CESAG

Centre Africain d'études Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF)

Diplôme d'Etudes Supérieures Spécialisées en Audit et Contrôle de Gestion

Promotion 22 (2010-2011)

Mémoire de fin d'étude

THEME

Audit de la sécurité des données informatiques : cas de la Société Nationale d'Electricité Congo-Brazzaville

Présenté par :

MOUAMANA SOUAMI Hugues

Dirigé par :

M. Alain SAWADOGO
PROFESSEUR ASSOCIE
CESAG

012

REMERCIEMENTS

J'adresse mes sincères remerciements à :

- Monsieur PELLA Albert Camille, Directeur général de la SNE pour nous avoir permis d'effectuer notre stage de fin d'étude dans leur structure.
- Monsieur SAWADOGO Alain pour l'encadrement de ce mémoire, pour ses conseils et le temps qu'il m'a accordé pour la réalisation de ce mémoire.
- Mon Grand frère SANCE Roland et sa femme SANCE Laudra pour le soutien et les encouragements qu'ils ne cessent de manifester en vers moi.
- Monsieur YAZI Moussa Directeur de l'Institut Supérieur de la Comptabilité pour son soutien considérable et ses conseils dans la réalisation du présent mémoire de fin d'études, le corps professoral et administratif du CESAG pour le service rendu.
- L'ensemble du personnel de la SNE pour leur collaboration.
- Mes sœurs et frères MOUAMANA Julie, MOUAMANA Rose, MAKOYE Brigitte, MAMPASSI Jean, MOUAMANA Eddie, MOUAMANA Simplice pour leur contribution à ma formation.
- Mes nièces, fils et neveux MABARI Belfruit, Ngoulou Arsène, MOUAMANA Adrich, NZABA Rophel, MOUAMANA Richy, MABARI MOUAMANA Cheril.
- Mes grands frères et amis AMBOULOU Alfred, MOKANGA Sylvain, LOUBASSOU Moïse, KEITA Souleymane, feu TCHIMBAKALA Bertin pour le soutien et le réconfort.
- Mes camarades de la promotion.
- La communauté congolaise au CESAG.

Et tous ceux qui de près ou de loin ont contribué à la réalisation de ce travail.

SIGLES ET ABREVIATIONS

ACISSI : Audit, Conseil, Installation et Sécurisation des Systèmes Informatiques

AFAI : Association Française de l'Audit et du Conseil Informatique

CA: Chiffre d'affaire

CMMI: Capability Maturity Model Integrated

COBIT: Control Objectifs for Information Technologie

COSO: Committee Of Sponsoring Organization of the Treadway Commission

CLUSIF : Club de la Sécurité des Systèmes d'Information Français

DAS : Direct Attached Storage,

EBIOS : Expression des besoins et identification des objectifs de sécurité

FAR : Feuille d'analyse des risques

FRAP : Feuille de révélation d'anomalie et de problèmes

GDC: Gestion de la Clientèle

GRH: Gestion des ressources Humaines

GRHS: Gestion des ressources humaines -Solde

IBM : International business Machines

IFACI : Institut Français de l'Audit et du Contrôle Internes

IP: Internet protocol

ISACA: Information systems Audit and Control Association

ISO: International Organisation for Standardization

ITIL: Information Technology Infrastrusture Librery

LAN: Local Area Network

MEHARI : Méthode Harmonisée d'Analyse des risques

MW: Mégawatts,

NAS: Network Attached Storage

OHADA : Organisation pour l'Harmonisation en Afrique du Droit des Affaires

PC: Personal Computer

RAID: Redundant Array of Inexpensive Disk

SAN: Storage Area Network

SANS: SysAdim Audit Network Security

SCSI: Small Computer System Interface

S.E.E.E : Société Equatoriale d'Energie Electrique

SGBD: Système de gestion de base des données

SMI : Société de Marketing Industriel

SNE : Société Nationale d'électricité

SoA: Statement of applicability

SoIP: Statement of Internet Protocol

UNELCO : Union Electrique d'Outre Mer en sigle

USB: Universal Serial Bus

WAN: Wide Area Network

Y2K: Year 2 kilos

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

Au cours des dernières années, la mondialisation, spécialement sous ses aspects économiques et financiers, a engendré des projets informatiques de dimension mondiale. On notera en particulier le passage informatique à l'an 2000 (Y2K), qui a nécessité la vérification et la conversion de 300 à 600 milliards de lignes de programme potentiellement affectées dans le monde (estimation du Gartner Group).

En Europe, le chantier du passage à l'euro a représenté un coût sensiblement équivalent à celui du passage à l'an 2000 sur le périmètre européen. Le projet s'est déroulé en deux phases : première phase début 1999 avec le passage à l'euro des marchés financiers et des applications financières des entreprises, deuxième phase, de loin la plus importante, la conversion de la plupart des autres applications informatiques, qui ne put s'effectuer en général qu'en 2000 et 2001, pour des questions de contraintes par rapport au passage informatique à l'an 2000 (Y2K), et par rapport aux exercices comptables. Dans ces deux projets, les exigences d'interopérabilité et les données informatiques ont joué un rôle essentiel, puisqu'il s'agissait du format des champs date (une métadonnée) et devise dans les systèmes et les enregistrements informatiques.

Les enjeux de la sécurité des données sont les suivants: la protection de la vie privée, la sécurité des données enregistrées sur le disque dur du micro-ordinateur (courriels, répertoires, fichiers documents, données des tableurs et des présentations…), le cihlage des parties prenantes internes et externes en fonction de leurs intérêts, l'identification des données nécessaires aux procédures de protection de la santé des employés, la protection du capital intellectuel de l'entreprise, l'identification des marchés sensibles, la sécurisation des données issues de la veille en entreprise. La sécurité des données implique certaines façons de les structurer. D'où l'utilisation de systèmes de stockage (SAN et NAS). C'est au regard de la criticité liée aux données informatiques que nous avons choisi pour thème « **Audit de la sécurité des données informatiques : Cas de la société S.N.E** »

Les données informatiques constituent l'essentiel de l'information dans l'entreprise, elles sont l'une des ressources les plus précieuses des entreprises. Tout comme les autres actifs vitaux, elles doivent être protégées. Toute faille de sécurité à ce niveau peut entraîner des préjudices majeurs pour les entreprises concernées.

Selon HENRI (2005 :123) « le problème de sécurité devient crucial : sécurité pour la protection des patrimoines et biens de l'entreprise, pour la protection contre les vols, les sabotages et l'espionnage industriel ». Ainsi, l'entreprise doit assurer l'intégrité de l'information qu'elle a stockée, aussi elle doit préserver la confidentialité de cette information car les risques d'accès ou de détérioration de ses données sont de plus nombreux.

L'explosion des délits informatiques est due au développement de l'informatique repartie et de l'informatique mobile, à l'émergence de l'internet. Selon un rapport de Ponemon institute publié en 2008, le préjudice moyen résultant d'un incident isolé peut atteindre plusieurs millions de dollars. Les sociétés basées aux États-Unis sont les plus affectées : chaque brèche de sécurité informatique leur coûtant en moyenne 6,6 millions de dollars. Les sociétés anglaises et allemandes s'en sortent un peu mieux, chaque incident de ce type se traduisant respectivement par un préjudice moyen de 1,73 million de livres sterling et 2,41 millions d'euros, (in DEVICE LOCK Inc, Proactive Network Security : 2009) . Cela représente une charge financière énorme. Les fuites de données sont ainsi devenues l'une des premières priorités des services en charge de la sécurité informatique en entreprises.

