primordiale pour la sécurité du système d'information de même que pour un réseau informatique. Elle permet à un utilisateur du PNUD Sénégal de s'identifier afin d'ouvrir une session sur le domaine undp.local ou d'accéder aux ressources du réseau UNDP. Au sein du PNUD Sénégal, l'authentification utilisée est l'authentification par mot de passe.

En utilisant le service d'annuaire Active Directory, le mécanisme d'authentification utilisé est Kerberos. Le service Kerberos est basé sur un système de clé crypté appelé KDC (KeyDistributionCenter).

Voici le processus d'authentification et d'accès aux ressources du réseau PNUD Sénégal avec Kerberos :

Figure 14 : Processus d'authentification et d'accès aux ressources du réseau via Kerberos



Source : Microsoft

1. L'utilisateur entre des informations d'identification qui sont cryptées par le centre de distribution de clefs.
2. Les informations d'identification cryptées du client sont comparées avec celles se trouvant sur Active Directory. Si les informations sont correctes le processus continue dans le cas contraire il est interrompu.
3. Le processus se poursuit, le client reçoit un ticket : le TGT (Ticket Granting Ticket). Le TGT contient les identificateurs de sécurité des groupes dont l'utilisateur est membre. L'utilisateur est maintenant authentifié et son profil peut être chargé. Note : Un TGT expire au bout de 8 heures ou bien quand l'utilisateur ferme sa session.
4. Pour accéder aux ressources du réseau, l'utilisateur utilise son TGT pour accéder au service d'accord de ticket TGS (Ticket Granting Service).
5. Le TGS transmet à l'utilisateur un ticket de session.
6. L'utilisateur utilise ce ticket de session pour accéder aux ressources d'un serveur de ficher seulement s'il possède les droits requis sinon le processus échoue.

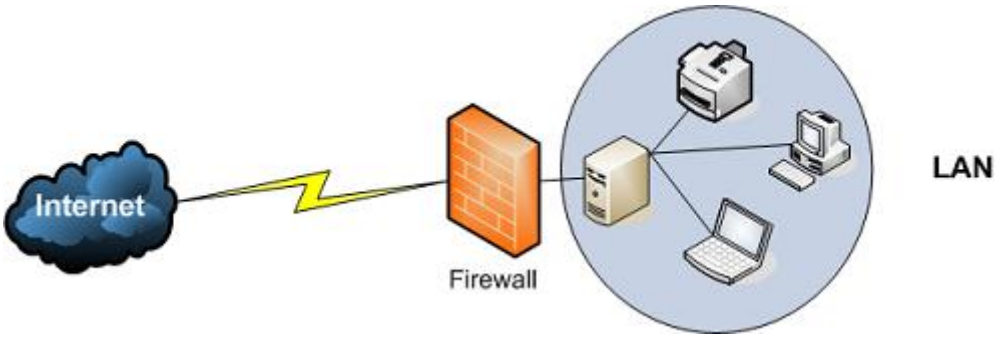
5.3.2. Description du système des pare-feux

Le réseau du PNUD Sénégal étant relié à Internet, il est donc plus vulnérable aux attaques venant de l'extérieur. Dans ce cas, pour surveiller et contrôler les données qui entrent et qui sortent de votre réseau, il est primordial d'utiliser un pare-feu. Il existe 2 types de pare-feu: le pare-feu logiciel et le pare-feu matériel. Pour une sécurité accrue, le PNUD Sénégal a décidé de combiner les 2 types :

5.3.2.1. Pare-feu logiciel : Microsoft ISA Server

Microsoft ISA Serveur est un produit Microsoft, il est à la fois un serveur proxy et un pare-feu. Le pare-feu permet de contrôler l'ensemble du trafic entrant et sortant au sein du PNUD Sénégal. Il est installé à l'interconnexion du réseau privé et Internet. Le trafic sortant est contrôlé par des règles ou des stratégies d'accès. Les stratégies d'accès sont constituées de règles sur les protocoles c'est à dire autoriser ou non un protocole, ou de règles sur les sites et le contenu. Le trafic entrant est contrôlé par différents types de filtres, les filtres de paquets IP basés sur l'adresse ou le port TCP/IP, les filtres d'application et les filtres de détection d'intrusion.

Figure 15 : Représentation d'un pare-feu au sein d'un réseau local



Source : Nous Même à partir de Cisco

5.3.2.2. Pare-feu matériel : Routeur Cisco ASA

Les routeurs Cisco au sein du PNUD Sénégal disposent d'un système d'exploitation (IOS) qui offre des possibilités très intéressantes de filtrage notamment le filtrage par Access List (ACLs).

Les listes de contrôle d'accès (ACL) nous permettent de filtrer le réseau à partir des adresses.

L'administrateur du réseau PNUD Sénégal peut contrôler le trafic réseau en autorisant ou en interdisant l'accès à une interface du routeur. Le routeur quant à lui vérifie chaque paquet afin de déterminer s'il doit l'acheminer ou pas d'après la règle d'accès fixée. Il y a 2 types de listes de contrôle d'accès, les ACLs standards et les ACLs étendues.

- **ACLs standards**

Les ACLs standards permettent de filtrer l'accès à un réseau entier.
Voici la syntaxe d'une ACL standard:
Router (config)# access-list {Numéro de la liste d'accès} {permit|deny} {condition}
Exemple:
Router (config)#access-list 101 permit 192.168.0.0 0.0.255.255
Cette ACL autorise le trafic provenant du réseau 192.168.x.x

- **ACLs étendues**

Les ACLS étendus permettent de filtrer l'accès en se basant sur des adresses précises (n° de port, adresse source, adresse de destination)

Voici la syntaxe d'une ACL étendue:

Router (config)# access-list {Numéro de la liste d'accès} {permit|deny} protocol source [source-mask destination destination-mask operator operand][established]

Exemple:

Router (config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 eq21
Cette ACL autorise tous les paquets FTP provenant des réseaux 192.168.2.x et 192.168.3.x

5.4. Description de la politique de sauvegarde au sein du PNUD Sénégal

L'administrateur du PNUD Sénégal a opté pour le type de sauvegarde totale. Ce type de sauvegarde lui permet d'assurer la pérennité et la récupération de la totalité des données critiques sans perturber le fonctionnement de son réseau.

5.4.1. Description du système de sauvegarde totale

La sauvegarde totale effectué au sein du PNUD Sénégal est une copie conforme de l'intégralité des données, quelque soit la taille du fichier, du type de données de tous les disques durs à un instant *t* bien précis. Cette sauvegarde implique une durée plus élevé de copie. Cependant, elle conserve des données redondantes car les données modifiées de même que les données non modifiées sont copiées à chaque exécution de la sauvegarde totale.

La sauvegarde totale est le type de sauvegarde utilisé au sein de l'organisation. Elle se fait journalièrement, hebdomadairement, mensuellement et semestriellement.

5.4.2. Description du système de RAID

Le RAID (Réseau redondant de disques indépendants) au sein du PNUD Sénégal consiste à mettre en place une combinaison de plusieurs disques durs formant une unité de stockage. Cette technologie RAID en plus d'augmenter les capacités de stockage, permet d'assurer une tolérance aux pannes en cas de crash ou de défaillance d'un disque au sein de l'organisation.

Nous distinguons plusieurs types de RAID, le choix portera sur la sécurité, la fiabilité, les performances et le coût. Les systèmes de RAID utilisés au sein de la structure sont le RAID 1 et le RAID 5.

5.4.2.1. Le mode opératoire

- définir le RAID au niveau du BIOS ;
- faire reconnaître le RAID avec le système d'exploitation ;
- installer la carte mère avant même les pilotes du raid et de la l'installation de Windows.

5.4.2.2. Le résultat obtenu

Les données sont mirrorées sur les disques qui sont réparties de manière équitable.

5.4.2.3. Le fonctionnement du RAID

Les données sont copiées sur les premiers disques ainsi de suite. Après celles sont copiées sur les disques redondants de manière à ce que lorsque les données sont perdues parce qu'un disque est crashé, elles peuvent être reproduites immédiatement dès que le disque a été changé.

5.4.2.4. La sécurité du RAID

En ce qui concerne la sécurité au niveau du RAID, nous avons des disques en spare qui nous permettent de changer le plus rapidement possible un disque défectueux.

Le PNUD Sénégal a adopté l'utilisation des RAID 1 et RAID 5 pour la sauvegarde et la pérennisation de ses données.

5.5. Description des autres besoins au sein du PNUD Sénégal

De nombreuses applications sont disponibles au sein de l'organisation pour parfaire notre infrastructure informatisée.

Dans le souci de faire passer des notes de services ou différentes informations importantes aux employés et pour une réelle cohésion au sein de notre groupe, le serveur de mail a été configuré de même que son backup.