La sécurité des données s'intéresse à l'intégrité, la confidentialité, la disponibilité, et la fiabilité. Elle concerne la destruction ou l'intrusion des outils, matériels logiques, de stockage, suite aux manipulations des données, des malveillances, des erreurs d'utilisation, des accidents. Ainsi, force est de constater comme le mentionne Alexei Lesnykh (2009), « la diffusion de données confidentielles et sensibles n'a jamais été aussi simple. Les périphériques de stockage amovibles compliquent la tâche des professionnels de la sécurité ».

La modernisation des équipements informatiques, l'activité humaine exposent la S.N.E aux risques de perte de données et font accroitre la probabilité de matérialisation des risques liés à l'informatique (vol des données, sabotage, destruction des données ou du système informatique, ...). De plus, l'importance des activités et le secteur d'activité où évolue la S.N.E, fait qu'elle gère des données ou informations importantes. Elle voit peser sur elle la menace de cybercriminalité, vol, destruction, etc. Ces attaques peuvent survenir sur le site informatique ou viser les données et les applications. Ces attaques sont l'œuvre d'individus ou organisations malveillants. Ces faits font augmenter la probabilité qu'un risque majeur se matérialise et menace l'intégrité, la disponibilité des données ou des informations.

Notons que la sécurité des données informatiques (sécurité informatique) peut être aussi mal assurée à cause des faits suivants :

- L'absence d'un Risk Manager ;
- l'absence d'un responsable de la sécurité informatique ;
- le manque de contrôle d'accès aux locaux informatiques ;
- l'ignorance de certains risques informatiques pouvant affecter les données informatiques ou informations ;
- l'absence d'une unité d'Audit interne pour évaluer la sécurité informatique ;
- le cumul des taches incompatibles au sein du service informatique ;
- l'absence d'une charte de sécurité informatique.

Les conséquences qui découlent des problèmes ci-dessus et qui peuvent toucher la S.N.E sont les suivantes :

- la perte des données ou informations ;
- la divulgation des informations confidentielles ;
- la non maitrise des risques informatiques ;
- des couts supplémentaires pour remplacement du matériel informatique qui pourrait être endommagé, détruit ou volé ;
- l'indisponibilité du système d'information.

Pour atteindre un niveau de sécurité adéquat des données informatiques les entreprises se doivent d'avoir :

- une organisation optimale répondant aux besoins du contrôle interne ;
- un bon pilotage de cette organisation et un suivi régulier ;
- un bon contrôle de la mise en œuvre des exigences de sécurité ;
- limiter l'accès à certaines données ou information ;
- un bon suivi du système de stockage des données à travers des audits informatiques réguliers.

Cette dernière activité constitue un élément clé de la sécurisation d'un système de stockage de données informatiques ou d'informations. L'audit des systèmes de stockage de données évalue l'exposition de l'entreprise aux sinistres informatiques. Des éléments de l'audit de la sécurité sont l'évaluation des risques informatiques liés à la sécurité physique du

système de stockage des données informatiques, à la sécurité logique, à la gestion des changements, à la continuité de l'activité, etc.

La principale question qui découle de ce qui précède est la suivante : Comment atteindre un niveau de sécurité optimal du système de stockage des données informatiques? Plus précisément, nous nous posons les questions suivantes :

- comment assurer la disponibilité, l'intégrité, la confidentialité des données ?
- comment mettre en place un système d'authentification pour l'accès aux données ?
- comment évaluer les risques liés aux données informatiques ?
- quelle approche méthodologique pour la protection des données ?

L'objectif de ce travail sur l'audit de la sécurité des données informatiques est de s'assurer du niveau de sécurité des données informatiques dans l'optique de réduire l'exposition aux vulnérabilités et sinistre et de minimiser les risques. Notre but est de faire un diagnostic des états des lieux afin d'obtenir un bon système de stockage de données informatiques fiables et crédibles pour un bon pilotage de l'entreprise.

De cet objectif principal découle les objectifs spécifiques suivants :

- s'assurer d'une bonne sauvegarde des données issues des traitements informatiques ;
- s'assurer de la gestion et de l'évaluation des risques informatiques;
- s'assurer de la mise en place des dispositifs de sécurité logique des données ;
- s'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques ;
- s'assurer de la mise en place d'un système de droit d'accès aux données informatique.

L'intérêt d'une telle étude pour l'entreprise, est de pouvoir évaluer et situer sa maitrise des risques informatiques, de savoir si ses pratiques en matière de sécurité informatique sont convenablement appliquées et si les dispositifs mis en place correspondent à ce qui se fait le mieux dans le domaine.

Pour les lecteurs, ce mémoire est un outil d'aide à la connaissance des risques informatique et les moyens de prévention de même qu'une aide à la connaissance des méthodes d'audit informatiques pour l'aspect sécurité.

Pour nous-mêmes : notre intérêt sera la mise en pratique des enseignements reçu tout le long de notre formation. Cette étude est le point culminant de notre formation d'une année.

Notre étude vise la sécurité des données informatiques ou informations de la S.N.E et se limitera aux :

- dispositifs mis en place pour le stockage et la sauvegarde des données puis du matériel informatique (hardware) ;
- dispositifs mis en œuvre pour protéger les données des menaces internes et externes (software) ;
- procédures mises en place pour une reprise rapide du service en cas de sinistre important (archivage et plan de reprise d'activité).

Le travail comporte deux parties, à savoir :

- la première partie, elle consistera à définir les données, leur support de stockage et moyens de protection. Il sera question d'aborder la méthodologie d'audit de sécurité des données informatique ou audit de la sécurité informatique, notamment l'adoption de l'approche par les risques ;
- la deuxième partie, elle portera sur la description et les missions de la S.N.E. L'analyse de la situation sur le terrain nous permettra d'élaborer un tableau de risques suivie des recommandations liées à la gestion des données informatiques.

PREMIERE PARTIE : CADRE THEORIQUE

Les données informatiques ou informations constituent le capital immatériel de l'entreprise; leur perte, leur destruction constitueraient un cout pour l'entreprise, ainsi leur protection est obligatoire. La montée en puissance des délits informatiques montre que les menaces sont d'origine interne ou externe à l'entreprise. Constituant les éléments de prise de décision, la destruction des données informatiques ou informations pourrait conduire à la ruine de l'entreprise. Sa sécurité doit donc être mis en place de façon pointilleuse, et être évaluée régulièrement.

La sécurité informatique pose un problème d'un ordre nouveau et qu'un simple ajout d'une serrure ne saurait résoudre. « La sécurité informatique est un enjeu considérable dont peu de responsables d'entreprise ont pris des mesures exactes ; les statistiques montrent que le risque s'accroit et peut mettre en cause la survie de l'entreprise » REIX (2002 :67).

L'évaluation de la sécurité des données informatiques ou informations implique de s'assurer que les procédures et les dispositifs mis en place sont efficaces, et qu'ils sont en adéquation avec les normes et les référentiels de bonnes pratiques, il s'agit de procéder à un audit.

Cette partie portera sur les données informatiques ou informations et à la sécurité, puis sur l'évaluation des risques par l'audit de la sécurité informatique et nous terminerons par l'approche méthodologique de notre recherche.

CHAPITRE I : DONNEES ET SECURITE INFORMATIQUE

Les entreprises modernes dépendent des données informatiques qui constituent le capital immatériel pour la prise de décision. Ce capital immatériel dépend du matériel informatique et ce dernier est rangé en système informatique. L'entreprise, communique avec ses partenaires, ses filiales et jusqu'aux particuliers, ce qui induit une ouverture à l'information.

Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise.

Dans ce chapitre, nous présenterons les données, le matériel de stockage des données ou informations, les risques pouvant affecter les données ou informations puis nous terminerons par la description des dispositifs relatifs à la sécurité des données ou informations et des outils de stockage.

1.1. Les données informatiques

« Dans les techniques de l'information, une donnée est une description élémentaire, souvent codée, d'une réalité (chose, transaction, événement, etc.). Ce sont des Informations utilisées par un logiciel. Elles peuvent être créées par l'utilisateur ou par le programme lui-même »(Wikipédia). Une donnée informatique est une représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement. Il n'est pas possible de traiter la sécurité des données, sans rappeler cet aspect fondamental : les données sont traitées avec des matériels informatiques et des systèmes d'exploitation. Les supercalculateurs, les micro-ordinateurs, les ordinateurs centraux et les systèmes ouverts(avec leurs périphériques) constituent les différents matériels informatiques. Ils se composent des supports physiques suivants : la Mémoire de l'ordinateur ; les disques, armoires (périphériques), pour la sauvegarde et le stockage ; les systèmes d'archivage.

Les données peuvent circuler entre ces systèmes dans des réseaux physique de communication notamment les réseaux de télécommunications, les réseaux locaux, réseaux de télécommunications par satellites. Sur les supports physiques, on doit implanter des systèmes qui gèrent les accès aux données et leur traitement : les accès logiques de ces systèmes peuvent être de type séquentiel ou indexé, les fichiers étant le plus souvent

remplacés par des bases de données permettant des accès et mises à jour plus évoluées.(Wikipédia)

Les systèmes de gestion de bases de données (SGBD) sont du niveau logiciel de base, et permettent à l'ordinateur de gérer ces différents types de traitement sur les données.

On distingue les niveaux conceptuels, logiques, physique.

1.1.1. Structuration des données

D'après Wikipédia, on peut distinguer les données selon :

- leur caractère structuré ou non :
    - une base de données orientée objet est un ensemble de données structurées ;
    - les documents, images, sons, ne sont pas a priori structurés du point de vue du système d'information (ils ont leur structure propre) ;
- leur place dans la hiérarchie on peut trouver :
    - des données élémentaires : bits, propriétés d'entités (objets ou relations) ;
    - des métadonnées.

La structuration des données joue un rôle clé dans la sécurité informatique, notamment dans la gestion des certificats électroniques. Les principales données impliquées dans les certificats sont les critères communs et les tiers de confiance.

1.1.2. Organisation de la gestion des données

Dans les grands services informatiques, les données doivent être répertoriées et organisées de manière à être aisément (ré-) trouvées et manipulées par tous les utilisateurs potentiels et par la communauté de développeurs. « D'un point de vue fonctionnel, les personnes responsables de donner une image des données du système d'information d'une façon plus ou moins macroscopique dans les entreprises sont les urbanistes de systèmes d'information et les architectes de données (data architect). D'un point de vue technique, les

personnes chargées d'organiser les données de l'entreprise sont les administrateurs de bases de données (DBA : Data base administrator).»,(Wikipédia).

1.2. Le système informatique et système d'information

Les données peuvent circuler entre les matériels informatiques en réseaux physique. Selon GRAEVE &POTIER (2001 : 3), « le système d'information peut être considéré comme la moelle épinière de l'entreprise, de même que le système de pilotage en est le cerveau et que le système opérant en est les membres »

D'après LAUDON & al.(2000 : 103), « bien que les systèmes d'information informatisés se fondent sur la technique informatique pour traiter les données brutes et pour les transformer en informations ayant une signification, il faut bien distinguer un ordinateur et les logiciels, d'une part, et un système d'information d'autre part. Les ordinateurs et les logiciels connexes constituent le fondement technique, les outils et le matériel nécessaire pour stocker l'information et pour la traiter ».

Selon (REIX 2005 :134) « Un système d'information est un ensemble de moyens techniques, administratifs, et humains qui servent à la collecte, au classement et à la transmission d'informations entre les membres d'une organisation (institution, entreprise, association)… ». Un système informatique est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons dans des organisations.

1.2.1. Architecture d'un système informatique

Selon DAYAN & al.(2008 :1075), « le système informatique est le support technique du système d'information de l'entreprise. Cela regroupe les moyens informatiques (serveurs et postes utilisateurs) et les moyens de communication (réseau) ».

Pour VOLLE (2004 :21), « le système informatique est l'ensemble de moyens matériels et logiciels assurant le stockage, le traitement et le transport des données sous forme électronique ».

De ces deux définitions, il ressort que le système informatique comprend les supports de stockage, de traitement et de transport des données sous forme électronique.

1.2.2. L'infrastructure réseau

Le transport des données sous forme électronique est assuré par l'infrastructure réseau. « L'infrastructure réseau ou support peuvent être des câbles dans lesquels circulent des signaux électriques, l'atmosphère (ou le vide spatial) où circulent des ondes radio, ou des fibres optiques qui propage des ondes lumineuses, des modems et des antennes réseau. Elles permettent de relier physiquement des équipements assurant l'interconnexion des moyens physiques »,(YADAV& SINGH, 2009 :182).

« Les équipements d'un réseau sont connectés directement ou non entre eux par des commutateurs(*Switch*), des concentreurs (*hub*) ou des routeurs », (LAUDON& al, 2000 :219).

1.2.3. La salle informatique ou data center

Selon la SMI (2010) & YADAV & SINGH (2009), cette salle héberge tous les équipements spécialisés, nécessaires à la fourniture des ressources informatiques. On y trouve les serveurs, calculateurs, solutions de sauvegarde et de restauration des données, baies de stockage, etc. Dans la plus part des sociétés de taille moyenne, cette salle contient également les éléments critiques du réseau (commutateurs, routeurs…) ainsi que les points d'accès et équipements servant à connecter la société vers le monde extérieur (central téléphonique, accès internet…).

1.3 Stockage et sauvegarde des données

La conservation d'objets numériques regroupe une vaste gamme d'activités qui visent à allonger la vie utile des fichiers informatiques et à les protéger contre les défaillances des supports, la perte physique et l'obsolescence. Il convient en effet d'assurer une possibilité de restitution et d'intelligibilité des contenus, ce qui signifie à la fois conserver le contenu, mais aussi sa forme, son style, son apparence et les fonctions sous-jacentes. Tout support de stockage est, par définition, dépendant d'une combinaison de hardware et de software. L'accessibilité à l'information ainsi stockée est très vulnérable eu égard à l'environnement technologique en rapide évolution. Le stockage et la sauvegarde sont réalisés par des supports physiques et sont tributaires de la taille de l'entreprise puis du volume des données ou informations.