Pour que les personnes étrangères puissent avoir un certain nombre de renseignement sur le fonctionnement et les offres de l'organisation sans avoir à s'y rendre ou par téléphone, un site web a été créé. Le site web est un atout majeur pour la promotion de l'organisation.

5.5.1. La messagerie

La messagerie est le moyen de communication le plus utilisé au sein du PNUD Sénégal. Pour cela, nous disposons d'un serveur mail. Exchange qui est le serveur de messagerie et d'espace collaboratif de Microsoft. Il nous permet de gérer l'échange des courriers électroniques interne et externe. Le transfert et la réception des e-mails sont basés sur des protocoles de routage de courrier. On y retrouve le protocole SMTP, POP et IMAP.

Les messageries utilisées au sein du PNUD Sénégal sont Iplanet et Microsoft Exchange 2010.

5.5.1.1. Le Protocole SMTP

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier entre des agents de transfert de message. Il fonctionne au niveau de la couche application du modèle OSI. C'est le protocole utilisé au sein du serveur de messagerie Microsoft Exchange 2010.

5.5.1.2. Le Protocole POP

Le protocole POP (Post Office Protocol) permet de récupérer le courrier depuis un serveur. Les utilisateurs n'étant pas en permanence connecté à Internet peuvent ainsi récupérer leurs mails et les consulter en mode hors connexion. C'est le protocole qui est implémenté au niveau du second serveur de messagerie Iplanet.

5.5.1.3. Le Protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) permet également d'accéder au courrier depuis un serveur. Un utilisateur a la possibilité de consulter ses mails depuis le serveur sans avoir à le rapatrier. Ce protocole est autant utilisé au niveau du serveur Exchange que du serveur Iplanet.

5.5.2. Le site web du PNUD Sénégal

Le site web est un ensemble de pages contenant diverses données (texte, image, vidéo…) liées entre elles par des liens hypertextes et formant un ensemble de données homogènes. Chaque site web possède une adresse Web et est consultable à partir d'un navigateur Web tel qu'Internet Explorer ou encore Mozilla Firefox.

La création, la gestion et le suivi du site a été confié à un prestataire externe. Il met à jour le site web, rajoute des articles ou documents demandés etc.

Le site web du PNUD Sénégal est www.undp.org.sn

5.5.3. Les applicatifs maisons

Les applicatifs maisons sont nos logiciels conçus exclusivement selon les besoins de l'organisation dans la mesure où nous n'avons pas trouvé un programme qui correspondrait entièrement à nos besoins.

Nous pouvons donc citer notre application qui permet de gérer les stocks, les courriers et ainsi que le carburant.

Atlas est un progiciel de gestion intégré qui nous permet de faire des achats, de préparer des requêtes de voyages.

Le PNUD Sénégal dispose d'un outil collaboratif nommé SharePoint qui est un espace de partage et d'échange et de dépôt de documents électroniques.

Les applicatifs maisons sont basés sous des logiciels libres comme SPIP pour la conception du site web du PNUD.

Le progiciel tourne avec une base de données Oracle.

Tous les logiciels propriétaires utilisés au sein de l'organisation font partie d'un accord nommé LTA avec Microsoft, Cisco, Symantec etc.

5.6. Description des types de réseau au sein du PNUD Sénégal

Le LAN : constitué d'une centaine d'ordinateurs qui sont reliés entre eux par des switch d'étage, un switch de distribution et enfin un switch core. Ce switch core est relié directement au routeur d'où provient la connexion internet. Tous les postes opèrent sous le système d'exploitation Windows XP and sont dotés des antivirus et anti spywares.

Les cartes réseaux utilisés par ses différents ordinateurs ont une capacité de 100/1000 bits/s.

Le WAN : constitué de deux (2) liaisons internationales pour relier le PNUD Sénégal au monde.

La première liaison est une liaison spécialisée de la Sonatel d'un débit de 1Mbps. Elle permet à l'organisation de gérer certaines facilités comme la messagerie, la vidéoconférence, la VoIP et l'accès internet aux utilisateurs.

La deuxième liaison est une liaison VSAT de EMC qui joue le rôle de liaison de secours au cas la liaison principale tomberait en panne. Elle est d'un débit de 256 Kbps. Il existe un système de basculement automatique dès que l'une ou l'autre des liaisons tombe.

Le WLAN : encore appelé Wi-Fi. Nous avons plus d'une dizaine de points d'accès. Par étage, nous pouvons en compter 2 ou 3. Il existe le Wi-Fi pour les visiteurs et le Wi-Fi pour le personnel.

La topologie utilisée au sein du PNUD Sénégal est la topologie étoilée. Elle permet de relier tous les ordinateurs d'un étage au même switch d'étage.

Le câblage utilisé au sein du PNUD Sénégal est un câblage VDI (voix Données Internet) utilisant la paire torsadée catégorie 6 et qui permet de transporter à la fois la voix, les données et l'internet.

La messagerie utilisée est une architecture client-serveur dans la mesure nous avons le serveur Microsoft Exchange 2010 et les clients Outlook 2007 qui essaient de s'y connecter pour récupérer les mails.

Différents protocoles réseaux sont utilisés pour le bon fonctionnement du réseau informatique. Nous avons le service DNS qui permet de faire la conversion adresse IP en nom de domaine, le DHCP qui permet l'attribution dynamique d'adresses IP aux utilisateurs du réseau, ARP qui fait la conversion de l'adresse IP en adresse MAC pour les différents machines

Matériels utilisés au sein du PNUD Sénégal : Nous avons un modem VSAT Paradise pour la communication VSAT, un modem V36 Sonatel pour la liaison louée, un routeur 3600 Cisco, un PABX pour la communication téléphonique, 4 switch d'étages de 48 ports de marque Cisco, 2 switch de distributions pour assurer la redondance et enfin un switch core.

Nous avons noté l'existence de quelques concentrateurs dans le réseau.

Le PNUD Sénégal dispose d'un intranet au niveau mondial qui permet à tous les employés de rester connectés et de pouvoir partager des informations.

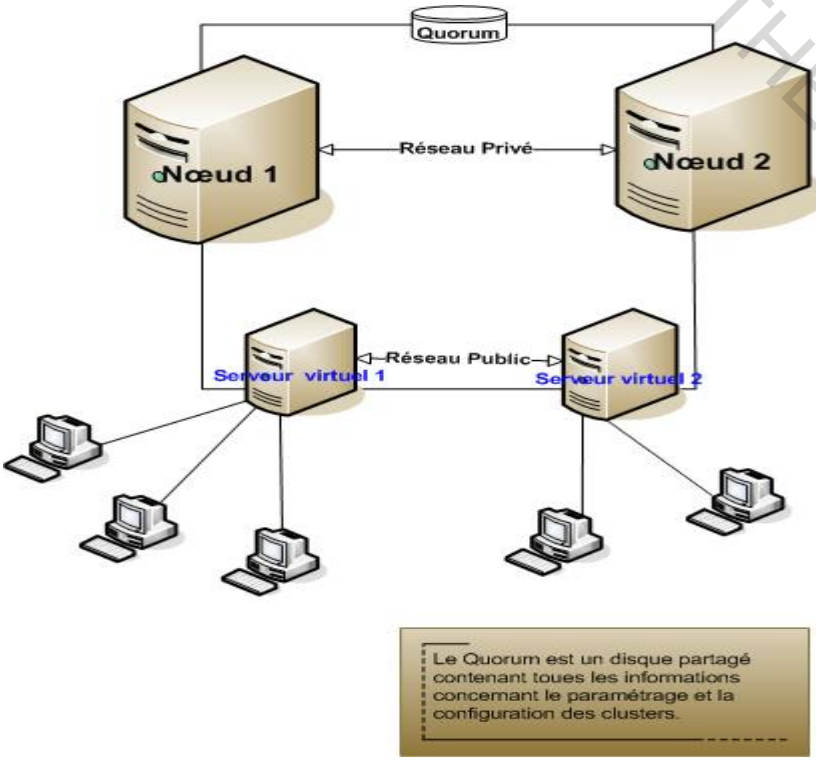
L'extranet du PNUD Sénégal est basé sur la plateforme Microsoft SharePoint qui permet aux partenaires externes de pouvoir interagir avec le PNUD Sénégal.

5.7. Description du système de répartition des charges au sein du PNUD Sénégal

La répartition des charges (load balancing) permet d'éviter la surcharge d'un serveur. En cas de connexion massive par exemple lors d'une heure de pointe (ouverture de l'entreprise), un grand nombre de requête est envoyé au serveur. Celui-ci perd en performance et le temps de réponse est beaucoup plus élevé. La solution serait d'utiliser un système de clustering. Un serveur de cluster est un groupe de serveurs gérant des ressources stockées sur des disques partagés. Chaque serveur du cluster est appelé nœud.

Au sein du PNUD Sénégal, le principe de la répartition des charges, de même que le clustering est appliqué.