1.3.1. Les support de stockage des données

Selon FAURE(2009a), les bandes magnétiques constituent encore les principaux supports de sauvegarde. La raison est principalement psychologique ! En réalité, sur la quantité toujours croissante de données stockées, beaucoup sont obsolètes et totalement inutilisées. La sauvegarde sur bandes gagne du terrain en tant que sauvegarde dorsale. Dans l'hypothèse où les données sont sauvegardées pendant sept ans, ce qui correspond en général aux standards de l'industrie, il en résulte 20 copies de la totalité des données. A ce rythme, les solutions de sauvegardes sur bandes magnétiques devraient rester prédominantes au moins jusqu'en 2020.

1.3.1.1. Les systèmes de stockage NAS et SAN

Le NAS est le standard du pauvre en matière de stockage car il permet de communiquer des données en mode IP sur un réseau Ethernet préexistant. Quant au SAN, il ne joue pas dans la même catégorie car ses liaisons spécialisées en fibres optiques autorisent des débits et une fiabilité hors normes. Les deux standards font bande à part depuis leur débuts et constituent l'essentiel de système de stockage. (KOMAR, 2006).

Le développement du commerce électronique, des datawarehouses ainsi que l'augmentation du nombre d'applications au sein des entreprises, notamment celles liées à la gestion de la relation client, sont autant de facteurs qui contribuent à l'accroissement exponentiel du volume des données. Pour répondre aux besoins de stockage considérables qui en découlent, des solutions apparaissent à un rythme soutenu, dans un secteur, celui du stockage, en pleine explosion. Nombre d'acteurs de l'industrie informatique, jusque là présents sur d'autres segments, abordent ce marché fort en perspectives de profits importants à moyen et long terme.(FAURE, 2009b)

A l'heure actuelle, la majeur des systèmes de stockage informatiques, tels que les disques durs, les systèmes RAID, etc., sont directement reliés à des ordinateurs clients à travers divers adaptateurs SCSI, Fibre Channel, ou autres. Ce type de stockage, ou attachement direct, est généralement appelé DAS. (KOMAR, 2006). Toutefois, la tendance à la consolidation des données ainsi que les besoins croissants d'un accès plus rapide à ces dernières dans les réseaux d'entreprises a conduit au développement de deux architectures de

stockage: les serveurs de stockage en réseau, ou NAS, et le SAN. De nouvelles variantes du SAN sont implémentées depuis peu, telles SoIP et iSCSI, protocole introduit récemment par IBM.

1.3.1.2. Les caractéristiques des architectures SAN et NAS

Les applications NAS utilisent les technologies réseau standards pour permettre un stockage partagé sur disques ou bandes et des sauvegardes sur bandes pour des postes clients et des serveurs à travers un LAN ou un WAN. Dans les configurations NAS, le système de fichiers réside dans l'application NAS lui-même, alors que dans les configurations SAN, le système de fichiers réside sur le serveur qui possède la portion de stockage partitionné qui lui est alloué.(FAURE, 2009b).

1.3.1.3 Caractéristiques essentielles de l'architecture NAS

Le NAS se distingue par les caractéristiques suivantes:

- directement connecté au réseau (il n'est pas nécessaire d'éteindre le serveur applications pour ajouter du stockage) et permet l'accès client aux données sans passer par un serveur d'applications.
- supporte le partage de fichiers dans des réseaux hétérogènes sous Windows NT, Windows 95/98/2000, Novell NetWare, Apple, ou les systèmes d'exploitation basés sur Unix.
- utilise un système d'exploitation et un système de fichiers dédiés qui résident dans le serveur NAS et qui sont gérés par ce dernier.
- relativement facile à déployer et à gérer.

La solution de stockage SAN est connectée à un serveur non-dédié à travers un réseau qui est séparé du LAN ou du WAN.

1.3.1.4. Caractéristiques essentielles de l'architecture SAN

Un SAN se distingue par les caractéristiques suivantes:

- permet aux serveurs un accès partagé à une ferme de stockage commune et à une ou plusieurs librairies de bandes pour la sauvegarde et la restauration ;
- utilise un réseau Fibre Channel séparé spécifique au stockage ;

- assure les transferts de données stockées entre les serveurs et les dispositifs de stockage sur le SAN, allégeant de ce fait la charge du LAN ;
- permet l'installation distante de sous-systèmes de disques durs et de librairies de bandes.

1.3.2. Les serveurs

Pour YADAV & SINGH (2009 :171), « un serveur est à la fois un ensemble de logiciels et l'ordinateur les hébergeant dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients (ordinateur et logiciel) via le réseau ». Les utilisations courantes des serveurs sont des serveurs fichiers, d'impression, de base de données, de courrier, ainsi que le serveur web, le serveur d'applications, le proxy et le serveur de jeu.
Un serveur de fichiers est utilisé pour le stockage et le partage de fichiers entre plusieurs utilisateurs. Un serveur impression est utilisé comme intermédiaire entre un ensemble d'utilisateurs et un ensemble d'imprimantes, tandis qu'un serveur est utilisé pour stocker et manipuler des données contenues dans une ou plusieurs bases et partagées entre plusieurs utilisateurs… Un serveur proxy (mandataire) reçoit des demandes, les contrôle, puis les transmet à d'autres serveurs.

1.3.3. Les postes utilisateurs ou ordinateurs

« Ce sont les ordinateurs de bureau, les ordinateurs portables, les ordinateurs de poches, les tablettes et les Smartphones qui permettent de se connecter de n'importe quel lieu où une connexion réseau est disponible », (DAYAN & al, 2004 :69).
Pour les utilisateurs de PC de bureau, la sauvegarde sur disque dur ou média amovible représente un gain de temps rendant les données rapidement accessibles, (Jean-Baptiste FAURE, 2009).

1.3.4. Les périphéries amovibles

Selon CARPENTIER (2009 :201), « c'est l'ensemble constitué par des appareils électriques qui peuvent être intégrés au système informatique… Afin de stocker ou

sauvegarder les données ou informations. Il s'agit de : disquettes, clés USB, disques durs externes… ».

1.4. La sécurité informatique

Selon ROYER (2004 :55), le domaine couvert par la sécurité informatique est vaste. Il le définit comme étant « la protection contre tous les dommages subis par ou causés par l'outil informatique ».

Selon (GODART, 2002 : 16-17), de manière plus concrète, une entreprise parle de sécurité pour protéger sa réputation, assurer la continuité de ses activités, protéger ses données stratégiques et ses propriétés intellectuelles, protéger les données privées de sa clientèle et de ses employés, se prémunir de la fraude, satisfaire aux exigences légales et éviter des pertes financières. La sécurité des données informatiques ou informations se caractérise par les principes suivants:

- la confidentialité, c'est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié. Ce principe traite la protection contre la consultation des données stockées ou échangées. Les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension ;
- l'intégrité ou la réalité, c'est le fait que les données sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) ;
- la disponibilité (aucun retard), cela nécessite un maintien de l'accessibilité en continu sans interruption, ni dégradation des données ;
- l'exactitude, cela implique que les données ne doivent comporter des erreurs.
- la pérennité, cela demande l'existence et la conservation des données et des logiciels pendant un temps nécessaire ;
- la non-répudiation assure le fait qu'une personne ou une entité ne puisse nier avoir effectué une activité. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à des clés privés. L'élément de la preuve de non-répudiation doit permettre l'identification de celui qu'il présente ; il doit être positionné dans le temps (horodatage), il doit présenter l'état ou le contexte dans lequel il a été élaboré ;

- la journalisation ou la preuve implique que tout accès ou opération aux données ou informations soit toujours enregistré ou répertorié ;
- l'exhaustivité implique que toute donnée devant être saisie l'a bien été.