Figure 16 : Schéma représentant le fonctionnement de la répartition des charges



Source : Technet

5.8. Description du système de maintenance au sein du PNUD Sénégal

La maintenance préventive appliquée au sein de l'organisation permet d'appliquer des mises à jour sur les systèmes, de prévenir des incidents de bogues aussi bien au niveau du hardware (ordinateurs, imprimantes, scanners, digital senders) que du software.

Une fois l'élément endommagé, la maintenance curative se met en place. Elle intervient sur l'élément endommagé ce qui conduit à la réparation de la panne de façon à remettre l'élément endommagé en marche et à éviter toute forme de dégradation.

La maintenance appliquée au sein du PNUD Sénégal est une maintenance interne.

Conclusion

Ce chapitre nous a permis de présenter l'organisation du réseau, le système de gestion des bases de données, la sécurité, la politique de sauvegarde et enfin le système de maintenance. Les risques liés au réseau informatique peuvent avoir des conséquences graves. Ainsi il convient d'analyser les différents compartiments du réseau informatique afin d'identifier, d'évaluer, d'hiérarchiser et de mesurer les risques qui pourraient en découler. Ceci nous permettra d'élaborer une cartographie des risques liés au réseau informatique qui fera l'objet du chapitre suivant.

Chapitre 6 : ELABORATION DE LA CARTOGRAPHIE DES RISQUES LIES AU RESEAU INFORMATIQUE AU SEIN DU PNUD SENEGAL

Les risques auxquels est exposé le réseau informatique du PNUD Sénégal nécessitent d'être maîtrisés. L'élaboration de la cartographie des risques permettrait de mettre en relief les risques susceptibles d'entraver la bonne marche du réseau informatique au sein du PNUD Sénégal.

Ce chapitre sera l'occasion d'analyser et d'identifier les risques à partir des différents compartiments cités au chapitre précédent, de les évaluer, de les hiérarchiser et d'élaborer la cartographie des risques liés au sein du PNUD Sénégal.

6.1. Identification des risques liés au réseau informatique

L'identification va consister à détecter les risques à partir des différents compartiments constituant les différentes entités constituantes du réseau informatique du PNUD Sénégal élaborées dans ce travail tels que l'organisation du réseau, le système de gestion des bases de données, la sécurité, la politique de sauvegarde et enfin le système de maintenance. L'identification des différents risques se fera à l'aide de tableaux. Nous avons à l'intérieur de ces tableaux des abréviations (Ob), (P), (S) utilisés respectivement pour Observations, Procédures et Systèmes.

6.1.1. Identification des risques matériels

Nous identifierons successivement les risques liés au matériel, les pannes et dysfonctionnement de matériel ou de logiciel de base.

Tableau 3 : Identification des risques matériels

Risques accidentels	Impact	Dispositif de maîtrise	Dispositif maîtrisé
Coupure câble électrique	Réseau informatique Hors service	- (Ob) Bonne protection des câbles d'alimentation - (P) Appel à un expert lors de la survenance d'un problème électrique	Oui
Incendie dans le local technique	Destruction totale des données et du matériel	- (Ob) Bonne protection des locaux techniques, dispositif Anti-incendie - (P) Formation du personnel en cas d'incendie sur la marche à adopter	Oui
Foudre, tempête au sein du local technique	Destruction partielle ou totale des données et du matériel	- (Ob) Mise en place d'un système de mise à la terre et d'un paratonnerre - (P) Procédure de veille et de contrôle des systèmes mis en place	Oui
Indisponibilité des serveurs	Impossibilité de travailler	- (Ob) Mise en place d'un système de redondance et d'un système de load balancing - (P) Procédure de vérification semestrielle du bon fonctionnement du système de redondance et de failover	Oui
Défectuosité des équipements switch routeurs PABX etc.	- Impossibilité de travailler - Communication impossible au sein de l'organisation	- (Ob) Disponibilité en spare de tous ses équipements au magasin - (P) Procédure de vérification si disponibilité il y a de tous les matériels au sein du magasin	Oui

Vol des matériels ou logiciels informatiques	- Dépenses supplémentaires - Divulgation des informations	- (Ob) Mise en place d'un système anti-intrusion - (P) Procédure de vérification périodique du bon fonctionnement du système	Oui
Indisponibilité du contrôleur de domaine	Non authentification des utilisateurs au sein du système	- (Ob) Mise en place d'un serveur redondant pour le contrôleur de domaine - (P) Procédure de vérification périodique du bon fonctionnement du serveur redondant	Oui
Mauvaise définition des GPO à appliquer aux ordinateurs et aux utilisateurs	- Non application des GPO - Non disponibilité des outils pour travailler	(P) Procédure de définition de la mise en place des GPO au sein du système	Oui
Mauvaise définition des utilisateurs dans une UO	Utilisateurs d'un même département ne pouvant pas partager des ressources	(P) Procédure de définition de la mise en place des utilisateurs dans les UO	Oui

Source : Nous même

6.1.2. Identification des risques liés aux erreurs

Nous identifierons successivement les risques liés aux erreurs de saisie, de transmission, d'utilisation de l'information, d'exploitation, de conception et de réalisation.

Tableau 4 : Identification des risques liés aux erreurs

Risques liés aux erreurs	Impact	Dispositif de maîtrise	Dispositif maîtrisé
Mauvaise manipulation des équipements réseaux	Réseau informatique Hors service	- (Ob) Système de niveau d'autorisation avant d'avoir accès sur un équipement - (P) Procédure claire définissant les tâches à effecteur durant une panne bien spécifique	Oui
Mauvaise manipulation des données	- Suppression des données - Divulgation des données à l'externe	- (Ob) Mise en place d'un système de backup automatique de toutes les données - (P) Approbation par des managers avant publication ou sortie d'un document de l'organisation	Oui
Introduction des logiciels malveillants dans le réseau	Destruction ou vol partiel ou total des données et du matériel	- (Ob) Installation de logiciel est assujettie à seulement l'administrateur du réseau - (P) Procédure de veille et de contrôle des machines des utilisateurs	Oui
Vol des informations confidentielles	Organisation exposée à l'extérieur	- (Ob) Pas de possibilité de copie des données sur des équipements externes - (P) Procédure de veille et de contrôle pour s'assurer que la mesure n'est pas transgressée	Oui
Non suppression d'un compte d'un utilisateur licencié ou partie à la retraite	Attaques du réseau et indisponibilité des services réseaux	- (Ob) Désactivation ou suppression automatique du compte de l'utilisateur - (P) Procédure claire à adopter lors du départ d'un utilisateur	Oui
Mauvaise saisie dans une base de données	Perte des données au sein de la BD	- (Ob) Mise en place de groupes de personnes habiletés à inscrire des informations dans la base de données - (P) Procédure de backup journalier des informations pour la restauration	Oui
Effacement accidentel des données, ou	- Organisation vulnérable sans système de	- (Ob) Mise en place d'une sauvegarde journalière des données utilisateurs, Backup	Oui

détérioration des informations sur le support de stockage	sauvegarde. - Perte de temps pour l'exécution des tâches	disponible en 2 exemplaires - (P) Procédure de sauvegarde des documents utilisateurs	
Mauvaise définition d'une politique de sécurité	- Denial of Service - Vol des informations - Pertes des données - Sabotage du local technique	- (Ob) Mise en place d'une politique de sécurité pour endiguer toutes sortes d'attaques - (P) Procédure de veille et de contrôle de la politique de sécurité	Oui
Mauvaise définition d'un système de sauvegarde	- -Perte des données utilisateurs. - -Arrêt de travail dans certaines situations	- (Ob) Mise en place d'une politique de sauvegarde pour endiguer toutes sortes de pertes de données - (P) Procédure de veille et de contrôle de la politique de sauvegarde	Oui
Mauvaise acquisition des logiciels et des applicatifs	- Ralentissement des objectifs de l'organisation - L'atteinte des objectifs est compromise	- (P) Procédure d'acquisition des logiciels et des applicatifs par une sélection rigoureuse des fournisseurs	Oui
Mauvaise exploitation ou des logiciels et des applicatifs	Rendement escompté non atteint	- (Ob) Mise en place d'une politique de formation pour l'utilisation des logiciels et des applicatifs - (P) Procédure de test sur l'utilisation des logiciels et des applicatifs	Oui
Absence d'un plan de continuité des activités	Rupture totale et complète des activités	- (Ob) Mise en place d'un plan de continuité des activités - (P) Procédure de test du plan de continuité des activités	Non

Source : Nous même

6.1.3. Identification des risques liés à la malveillance

Nous identifierons successivement les risques liés au vol, sabotage du matériel, à la fraude, aux indiscrétions et détournements de logiciels.