Ces propriétés, en fonction de la valeur des données ou informations et de leur processus de vie doivent être garanties par des mesures sécurité mises en place par les dirigeants de l'entreprise d'où la nécessité d'une politique de sécurité dans l'entreprise.

1.4.1. Définition de la sécurité informatique

La sécurité informatique est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

1.4.2. Description de la sécurité informatique

Les techniques de la sécurité informatique sont : l'analyse de risques, la politique de sécurité, les techniques de sécurisation.

1.4.2.1. Analyse de risques

Plus aucune entreprise ne peut se passer de l'outil informatique, d'où la nécessité d'en assurer la sécurité, et de la protéger contre les risques liés à l'informatique. Or, comme on ne se protège efficacement que contre les risques qu'on connaît, il importe de mesurer ces risques, en fonction de la probabilité ou de la fréquence de leur apparition et de leurs effets possibles. Chaque organisation a intérêt à évaluer, même grossièrement, les risques qu'elle court et les protections raisonnables à mettre en œuvre. Les risques et les techniques de sécurisation seront évalués en fonction de leurs coûts respectifs.

1.4.2.2. Politique de sécurité

À la lumière des résultats de l'analyse de risques, la politique de sécurité :

- définit le cadre d'utilisation des ressources du système d'information ;

- identifie les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation ;
- sensibilise les utilisateurs à la sécurité informatique.

La politique de sécurité est le document de référence en matière de sécurité informatique. Elle pour objectif de protéger les données informatiques ou informations pour ce cas de figure et du système d'informations de façon large.

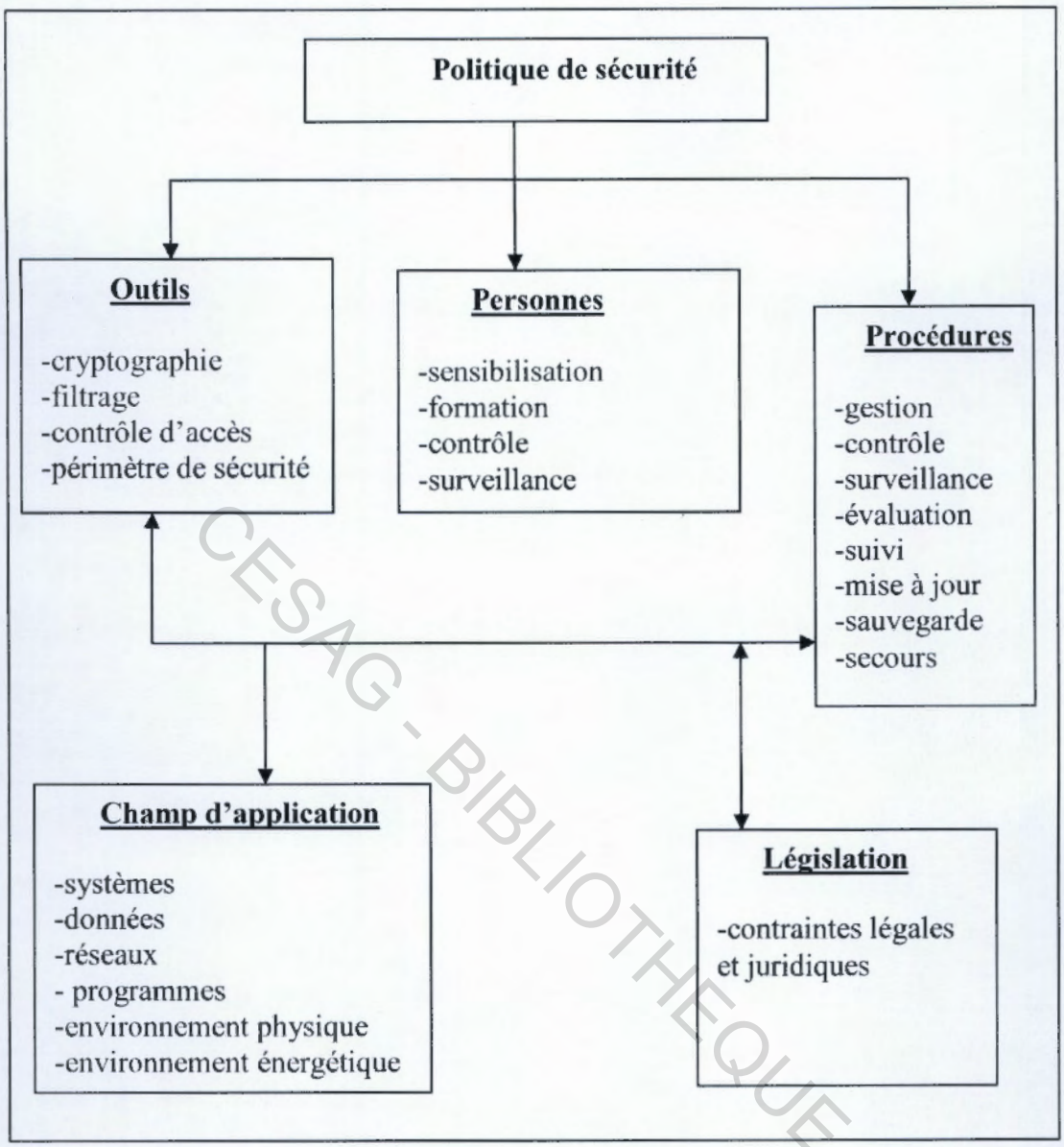
« La politique de sécurité se présente sous la forme d'un ensemble de documents qui présentent de manière ordonnée les règles de sécurité, les directives, procédures, règles organisationnelles et techniques à appliquer et à respecter. Ces règles sont généralement issues d'une étude des risques informatiques (système informatique et système d'information) », (PILLOU, 2010).

Les données ou informations faisant partie intégrante du système d'information leur politique de sécurité est étroitement liée ou dépendante de la politique de sécurité du système d'information.

Ainsi ANSSI (2007) retient comme éléments essentiels de la sécurité ce qui suit :

- l'élaboration des règles et des procédures à mettre en œuvre dans les différents services ;
- la définition des actions à entreprendre et les personnes à contacter en cas de survenance d'un risque ;
- sensibilisation des utilisateurs aux problèmes liés à la sécurité des systèmes d'informations ;
- les considérations de protection des données ou de l'information ;
- la désignation d'un responsable de sécurité ;
- la codification des règles concernant chaque utilisateur et son utilisation comme source des connaissances et référence en matière de meilleures méthodes de travail.

Figure 1 : politique de sécurité informatique



Source : CARPENTIER (2009 : 34)

1.4.2.3. Techniques de sécurisation

Elles assurent la disponibilité (les services et les informations doivent être accessibles aux personnes autorisées quand elles en ont besoin et dans les délais requis), l'intégrité (les services et les informations ne peuvent être modifiés que par les personnes autorisées), et la confidentialité (l'information est accessible uniquement à ceux qui y ont droit). Les techniques de sécurisation d'un système incluent :

- audit de vulnérabilités, essais de pénétration ;
- sécurité des données: chiffrement, authentification, contrôle d'accès ;

- sécurité du réseau: pare-feu, IDS ;
- surveillance des informations de sécurité ;
- éducation des utilisateurs ;
- plan de reprise des activités.

1.5. Définition du risque

Selon le référentiel ISO Guide 73 qui a été revu lors du développement de la norme ISO 31000:2009, la nouvelle définition abandonne la vision de l'ingénieur (« le risque est la combinaison de probabilité d'évènement et de sa conséquence ») pour coupler les risques aux objectifs de l'organisation : « le risque est l'effet de l'incertitude sur les objectifs »

Pour l'IFACI (in RENARD 2010 : 155), « 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 maitrise », quant à 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 ».

« Ainsi nous faisons le constat que la notion de risque comporte trois dimensions : le péril ou le danger identifié, diffus ou non identifié, ce que touchent les périls, et la mesure de vulnérabilité dépendante de la probabilité de survenance et de la mesure d'impact », (MOREAU 2002 :111).

Selon DUGLAY (2003 :17) « les risques inhérents non exhaustifs aux données et les systèmes informatiques sont : incendie, inondation, explosion, panne des installations, malveillance, Vol, erreur humaine, pirate, défaillance fournisseurs, environnemental, cyber-attaque, virus, rupture d'approvisionnement, externalisation défaillante, panne d'énergie, défaillance technologique, destruction, sabotage… ».

Comme nous le savons, les données ont pour support le matériel du système informatique, les risques inhérents aux données informatiques sont d'une part physique, et d'autre part les risques logiques qui eux sont relatifs à une partie immatérielle, et ceci sans prendre en ligne le contrôle interne qui peut exister dans l'entreprise ou l'organisation.

1.5.1. Les risques informatiques

On qualifie généralement de risques informatiques, toutes les causes externes qui peuvent compromettre l'efficacité d'un système, à l'exclusion de toute anomalie fonctionnelle (panne machine, bug, erreur de programmation...).

On peut les répartir en deux catégories :

- **les risques logiques** : d'origine humaine (cette appellation est donc teintée d'humour). On peut citer les différents types de malveillances, venant du personnel, d'un voleur ou d'un hacker ;
- **les risques physiques** : ils sont liés à l'environnement du système informatique (accès, bâtiments, fourniture électrique, climatisation...).

Il est indispensable de combattre les risques informatiques par une politique cohérente et systématique, ce n'est pas toujours le cas.

On peut également effectuer un classement des risques en fonction de leur nature :

- les accidents :
  - accidents physiques (incendies, explosion, dégât des eaux) ;
  - Pannes ;
  - Force majeure (tremblement de terre, tempête, inondation) ;
  - Pertes de services essentiels (électricité, télécommunications, eau).
- les erreurs :
  - erreurs à la conception ;
  - erreurs à la réalisation ;
  - erreurs à l'utilisation.
- la malveillance :
  - vols et vandalisme ;
  - fraude (Utilisation non autorisée des ressources du système d'information pour un travail personnel, pour détourner des fonds ou des informations) ;
  - sabotage (Attentat, vandalisme, action malveillante conduisant à un sinistre matériel) ;

- attaques logiques (sabotage immatériel, infection informatique, programme "simple", bombe logique, cheval de Troie, sabotage "manuel", programme auto-reproducteur, ver, virus, etc.) ;
- divulgations (Utilisation non autorisée des ressources du système d'information entraînant la divulgation à des tiers d'informations confidentielles).

Le souci de maîtriser les risques implique une identification préventive, systématique et périodique de tous les problèmes pouvant avoir une répercussion sur le fonctionnement de l'entreprise :

- identifier le risque et déterminer sa probabilité ;
- chiffrer ses conséquences sur le projet (coût, délai, performances) ;
- sélectionner les risques assurables ;
- adopter des provisions, des stocks et des marges de sécurité.

Face aux risques identifiés, la sécurité des systèmes d'information repose sur :

- la disponibilité des systèmes et l'intégrité des données ;
- la confidentialité des données et l'authentification des utilisateurs ;
- la possibilité de contrôle et de preuve et la non répudiation des transactions et des échanges.

La disponibilité marque l'aptitude des systèmes à remplir une fonction en particulier l'accès aux données de l'entreprise- dans des conditions prédéfinies d'horaires, de délais et de performances.

Affirmer que l intégrité des données est assurée implique que soient respectées les valeurs que peut prendre une quelconque de ces données, qu'elle soit considérée en tant que telle (un montant inscrit dans un compte ne peut être négatif) ou qu'elle soit placée en relation avec d'autres (le montant des fonds propres ne peut excéder le total du passif). Dans une Base de Données, les contrôles d'intégrité référentielle permettront d'empêcher la saisie de commandes pour un client déclaré clôturer ou de clôturer un client pour lequel il reste encore des créances en cours.

Affirmer que la confidentialité des données est assurée implique qu'elles soient accessibles pour consultation, mise à jour ou suppression, uniquement aux personnes ayant

reçu l'habilitation nécessaire. Authentifier un utilisateur implique de vérifier qu'il s'agit bien de lui et qu'il n'agit pas sous la contrainte.

Ne pas répudier une transaction implique de ne pouvoir nier avoir reçu ou transmis un message lorsque ceci a été effectivement le cas.

1.5.2. Les risques physiques

Pour GODARD (2002 :175) & ACISSI (2009 :145), n'étant pas exhaustifs, les plus envisagés sont : le feu, l'électricité, les défauts de climatisation, les intrusions physiques, les phénomènes électrostatiques, les dégâts des eaux.

Nous présenterons les risques physiques dont la nomenclature se distingue des risques humains, électriques et les sinistres.

1.5.3. Les risques logiques

Ces risques touchent, les personnes, les logiciels, les données ou les informations du système informatique. Ils sont l'œuvre des personnes internes de l'entreprise ou externes à travers le réseau internet ou wifi. L'être humain représente ainsi un grand danger pour la sécurité informatique (données ou information)

Du jour au lendemain, des nouveaux risques apparaissent. Nous présenterons les plus importants.

Pour ACISSI (2009), CALE & TOUITOU (2007), les malwares sont des programmes malveillants qui sont utilisés par les pirates pour commettre leur forfait. Ils sont multiples :

- le virus informatique, il s'installe dans des programmes légitimes pour se reproduire et contaminer le plus des fichiers possibles et ensuite déclenche l'action pour laquelle il a été crée ;
- le ver informatique, différent du virus; il est un programme autonome qui se déplace dans le réseau informatique grâce à une faculté d'auto-duplication ;
- le cheval de Troie est un logiciel se présentant sous une apparence bénigne (utilitaire, jeu, etc.); mais il recèle en son sein des fonctionnalités cachées lui permettant d'effectuer en toute discrétion du vol de fichiers, de la destruction des données, établissement d'une connexion avec le pare-feu. Il permet à son concepteur de faire du chantage, de l'espionnage industriel et commercial, des détournements des fonds, des

prises de contrôle à distance etc. La bombe logique est un cheval de Troie qui a la particularité de s'activer à un moment précis pour causer un maximum de dégâts dans le système informatique (équipement, données ou informations) où il aura réussi à s'introduire ;

- le back door est une fonctionnalité cachée incluse dans un logiciel ou un système d'exploitation par un développeur ou un cheval de Troie qui permet à son concepteur d'avoir accès à certaines fonctions sans passer par le processus d'authentification (session d'utilisateur et mot de passe) ;
- les logiciels espions permettent de voler des informations ou d'effectuer des tâches à l'insu de l'utilisateur un peu comme les chevaux de Troie. Il en existe une multitude :

  a) le spyware est un petit logiciel qui s'installe à l'insu de l'utilisateur pour transmettre des données et des fichiers ;

  b) le keylogger ou enregistreur de touche, enregistre les touches tapées sur le clavier de l'ordinateur sur lequel il a été installé et transmet les informations à son propriétaire ;

  c) le rootkit ou Kit de démarrage est un programme malveillant qui est utilisé par une personne malintentionnée et qui dissimule la présence de programme néfastes aux yeux de l'utilisateur et des logiciels de sécurité.