Tableau 5 : Identification des risques liés à la malveillance

Risques liés à la malveillance	Impact	Dispositif de maîtrise	Dispositif maîtrisé
Copie illicite de logiciels	- Poursuites pénales et sanctions financières encourues - Bugs sur des bons logiciels avec License	- (Ob) Dispositif de lutte contre la copie illicite de logiciels - (P) Procédure claire sanctionnant les auteurs de copie de logiciels	Oui
Indiscrétion, détournement d'informations	- Exposition de l'organisation aux menaces et attaques extérieures - -Concurrence déloyale	- (Ob) Mise en place d'un système de validation avant sortie divulgation d'informations à l'extérieur - (P) Système d'approbation avant sortie de toute information	Oui
Attaque logique du réseau via les vers, les virus et différents types d'attaques	- Réseau fonctionnant au ralenti - Vol ou destruction des données	- (Ob) Mise en place de pare feux matériels et logiciels - Mise en place d'un système d'anti-virus - (P) Procédure de surveillance en permanence du réseau.	Oui
Destruction involontaire des données ou des programmes	Ralentissement des objectifs de l'organisation	- (Ob) Possibilité restreinte aux données sensibles à certains utilisateurs. - (P) Procédure désignant les niveaux d'accès des utilisateurs aux données sensibles	Oui
Utilisation de matériels hors standards	Vulnérabilité du réseau du aux équipements non standards utilisés	- (Ob) Interdiction formelle d'utilisation des machines non standards sur le réseau de l'organisation - (P) Procédure claire interdisant l'utilisation des machines personnelles sur le réseau	Oui
Fraude au sein du réseau informatique	- Détournement de biens et de fonds - Sabotage du fonctionnement du réseau informatique	- (Ob) Mise en place d'un système de détection de fraude - (P) Procédure de séparation des fonctions dans l'exécution des tâches	Oui
Modification non autorisée de certains programmes	- Destruction totale ou partielle des données - Sinistre matériel	- (Ob) Mise en place d'une procédure de validation avant modification des programmes - (P) Procédure de contrôle routinier et de documentation de toutes les	Oui

		modifications	
Bombes logiques, cheval de Troie, virus, vers et les logiciels espions	- Vol des informations - Pertes des données - Neutralisation du fonctionnement du réseau	- (Ob) Mise en place d'une politique de sécurité pour endiguer toutes sortes d'attaques - (P) Procédure de veille et de contrôle de la politique de sécurité	Oui
Blocage du central téléphonique	- Communication téléphonique hors service - Rendement de l'organisation non optimal	- (Ob) Mise en place d'un système de protection du central téléphonique - (P) Procédure de surveillance de tous les appels entrants et sortants.	Oui
Remplacement de la page d'accueil du site internet par une page d'accueil d'un site pornographique	Mauvaise publicité pour l'organisation auprès de ses partenaires externes	- (Ob) Mise en place d'un système de filtrage des requêtes vers le site web de l'organisation - (P) Procédure de veille et de surveillance du site web	Oui
Indiscrétions sur des informations confidentielles de l'organisation	- Vulnérabilité de l'organisation - Concurrence déloyale	- (Ob) Interdiction formelle de divulguer des informations de l'organisation à l'extérieur - (P) Procédure de signature d'une charte par tous les employés déclarant ne pas se livrer à de telles activités délictuelles	Oui
Détournement d'informations confidentielles de l'organisation	- Vulnérabilité de l'organisation - Concurrence déloyale	- (Ob) Interdiction formelle de divulguer des informations de l'organisation à l'extérieur - (P) Procédure de signature d'une charte par tous les employés déclarant ne pas se livrer à de telles activités délictuelles	Oui
Piratage ou détournement des logiciels	- Paiement d'indemnités pouvant s'élever à 200% des prix des licences - Le défraiement des frais de procédures (frais de justice, d'huissier, d'expert judiciaire)	- (Ob) Mise en place d'un système de détection de l'utilisation de licences frauduleuses - (P) Procédure de signature d'une charte par tous les employés déclarant ne pas copier les logiciels de l'organisation	Oui

Source : Nous même

L'analyse et l'identification des risques liés au réseau informatique achevés nous passons à l'évaluation de la probabilité de leur survenance.

6.2. Evaluation des risques liés au réseau informatique

La probabilité du risque inhérent consiste à la possibilité de survenance du risque lors de l'absence de dispositif de contrôle interne. Elle sera faite de manière qualitative.

6.2.1. Evaluation de la probabilité de survenance du risque

Chaque risque est côté de 1 à 5 en fonction de ses caractéristiques toutefois les pondérations diffèrent en fonction de l'importance du facteur et varient d'une procédure à l'autre.

Tableau 6 : Echelle d'évaluation de la probabilité et de la qualité du dispositif de contrôle

Côte	Probabilité d'occurrence	Description
1	Très fiable	Quasi impossibilité que le risque se produise
2	Assez fiable	Environnement peu vulnérable
3	Fiable	Possibilité que le risque se produise
4	Peu fiable	Très grande chance que le risque se produise
5	Non fiable	Environnement extrêmement vulnérable

Source : Nous même (inspiré des approches de RENARD)

La probabilité de survenance du risque ainsi que la qualité du contrôle ont été faites dans les différents services concernés par le réseau informatique à savoir le service Finance, le service Opérations ainsi que le service Economie. Le tableau récapitulant la probabilité de survenance des risques liés au réseau informatique a été obtenu grâce à :

- des analyses documentaires ;
- des observations ;
- des entretiens ;

Le tableau ci-dessous récapitule la probabilité de survenance des risques liés au réseau informatique du PNUD Sénégal.

Tableau 7 : Evaluation de la probabilité et de la qualité du dispositif de contrôle

Risques	Qualité du dispositif		Probabilité	
	Catégorie	**Côte**	**Catégorie**	**Côte**
1. Introduction des logiciels malveillants	Peu Fiable	4	Peu Fiable	4
2. Utilisation de matériels hors standards	Peu Fiable	4	Peu Fiable	4
3. Fraude au sein du réseau informatique	Fiable	3	Fiable	3
4. Indisponibilité des serveurs	Fiable	3	Fiable	3
5. Défectuosité des équipements (switch, routeurs etc.)	Fiable	3	Fiable	3
6. Vol des matériels ou logiciels informatique	Fiable	3	Fiable	3
7. Indisponibilité du contrôleur de domaine	Fiable	3	Fiable	3
8. Mauvaise définition des GPO	Fiable	3	Fiable	3
9. Mauvaise définition des utilisateurs dans une UO	Fiable	3	Fiable	3
10. Mauvaise manipulation des équipements	Fiable	3	Fiable	3
11. Mauvaise manipulation des données	Fiable	3	Fiable	3
12 Modification non programmée de certains programmes	Fiable	3	Fiable	2
13. Vol des informations confidentielles	Fiable	3	Fiable	3
14. Non suppression d'un compte d'un employé licencié ou parti à la retraite	Fiable	3	Fiable	3
15. Mauvaise saisie des informations dans une base de données	Fiable	3	Fiable	3
16. Effacement accidentel des données ou détérioration des informations sur un support de stockage	Fiable	3	Fiable	3
17. Mauvaise définition d'une politique de sécurité	Fiable	3	Fiable	3
18. Mauvaise définition d'un système de sauvegarde	Fiable	3	Fiable	3
19. Mauvaise acquisition des logiciels et des applicatifs	Fiable	3	Fiable	3
20. Absence d'un plan de continuité des activités	Fiable	3	Fiable	3
21. Copie illicite des logiciels	Fiable	3	Fiable	3
22. Indiscrétions, détournement d'informations	Fiable	3	Fiable	3
23. Attaque logique du réseau via des vers, des virus, spywares etc.	Fiable	3	Fiable	3
24. Destruction involontaire des données ou des	Fiable	3	Fiable	3

programmes				
25. Bombes logiques, logiciels espions	Fiable	3	Fiable	2
26. Blocage du central téléphonique	Fiable	3	Fiable	3
27. Remplacement de la page d'accueil du site internet par celui d'un site pornographique	Assez fiable	2	Assez fiable	2
28. Piratage ou détournement de logiciels	Assez fiable	2	Assez fiable	2
29. Incendie dans le local technique	Assez fiable	2	Assez fiable	2
30. Foudre, tempête au sein du local technique	Assez fiable	2	Assez fiable	2
31. Coupure câble électrique	Très fiable	1	Très fiable	1

Source : Nous même

6.2.2. Evaluation de l'impact des risques

La quantification de l'impact des risques est également faite de manière qualitative. La connaissance des conséquences potentielles si le risque survenait ainsi que la détermination du niveau d'impact constitue les étapes de la démarche.