1.5.4. Les risques opérationnels

Le régulateur du dispositif Bâle II définit le risque opérationnel comme celui de pertes directes ou indirectes dues à une inadéquation ou à une défaillance des procédures, du personnel et des systèmes internes. Cette définition inclut le risque juridique; toutefois, le risque de réputation (risque de perte résultant d'une atteinte à la réputation de l'institution hancaire) et le risque stratégique (risque de perte résultant d'une mauvaise décision stratégique) n'y sont pas inclus.

Cette définition recouvre notamment les erreurs humaines, les fraudes et malveillances, les défaillances des systèmes d'information, les problèmes liés à la gestion du personnel, les litiges commerciaux, les accidents, incendies, inondations.

1.5.4.1. Les facteurs humains

Il s'agit de :

- des erreurs humaines commises par les informaticiens qui peuvent être lourdes de conséquences. Ce sont des erreurs de conception, de configuration, de programmation ou des erreurs par négligence. Pour les utilisateurs, les erreurs de saisie, erreurs de manipulation, négligence ;
- des comportements malveillants qui peuvent se manifester par le vol des données ou d'informations, la destruction des données, etc. par les personnes internes ou externes à l'entreprise ;
- l'ingénierie sociale qui consiste à exploiter la confiance humaine pour obtenir des informations (organigramme, mot de passe, numéro de téléphone, etc.) qui serviront à mener des attaques ou à faire effectuer certaines actions par les victimes en se faisant passer pour quelqu'un d'autre.

1.5.4.2. Les compromissions des données et usurpations d'identité

Pour GODART (2002 :111), il s'agit ici de vol des données ou informations confidentielles par cassage de message crypté ou cassage de mot de passe, le *snifing* ou encore récupération des données effacées.

« Un pirate peut se déguiser et prendre l'identité d'une ressource qui est considéré comme étant de toute confiance », (ACISSI, 2009 :167).

Suite à cette présentation non exhaustive des risques liés aux données ou informations et de leurs supports, il sied de constater que les menaces sont multiples et de divers types. Pour protéger ses données ou informations, l'entreprise doit mettre des dispositifs et procédures de sécurité afin de se prémunir des menaces ou danger.

1.5.4.3. Les risques environnementaux

Il s'agit des fluctuations de température, de l'hygrométrie et de la poussière. Ces éléments peuvent provoquer des incidents sur les supports de stockage des données ou informations. La survenance d'un tremblement de terre peut endommager les bâtiments où sont gardés les supports de stockage des données ou informations.

1.5.5. Les conditions de succès d'une démarche de sécurité

La mise en place d'une démarche sécurité passe par la réalisation des points suivants :

- une volonté directoriale ;
- une politique de sécurité simple, précise, compréhensible et applicable ;
- la publication de la politique de sécurité ;
- une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité ;
- un niveau de confiance déterminé des personnes, des systèmes, des outils impliqués ;
- un personnel sensibilisé et formé à la sécurité, possédant une haute valeur morale ;
- des procédures d'enregistrement, de surveillance et d'audit ;
- la volonté d'éviter de mettre le système d'information de l'entreprise en situation dangereuse ;
- l'expression, le contrôle et le respect des clauses de sécurité dans les différents contrats ;
- une certaine éthique des affaires et respects des contraintes légales.

Le management de la sécurité exige une démarche globale de maîtrise des risques liés à l'usage de système informatique et contribue à la protection des valeurs (matériel informatiques, données ou informations, etc.). La difficulté de mise en œuvre de solutions efficaces de sécurité provient du fait qu'elle qu'elles doivent être à la fois d'ordre technologique, procédural, réglementaire, organisationnel, humain et managérial. Ces différents angles sont à intégrer de façon cohérente doivent être acceptés et gérés efficacement par l'ensemble des acteurs intervenant dans une opération.

1.6. Les mécanismes de sécurité des données

Ici, il sied de présenter les dispositifs proposes par les grands éditeurs qui une fois mis en place peuvent assurer la sécurité des données informatiques ou informations et de leurs supports de stockage (matériels informatiques), du point de vue physique et logique. Nous allons reprendre le répertoire de présentation des risques de la section 4 afin d'associer chaque mécanisme de sécurité au risque qu'il permet de maitriser.

1.6.1. Les mécanismes de sécurité physique

Ses mécanismes protègent les supports de stockage et de traitement des données ou informations de façon physique.

La solidité des bâtiments est obligatoire, la souscription d'un contrat d'assurance est importante. Ce contrat d'assurance peut être ventilé en :

- contrat «tout risque informatique » qui couvre selon les garanties tout ou partie des dommages liés à des événements accidentels ;
- contrat « extension aux risques informatiques » qui couvre, selon les garanties, tout ou partie des dommages liés à une utilisation non autorisée des systèmes informatiques (actes frauduleux ou malveillants) ;
- contrat de type « globale informatique », qui cumule les deux premières.

1.6.2. Les mécanismes de sécurité logique

Pour la sécurité logique, les solutions des grands éditeurs sont :

- les malwares : la solution de sécurité est l'usage d'un progiciel antivirus sur les postes clients ainsi que sur les serveurs, couplé à un dispositif pare-feu ou *firewall*, (CLEUET & al, 2008a :41) ;
- les facteurs humain : les erreurs humaines peuvent être détectées quand la séparation des taches et des environnements est effective et que le personnel est supervisé. La sensibilisation et une grande vigilance du personnel de l'organisation ou de l'entreprise permettent de se prévenir de l'ingénierie sociale, du *phising*. L'usage d'un *proxy*, d'un firewall, de sonde de réseaux réduisent l'accès et détecte les intrusions aux réseaux ;
- la compromission de l'information et l'usurpation d'identité : l'environnement étude et exploitation doivent être séparés de telle sorte que le personnel qui développe les applications et ceux qui gère les postes clients n'accèdent pas aux mêmes fichiers ou données. Le second est la limitation des accès aux utilisateurs comme le souligne STALLINGS (2002 : 346), « les contrôles d'accès utilisateur limitent l'accessibilité aux données ou informations et privilégient une catégorie du personnel vue la confidentialité des données ou de l'information » ;

En dehors du chiffrement du message, la cryptographie permet avec l'usage de ses algorithmes :

- l'authentification, mécanisme permettant de s'assurer de l'identité de la personne à l'origine de l'opération (envoi du message, etc.) ;
- l'intégrité, mécanisme facilitant de s'assurer qu'un message n'a pas été modifié après avoir été envoyé ou qu'une donnée n'a pas été altérée après avoir été enregistrée ;
- la non répudiation, permet d'assurer qu'une personne ne puisse nier avoir réalisé une opération après l'avoir effectuée (lecture d'un message, transaction financière, etc.). « La détection de l'altération des données est assurée par des outils basés sur des algorithmes de hachage tels que MD-5 et SHA-1 qui permettent de créer un condensé (ou *has*) d'un texte. Ainsi, si ce dernier est modifié, le résultat de l'algorithme sera différent », (CALE & TOUITOU, 2007 : 99).