Tableau 8 : Echelle de la mesure de l'impact des risques

Côte	Probabilité d'occurrence	Description
1	Non significatif	Impact très négligeable
2	Mineur	Impact faible
3	Modéré	Conséquences modérées
4	Majeur	Conséquences fâcheuses
5	Très significatif	Conséquences extrêmement fâcheuse

Source : Nous même

L'évaluation de l'impact des risques liés au réseau informatique au sein du PNUD Sénégal se présente comme suit :

Tableau 9 : Evaluation de l'impact des risques

Risques	**Conséquences potentielles**	**Niveau d'impact**
1. Introduction des logiciels malveillants	Destruction ou vol partiel ou total des données et du matériel	Majeur
2. Utilisation de matériels hors standards	Vulnérabilité du réseau	Majeur
3. Fraude dans le réseau informatique	Détournement de biens et de fonds	Majeur
4. Indisponibilité des serveurs	Impossibilité de travailler	Majeur
5. Défectuosité des équipements (switch, routeurs etc.)	Partage non possible	Modéré
6. Vol des matériels ou logiciels informatique	Dépenses supplémentaires	Modéré
7. Indisponibilité du contrôleur de domaine	Non authentification des utilisateurs	Majeur
8. Mauvaise définition des GPO	Logiciels non disponibles	Mineur
9. Mauvaise définition des utilisateurs dans une UO	Non partage	Mineur
10. Mauvaise manipulation des équipements	Réseau informatique HS	Majeur
11. Mauvaise manipulation des données	Données supprimées	Majeur
12 Modification non programmée de certains programmes	Destruction partielle ou totale des programmes	Majeur
13. Vol des informations confidentielles	Organisation exposée à l'externe	Majeur
14. Non suppression d'un compte d'un employé licencié ou parti à la retraite	Attaques externes du réseau	Majeur
15. Mauvaise saisie des informations dans une base de données	Perte des données	Majeur
16. Effacement accidentel des données ou détérioration des informations sur un support de stockage	Perte et dommages collatéraux	Majeur
17. Mauvaise définition d'une politique de sécurité	Attaques, Sabotage	Majeur
18. Mauvaise définition d'un système de sauvegarde	Perte de données, Arrêt du travail	Majeur
19. Mauvaise acquisition des logiciels et des applicatifs	Compromission des objectifs	Modéré
20. Absence d'un plan de continuité des activités	Rupture totale et complète des activités	Très significatif
21. Copie illicite des logiciels	Poursuites pénales et sanctions financières	Mineur
22. Indiscrétions, détournement d'informations	Concurrence déloyale	Majeur
23. Attaque logique du réseau via des vers, des virus, spywares etc.	Ralentissement du réseau	Majeur
24. Destruction involontaire des données ou des programmes	Ralentissement des objectifs de l'organisation	Mineur

25. Bombes logiques, logiciels espions	Vol, Perte et Neutralisation	Majeur
26. Blocage du central téléphonique	Communication HS	Modéré
27. Remplacement de la page d'accueil du site internet par celui d'un site pornographique	Mauvaise réputation auprès de partenaires	Mineur
28. Piratage ou détournement de logiciels	Paiement d'indemnités et du matériel	Mineur
29. Incendie dans le local technique	Destruction totale des données	Très significatif
30. Foudre, tempête au sein du local technique	Destruction totale des données et du matériel	Très significatif
31. Coupure câble électrique	Réseau informatique HS	Très significatif

Source : Nous même

L'évaluation des risques de l'entreprise faite, la prochaine étape consiste en la hiérarchisation des risques liés au réseau informatique.

6.3. Hiérarchisation des risques

L'appréciation du niveau des risques permet de les classer et de les hiérarchiser. Les risques liés au réseau informatique au sein du PNUD Sénégal seront présentés dans le tableau ci-dessous

6.3.1. Hiérarchisation des risques selon leur probabilité de survenance

Le tableau ci-dessous représente la hiérarchisation des risques selon leur probabilité

Tableau 10 : Hiérarchisation des risques selon leur probabilité de survenance

Risques	**Qualité du dispositif**		**Probabilité**	
	Catégorie	**Côte**	**Catégorie**	**Côte**
1. Introduction des logiciels malveillants	Peu Fiable	4	Peu Fiable	4
2. Utilisation de matériels hors standards	Peu Fiable	4	Peu Fiable	4
3. Fraude dans le réseau informatique	Fiable	3	Fiable	3
4. Indisponibilité des serveurs	Fiable	3	Fiable	3
5. Défectuosité des équipements (switch, routeurs etc.)	Fiable	3	Fiable	3
6. Vol des matériels ou logiciels informatique	Fiable	3	Fiable	3

7. Indisponibilité du contrôleur de domaine	Fiable	3	Fiable	3
8. Mauvaise définition des GPO	Fiable	3	Fiable	3
9. Mauvaise définition des utilisateurs dans une UO	Fiable	3	Fiable	3
10. Mauvaise manipulation des équipements	Fiable	3	Fiable	3
11. Mauvaise manipulation des données	Fiable	3	Fiable	3
12 Modification non programmée de certains programmes	Fiable	3	Fiable	2
13. Vol des informations confidentielles	Fiable	3	Fiable	3
14. Non suppression d'un compte d'un employé licencié ou parti à la retraite	Fiable	3	Fiable	3
15. Mauvaise saisie des informations dans une base de données	Fiable	3	Fiable	3
16. Effacement accidentel des données ou détérioration des informations sur un support de stockage	Fiable	3	Fiable	3
17. Mauvaise définition d'une politique de sécurité	Fiable	3	Fiable	3
18. Mauvaise définition d'un système de sauvegarde	Fiable	3	Fiable	3
19. Mauvaise acquisition des logiciels et des applicatifs	Fiable	3	Fiable	3
20. Absence d'un plan de continuité des activités	Fiable	3	Fiable	3
21. Copie illicite des logiciels	Fiable	3	Fiable	3
22. Indiscrétions, détournement d'informations	Fiable	3	Fiable	3
23. Attaque logique du réseau via des vers, des virus, spywares etc.	Fiable	3	Fiable	3
24. Destruction involontaire des données ou des programmes	Fiable	3	Fiable	3
25. Bombes logiques, logiciels espions	Fiable	3	Fiable	2
26. Blocage du central téléphonique	Fiable	3	Fiable	3
27. Remplacement de la page d'accueil du site internet par celui d'un site pornographique	Assez fiable	2	Assez fiable	2
28. Piratage ou détournement de logiciels	Assez fiable	2	Assez fiable	2
29. Incendie dans le local technique	Assez fiable	2	Assez fiable	2
30. Foudre, tempête au sein du local technique	Assez fiable	2	Assez fiable	2
31. Coupure câble électrique	Très fiable	1	Très fiable	1

Source : Nous même

6.3.2. Hiérarchisation des risques selon leur impact

Le tableau ci-dessous représente la hiérarchisation des risques selon leur impact

Tableau 11 : Hiérarchisation des risques selon leur impact

Risques	Conséquences potentielles	Niveau d'impact
20. Absence d'un plan de continuité des activités	Rupture totale et complète des activités	Très significatif
29. Incendie dans le local technique	Destruction totale des données et du matériel	Très significatif
30. Foudre, tempête au sein du local technique	Destruction totale des données et du matériel	Très significatif
31. Coupure câble électrique	Réseau informatique HS	Très significatif
1. Introduction des logiciels malveillants	Destruction ou vol partiel ou total des données et du matériel	Majeur
2. Utilisation de matériels hors standards	Vulnérabilité du réseau	Majeur
4. Indisponibilité des serveurs	Impossibilité de travailler	Majeur
7. Indisponibilité du contrôleur de domaine	Non authentification des utilisateurs	Majeur
10. Mauvaise manipulation des équipements	Réseau informatique HS	Majeur
11. Mauvaise manipulation des données	Données supprimées	Majeur
12 Modification non programmée de certains programmes	Destruction partielle ou totale des programmes	Majeur
13. Vol des informations confidentielles	Organisation exposée à l'externe	Majeur
14. Non suppression d'un compte d'un employé licencié ou parti à la retraite	Attaques externes du réseau	Majeur
15. Mauvaise saisie des informations dans une base de données	Perte des données	Majeur
16. Effacement accidentel des données ou détérioration des informations sur un support de stockage	Perte et dommages collatéraux	Majeur
17. Mauvaise définition d'une politique de sécurité	Attaques, Sabotage	Majeur
18. Mauvaise définition d'un système de sauvegarde	Perte de données, Arrêt du travail	Majeur
22. Indiscrétions, détournement d'informations	Concurrence déloyale	Majeur
23. Attaque logique du réseau via des vers, des virus, spywares etc.	Ralentissement du réseau	Majeur
25. Bombes logiques, logiciels espions	Vol, Perte et Neutralisation	Majeur
3. Fraude dans le réseau informatique	Détournement de biens et de fonds	Majeur
26. Blocage du central téléphonique	Rendement de l'organisation non	Modéré

	optimal	
5. Défectuosité des équipements (switch, routeurs etc.)	Partage non possible	Modéré
6. Vol des matériels ou logiciels informatique	Dépenses supplémentaires	Modéré
19. Mauvaise acquisition des logiciels et des applicatifs	Compromission des objectifs	Modéré
8. Mauvaise définition des GPO	Logiciels non disponibles	Mineur
9. Mauvaise définition des utilisateurs dans une UO	Non partage	Mineur
21. Copie illicite des logiciels	Poursuites pénales et sanctions financières	Mineur
24. Destruction involontaire des données ou des programmes	Ralentissement des objectifs de l'organisation	Mineur
27. Remplacement de la page d'accueil du site internet par celui d'un site pornographique	Mauvaise réputation auprès de partenaires	Mineur
28. Piratage ou détournement de logiciels	Paiement d'indemnités et du matériel	Mineur

Source : Nous même

6.4. Elaboration de la cartographie des risques liés au réseau informatique

Le risque identifié, évalué, hiérarchisé, nous allons dresser la matrice des risques liés au réseau informatique au sein du PNUD Sénégal.

Figure 17 : Matrice des risques liés au réseau informatique au sein du PNUD Sénégal

PROBABILITE	Non significatif	Mineur	Modéré	Majeur	Très significatif
Non fiable					
Peu fiable				1. Introduction des logiciels malveillants **2**. Utilisation de matériels hors standards	
Fiable		8. Mauvaise définition des GPO 9.Mauvaise définition des utilisateurs dans une UO 21. Copie illicite des logiciels 24. Destruction involontaire des données ou des programmes	5.Défectuosité des équipements (switch, routeurs etc.) 6. Vol des matériels ou logiciels informatique 19. Mauvaise acquisition des logiciels et des applicatifs 26. Blocage du central téléphonique	3. Fraude dans le réseau informatique 4. Indisponibilité des serveurs 7. Indisponibilité du contrôleur de domaine 10. Mauvaise manipulation des équipements 11. Mauvaise manipulation des données 12 Modification non programmée de certains programmes 13. Vol des informations confidentielles 14. Non suppression d'un compte d'un employé licencié ou parti à la retraite 15. Mauvaise saisie des informations dans une base de données 16. Effacement accidentel des données ou détérioration des informations sur un support de stockage 17. Mauvaise définition d'une politique de sécurité 18. Mauvaise définition d'un système de sauvegarde 22. Indiscrétions, détournement d'informations 23. Attaque logique du réseau via des vers, des virus, spywares etc. 25. Bombes logiques, logiciels espions	20. Absence d'un plan de continuité des activités
Assez fiable		27. Remplacement de la page d'accueil du site internet par celui d'un site pornographique 28. Piratage ou détournement de logiciels			29. Incendie dans le local technique 30. Foudre, tempête au sein du local technique
Très fiable					31. Coupure câble électrique

IMPACT

Echelle :

RISQUES FAIBLES
RISQUES MOYENS
RISQUES MAJEURS
RISQUES ELEVES

6.5. Les plans d'action

Les plans d'actions doivent être mis en place afin de ramener les niveaux de risque forts à des niveaux acceptables ou risques cibles. Le tableau ci-dessous présente les propositions de plan d'action que nous avons conçu.

Tableau 11 : Proposition de plan d'action

Risques	Actions	Moyens
1. Introduction des logiciels malveillants	Scanner tout le réseau, Méthode de purification	Firewall, Serveur Anti virus et Antispyware
2. Utilisation de matériels hors standards	Non accessible au réseau informatique	Mise en place d'un système pour la détection de matériels non standards
20. Absence d'un plan de continuité des activités	Rédiger et faire participer toutes les entités de l'organisation	Mise en place d'un système de continuité des activités
29. Incendie dans le local technique	Vérifier tous les éléments pouvant causer un incendie	Mise en place d'un dispositif anti incendie
30. Foudre, tempête au sein du local technique	Vérifier le bon fonctionnement du matériel	Mise en place d'un système de parafoudre et paratonnerre
31. Coupure câble électrique	Vérifier par un expert l'état des câbles électriques	Dispositif d'accès sécurisé au câble électrique
3. Fraude dans le réseau informatique	Vérifier le bon fonctionnement du système	Mise en place d'un système de détecteur de fraude sur le réseau
4. Indisponibilité des serveurs	Faire un backup journalier des données des serveurs	Mise en place d'un système de redondance
5. Défectuosité des équipements (switch, routeurs etc.)	Vérifier si disponibilité il y a, sinon passer la commande	Disponibilité des équipements en stock
6. Vol des matériels ou logiciels informatique	Faire l'inventaire physique de tous les matériels et logiciels	Dispositif d'anti vol pour le matériel et verrouillage de tous les codes des logiciels
7. Indisponibilité du contrôleur de domaine	Faire un backup journalier des données des serveurs	Mise en place d'un système de redondance

10. Mauvaise manipulation des équipements	Manipulation des équipements suite à un document de validation	Mise en place d'un système de validation pour la manipulation des équipements
11. Mauvaise manipulation des données	Manipulation des données suite à un document de validation	Mise en place d'un système de validation pour la manipulation des données
12 Modification non programmée de certains programmes	Modification des programmes suite à un document de validation de la hiérarchie	Mise en place d'un système de validation pour la modification des programmes
13. Vol des informations confidentielles	Les infos confidentielles sont sous la responsabilité d'une personne connue de tous	Mise en place d'un dispositif anti vol des infos confidentielles
14. Non suppression d'un compte d'un employé licencié ou parti à la retraite	Suppression automatique	Mise en place d'un système d'alerte pour une désactivation
15. Mauvaise saisie des informations dans une base de données	Vérifier toutes les infos avant de les saisir dans la base de données par 2 personnes de départements différents	Mise en place d'un système de rejet si les informations sont inexactes
16. Effacement accidentel des données ou détérioration des informations sur un support de stockage	Supports de stockage sont mis dans un coffre fort fermé	Dispositif de coffre fort pour une bonne sauvegarde des données
17. Mauvaise définition d'une politique de sécurité	Vérifier la politique de sécurité par rapport aux recommandations du siège	Politique de sécurité du siège à new York
18. Mauvaise définition d'un système de sauvegarde	Vérifier le système de sauvegarde par rapport aux recommandations du siège	Système de sauvegarde du siège à new York
19. Mauvaise acquisition des logiciels et des applicatifs	Suivre les standards pour l'acquisition des logiciels	Documents du siège pour l'acquisition des logiciels
22. Indiscrétions, détournement d'informations	Faire signer une clause de confidentialité à tous les employés	Contrats
23. Attaque logique du réseau via des vers, des virus, spywares etc.	Surveiller le réseau pour détecter des attaques éventuelles	Firewalls
25. Bombes logiques, logiciels espions	Surveiller le réseau pour détecter des attaques éventuelles	Firewalls

26. Blocage du central téléphonique	Vérifier de temps en autre le bon fonctionnement du central	Système de secours : mise en place des téléphones IP
8. Mauvaise définition des GPO	Vérifier la définition des GPO par rapport aux documents de référence utilisés par le siège	Document de définition des GPO utilisé au siège à new York
9. Mauvaise définition des utilisateurs dans une UO	Vérifier la définition des utilisateurs au sein des UO par rapport aux documents de référence utilisés par le siège	Document de définition des utilisateurs dans les UO utilisé au siège à new York
21. Copie illicite des logiciels	Fermer toutes les issues pour la copie des logiciels. Sécuriser les licences pour les logiciels	Mise en place d'un système de détection de copie des logiciels
24. Destruction involontaire des données ou des programmes	Vérifier le système d'accès pour les différents programmes	Mise en place de validation avant d'avoir accès à ces programmes

Source : Nous même

6.6. Analyse de la cartographie des risques

Le niveau des risques et la qualité du contrôle interne pourront être connus par les dirigeants du PNUD Sénégal grâce à la cartographie. Cette dernière a permis de déceler des risques élevés et majeurs dont la réponse devait être amenée par une réponse rapide des dirigeants qui devront renforcer les dispositifs de contrôle interne ; des risques moyens qui nécessitent un suivi régulier afin de les ramener à un niveau faible ou les stabiliser à leur niveau actuel et enfin les risques faibles.

La cartographie des risques liés au réseau informatique du PNUD Sénégal a permis de faire ressortir trois catégories de risques

La première catégorie de risques comprend les risques « élevés » et « majeurs » qui est constitué par les risques se trouvant dans la partie de la matrice ayant les couleurs rouge et jaune brun. Les risques qui s'y trouvent nécessitent que des actions rapides soient menées par les dirigeants en vue de les réduire considérablement ou de les ramener à un niveau acceptable.

La seconde catégorie de risques comprend les risques dits moyens qui sont des risques se trouvant dans la partie de la matrice coloriée en jaune. Ces risques sont sujets à des mesures de contrôle acceptable et nécessitent un suivi régulier de la part des dirigeants.

La troisième catégorie de risques identifiés sont constitués des risques dits « faibles » ; ils sont sujets à des mesures de contrôle adéquates et ne méritent pas de commentaires particuliers vus la mise sous contrôle des risques en plus de leur niveau faible.

La cartographie analysée, nous achèverons notre travail par les recommandations relatives aux différents risques liés au réseau informatique du PNUD Sénégal.

6.7. Recommandations

Les risques étant cartographiés, nous procédons à la formulation de recommandations à l'endroit des différents acteurs afin de mieux maitriser les risques liés au réseau informatique du PNUD Sénégal.

- Nous recommandons vivement de mettre en place un système de détection et de supervision de tout le réseau informatique à savoir un firewall, un système anti virus et anti spyware.
- Nous recommandons la mise en place d'un système de détection des machines non standards au réseau informatique du Sénégal.
- Nous recommandons vivement au PNUD Sénégal l'élaboration et la divulgation d'un plan de continuité des activités.
- Nous recommandons de mettre en place un système de détecteur d'incendie et de fumée, un paratonnerre dans les locaux techniques.
- Nous recommandons également que l'accès aux locaux techniques soit strictement réservé aux personnes qui ont des compétences dans le domaine de l'informatique.
- Nous recommandons un suivi journalier ou hebdomadaire de la disponibilité des matériels informatiques en stock.
- Nous recommandons la mise en place d'un système d'antivol pour le matériel informatique et d'un système de verrouillage des programmes ou logiciels informatiques.
- Nous recommandons expressément la mise en place d'un système de redondance pour tous les serveurs opérant dans le réseau informatique du PNUD Sénégal.
- Nous recommandons la mise en place d'un système de validation pour une modification à opérer sur un programme ou une intervention sur un équipement informatique.

- Nous recommandons la mise en place d'un système d'alerte et de veille pour la purification de la base de données des utilisateurs ou des équipements.
- Nous recommandons la mise en place d'un système de politique de sécurité en adéquation avec les besoins du réseau informatique du PNUD Sénégal.
- Nous recommandons de mettre en place une sauvegarde incrémentale qui est très efficace et moins couteuse en temps et qui soit en adéquation avec les besoins du PNUD Sénégal et conforme aux recommandations venues du Siège.
- Nous recommandons de mettre en place un comité pour le choix et la validation des achats de matériels ou des logiciels informatique.
- Nous recommandons de faire signer aux employés une charte de confidentialité et de discrétion des informations liés au réseau informatique du Sénégal.
- Nous recommandons de mettre en place un système de téléphonie classique et un système de téléphonie sur IP pour assurer la redondance.
- Nous recommandons de verrouiller tous les accès aux medias externes pour la copie des informations

Conclusion de la deuxième partie

Cette deuxième partie a été l'occasion de présenter le PNUD Sénégal, l'organisation, l'architecture du réseau informatique, et de les analyser. Les informations reçues ont permis la mise en œuvre de notre démarche référentielle et l'élaboration de la cartographie des risques liés au réseau informatique du PNUD Sénégal.

La cartographie des risques liés au réseau informatique permettra au PNUD Sénégal d'améliorer certaines défaillances constatées et d'y faire face.

CONCLUSION GENERALE

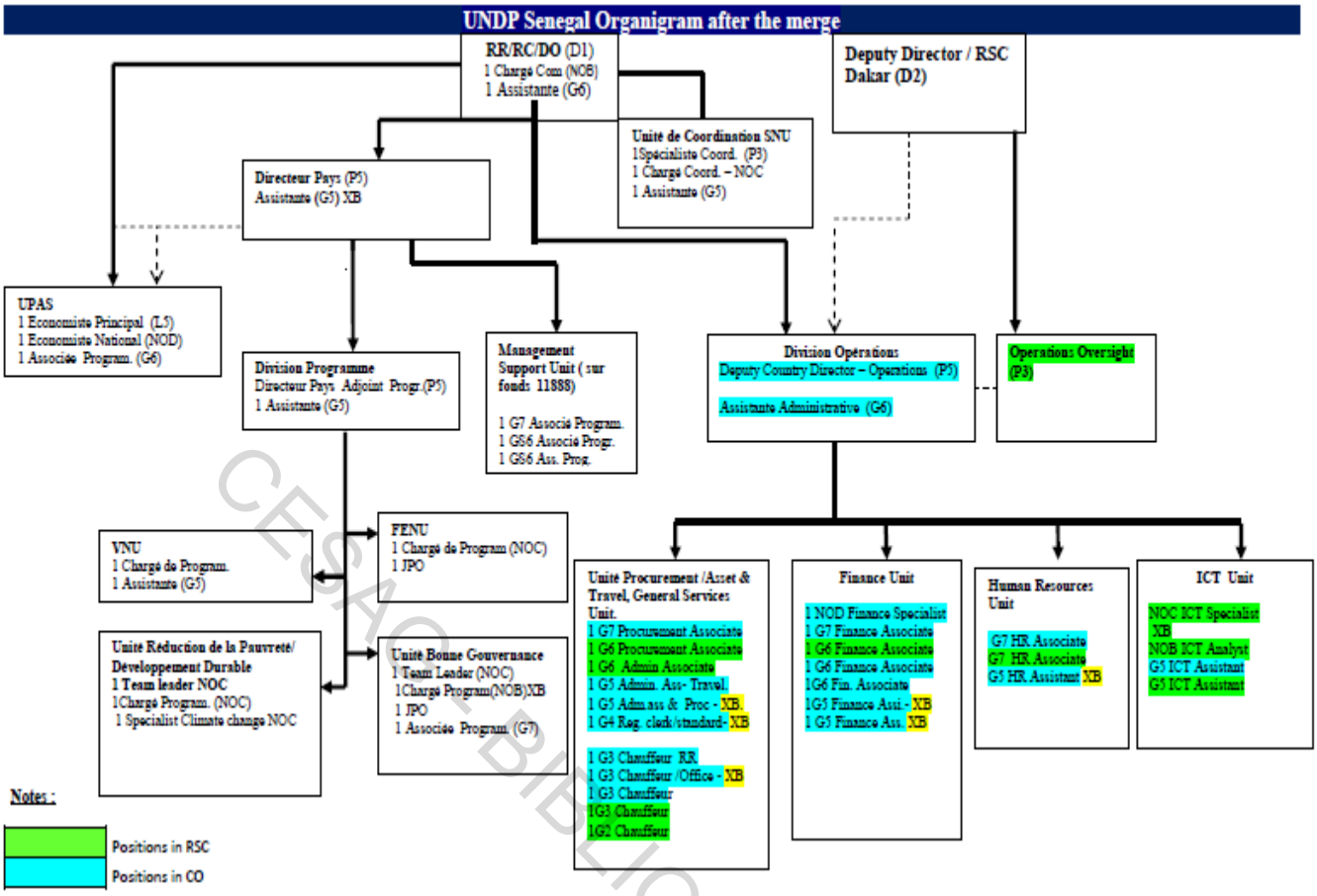
Ce travail s'achève par l'élaboration de la cartographie des risques liés au réseau informatique du PNUD Sénégal. Le réseau informatique est la pierre angulaire de l'organisation et nécessite à ce titre une attention particulière. Les risques liés au réseau informatique peuvent entrainer de nombreuses conséquences telles de mauvaises performances et la disparition de l'entreprise ; aussi il s'avère important de les maîtriser. Ainsi l'un des outils modernes utilisés pour faire face aux risques liés au réseau informatique est la cartographie des risques.

Point de départ presque incontournable, la cartographie des risques est l'outil le plus efficient pour effectuer un inventaire et une évaluation des risques. D'ailleurs, sa mise en place est recommandée par certains travaux de référence comme les travaux du comité de Bâle (2003). La cartographie peut être intégrée à une démarche de gestion plus globale qui favorise l'amélioration des performances de l'organisation. Sa conception ou son élaboration devrait être l'œuvre du risk manager pour les organisations qui en possèdent, dans le cas contraire elle est l'œuvre de l'audit interne.

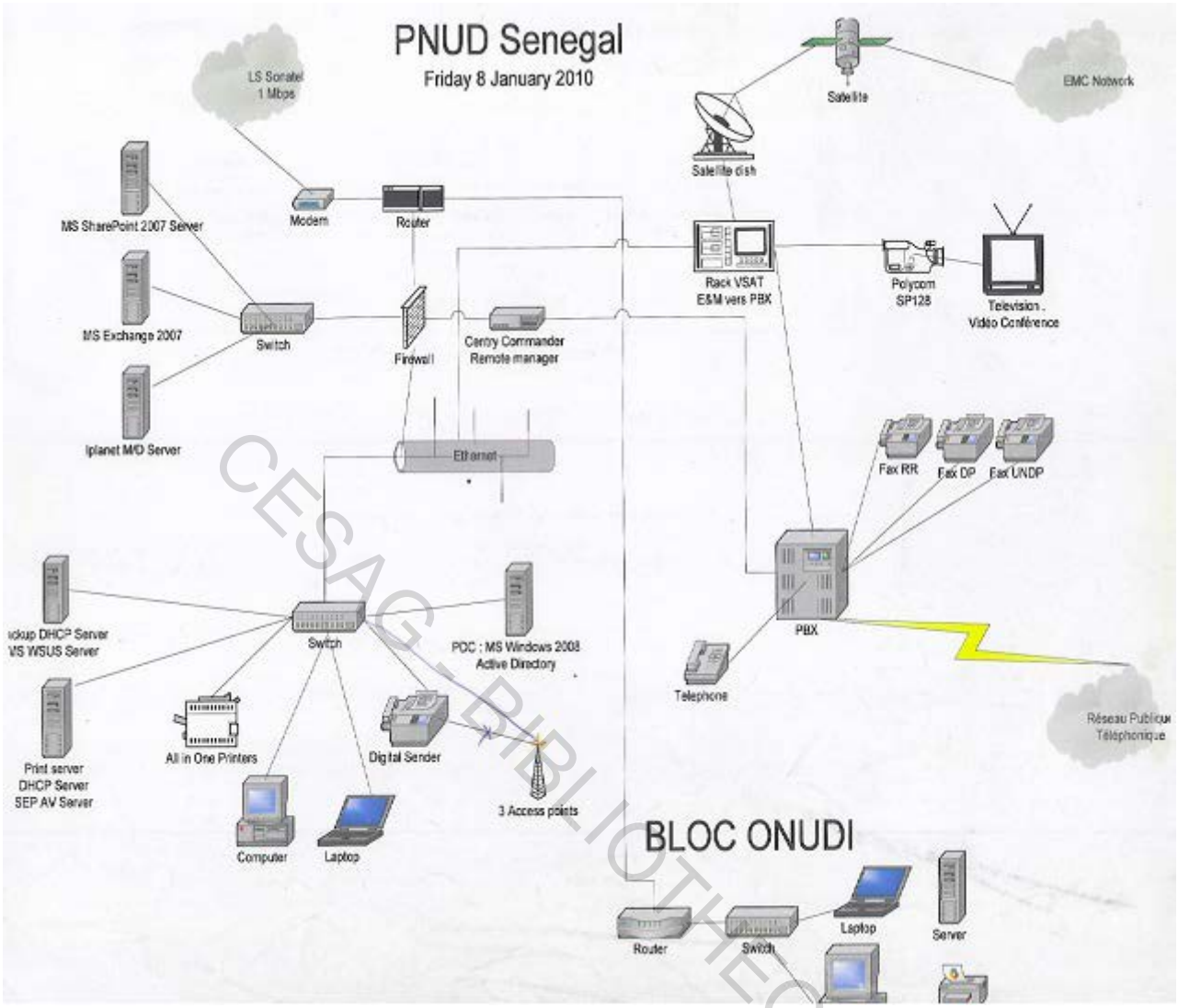
Notre étude nous a permis de souligner les étapes à suivre dans la conception d'une cartographie des risques et sa mise en œuvre à travers notre démarche référentielle. Nous avons ainsi pu identifier, analyser, hiérarchiser les risques en fonction de leur probabilité de survenance et de leur impact. Cette étude a permis une visualisation des risques liés au réseau informatique du PNUD Sénégal, la mise en place de plans d'actions en vue d'éliminer ou de réduire les risques liés au réseau informatique et l'énonciation des recommandations relatives aux différents risques liés au réseau informatique.

ANNEXES

Annexe 1 : Organigramme du PNUD Sénégal



Annexe 2 : Architecture du réseau informatique du PNUD Sénégal



BIBLIOGRAPHIE

Ouvrages

1. ANDREW S. Tanenbaum, David J. Wetherall (2010), Computer Networks, 5th Edition, 960 Pages – Etats Unis d'Amerique – Editeurs: Prentice Hall
2. BARROIN & al. (2002), Vers un risque opérationnel mieux géré et mieux contrôlé
3. CLAUDE Servin (2013), Réseaux Et Télécoms Paris - Dunod 4ème édition - 304 pages
4. COOPERS & LYBRAND (2000), La nouvelle pratique du contrôle interne, Edition d'organisations¸ Paris, P.378
5. DAN Holme, NELSON Ruest, DANIELLE Ruest (2008), Configuration d'une infrastructure Active Directory avec Windows Server - Microsoft Press - Paris, - 976 pages
6. DE MARESCHALL Gilbert (2003), La cartographie des risques, Edition AFNOR, Paris. P.45
7. DESROCHES Alain, LEROY Alain & VALLEE Frédérique (2003), La gestion des risques : principes & pratiques, Lavoisier, P.105-110.
8. DESROCHES Alain, LEROY Alain, VALLEE Frédérique Hermès - Lavoisier (2007), La gestion des risques Principes et pratiques, 2e édition, 298 pages – France - Editeur(s) : Hermès – Lavoisier
9. DORDOIGNE José (2013), Réseaux Informatiques, Maîtrisez Les Fondamentaux - Coffret 2 Volumes : Réseaux Informatiques, Notions Fondamentales - Les Réseaux : Administrez Un Réseau Sous Windows Ou Sous Linux Editions Eni , Paris
10. DORDOIGNE José (2005), Réseaux Locaux Et Étendus - Notions Fondamentales Editions Eni - Paris
11. ERIC Larcher (2000), L'Internet Sécurisé , Eyrolles, 450 pages - Paris
12. HAMZAOUI, Mohamed & PIGE, Benoît (2005), Audit : gestion des risques d'entreprise et contrôle interne : normes ISA 200, 315, 330 et 500, Paerson Education, Paris, 243 P.
13. Kenneth Lindup (1999), The Computer Security And Fraud Prevention Audit Pearson Education Limited- United States of America

14. MC NAMEE, David (1998), Business risk assessment, The Institute of Internal Auditors, Altamonte Spring, P.107
15. MOREAU, Franck (2002), Comprendre et gérer les risques, Editions d'organisations, Paris. P.222
16. NUSSBAUMER H., Téléinformatique, Presses Polytechniques romandes, 1987. Chapitre 1.3.
17. PHILIP, Laurent & al. (1991), Pratique de l'audit opérationnel : pour une dynamique de progrès dans l'entreprise, Edition d'organisation, Paris
18. PUJOLLE Guy, Les Réseaux, 8ème Edition, 1000 pages - Eyrolles - Paris
19. RENARD, Jacques (2002), Théorie et pratique de l'audit interne, 4ème édition, Edition d'organisation, Paris, P.462.
20. RENARD, Jacques (2005), Théorie et pratique de l'audit interne, 4ème édition, Editions d'organisation, Paris. P. 462
21. RENARD, Jacques (2006), Théorie et pratique de l'audit interne, 6ème édition, Edition d'organisation, Paris
22. RENARD, Jacques (2008), théorie et pratique de l'audit interne, 6ème édition, Editions d'organisation, Paris, 479 Pages
23. SANDRA Senft (2008), Information Technology Control And Audit - Auerbach Pubn – 2nd edition (2008) – United States of America
24. SOLANGE Ghernaouti-Hélie (2008), Sécurité Informatique Et Réseaux Dunod –Paris
25. SUTTON Stephen A. (1996), Windows NT Security Guide- Addisson-Weslsy - Boston

Articles

26. BAPST, Pierre-Alexandre & BERGERET, Florence (2002), Pour un management des risques orientés vers la protection de l'entreprise et la création de la valeur, Revues Françaises de l'Audit Interne, n°162, P.30-33
27. LECLERC, Hélène, D'ALDRAND, Guy, POTVIN, Kim-Andrée & RICARDO, Alexandre (2003), le risk assessment: quelques bonnes pratiques, Revues Françaises de l'Audit Interne, n°163, P.6

28. MATTE, Paul Henri (2003), Un outil de gestion : la cartographie des risques à la régie des rentes du QUEBEC, Revues Françaises de l'Audit Interne, n°167, P.39.-40
29. POULIOT, Daniel & BILODEAU, Yves (2002), Mesurer les risques en vue de les contrôler et de les gérer : l'approche matricielle des pertes, Revue Française de l'Audit Interne, n°161, P.36-37 ;

Sources Internet

30. AFAI- Formes et méthodologies d'audit de la sécurité informatique www.afai.fr/public/doc/84.doc
31. COBIT, Socle de la gouvernance des SI http://home.nordnet.fr/~ericleleu/cours/cobit/cobit.pdf
32. FONTUGNE, Muriel (2001), Cartographie des risques: Quelle valaur ajoutée? Quel processus ? www.amrae.asso.fr/les rencontres/Lille2002/actes/p10/p10.Fontugne.pdf
33. INGRAM, David, Best practices for the risk mapping process, www.milliman.com/pubs/life/content/research reports/ best practices risk mapping RR 07 01 04. Pdf
34. www.undp.org.sn