  Ces mécanismes doivent faire partie d'une gestion organisationnelle de la sécurité.

1.6.3. Le plan de sauvegarde des données et secours informatique

Ces éléments permettent la continuité des activités. Leur mise en place est du fait que l'entreprise est dépendante de ses informations et de l'informatique. Ces éléments permettent à l'entreprise de continuer son activité en mode dégradé en cas de sinistre important, de récupérer les données effacées ou d'utiliser des versions antérieures des logiciels et informations du système informatique.

1.6.3.1. Le plan de sauvegarde

Pour BUTEL (2008 : 22) et LESSAUVEGARDES (2007), le plan de sauvegarde doit permettre de récupérer, de manière transparente, les informations indispensables au fonctionnement opérationnel de l'entreprise, voire vitales pour sa survie. Un bon plan de sauvegarde doit être exhaustif, fiable, évolutif, cohérent et auditable. Il est composé de :

- une analyse des besoins qui détermine ce qui doit être protégé, le degré de sécurisation et la facilité de récupération ;
- les procédures et les règles générales qui s'appliquent pour chaque type de fichiers, de données, d'applications et de matériel ;
- la documentation détaillés des actions à entreprendre pour sauvegarder les données, les méthodes et outils employés, les fréquences de sauvegarde, le

nombre de génération concernées, les supports utilisés, les procédures de marquage et d'identification, les documentations concernées, les règles de restauration ainsi que le lieu de stockage des sauvegardes (interne ou externe à l'entreprise).

1.6.3.2. Le plan de secours informatique

Selon (MENTHONNEX, 1995 : 211), « le plan de secours est l'ensemble des solutions étudiées par la Direction Générale de l'entreprise et par la direction informatique pour reprendre l'activité informatique, après un sinistre total, dans les conditions qui permettent la survie de l'entreprise ».

Ce plan de secours est composé de dispositifs élémentaire dont l'activation dépendra de l'événement survenu et du contexte général. Cela nécessite suivant le type d'activité la mobilisation des ressources ; le secours des équipements informatiques, des réseaux et de la télépbonie ; la reprise des traitements ; la logistique ; le relogement ; la reprise des activités des services utilisateurs ; la communication de la crise et les dispositifs post-reprise.
« Les dispositifs de secours doivent être accompagnés de dispositifs permanents tels qu'un plan de sauvegarde, la formation des acteurs pour garantir leur niveau », (CLUSIF, 2003).

Le plan de secours permet à l'entreprise de retrouver assez rapidement son niveau d'activité.

1.6.3.3. Les contraintes légales et réglementaires

L'acte uniforme de l'Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA) portant sur l'barmonisation des comptabilités en son article 22 relatif au traitement informatique de la comptabilité reprend dans son alinéa 1à 7 les principes de sécurité informatique : confidentialité, intégrité, disponibilité, la journalisation ou preuve, la non-répudiation. Dans son article 24, l'acte uniforme évoque la conservation des pièces comptables pour 10 ans, ce qui conduit à la sauvegarde et l'archivage informatique.

Conclusion

Les données informatique ou informations sont des ressources capitales pour l'entreprise car elles sont des éléments de prise de décision, de gestion. Cependant elles sont sous la menace de nombreux risques. La sécurité informatique qui est dispositif de contrôle interne, technique et organisationnel, doit donc prémunir les données informatiques en sécurisant le système informatique de la survenance d'un risque qui peut avoir des conséquences graves, voire même mettre l'entreprise en péril.

CHAPITRE II : L'EVALUATION DU RISQUE ET L'AUDIT DE LA SECURITE INFORMATIQUE

Le risque est un concept selon lequel l'entreprise exprime ses inquiétudes concernant les effets probables d'un événement sur les objectifs de l'entité dans un environnement incertain. Dans la mesure où il est imprévisible, l'entreprise doit tenir compte d'une gamme d'événements possibles qui pourraient intervenir dans un univers incertain. Chacun de ces événements pourrait avoir une conséquence significative sur l'entité et sur ses objectifs. Dans la mesure où il est contrôlé (maitrisé), le risque issu de l'incertitude et de l'aléa n'est pas inquiétant en soi. La gestion des risques inclut l'analyse de ces risques et une démarche prudente et progressive conduisant à une meilleure compréhension et à une plus grande appréhension des conséquences de la gestion dans un monde incertain.

2.1. Définition et objectifs de l'évaluation des risques

Au regard des mutations économiques et technologiques actuelles, tout n'est que risque. Certes, la prise de risques est inhérente à la fonction de chef d'entreprise. Mais ce risque doit être mesuré, calculé. La pérennité d'une structure telle que l'entreprise passe par la maîtrise du risque.

2.1.1. Définition de l'évaluation des risques

L'évaluation des risques est la première étape dans un processus de management des risques pour les entreprises dépourvues d'une culture de risk management. Selon les normes de fonctionnement et normes de mise en œuvre associées, l'évaluation des risques doit être au moins annuelle et prendre en compte tous les processus de l'entreprise.

L'évaluation des risques est donc le processus qui consiste en une inspection approfondie de l'entreprise en vue d'identifier entre autres les éléments, situations et procédés qui peuvent causer un préjudice. Une fois cette étape terminée, il faut évaluer la probabilité et la gravité du risque, puis déterminer quelles mesures adopter afin d'empêcher le préjudice de se concrétiser. L'évaluation des risques consiste à identifier et à analyser les facteurs susceptibles d'affecter la réalisation des objectifs. Cette évaluation des risques se fait souvent par des missions d'audit.

2.1.2. Objectifs de l'évaluation des risques

L'objectif du processus d'évaluation des risques consiste à éliminer un danger ou à réduire le niveau de risque en instaurant des mesures de maîtrise ou en adoptant des précautions appropriées, s'il y a lieu.

Au niveau de l'entreprise, l'évaluation des risques permet d'atteindre trois objectifs :

- inventorier, évaluer et classer les risques de l'organisation ;
- informer les dirigeants pour une meilleure adaptation des activités au management des risques ;
- l'élaboration d'une politique des risques par la direction générale avec l'aide du risk manager. Cette politique s'imposera aux responsables opérationnels et aux auditeurs internes.

L'évaluation des risques sert de base à la programmation des missions d'audit au sein de l'entreprise.

2.2. Identification des risques

C'est le passage obligé dans la construction d'une structure rationnelle et globale de gestion des risques pour permettre l'élaboration d'un contrôle interne efficace. En effet c'est le point de départ pour une évaluation des risques. L'identification requiert une connaissance appropriée et une compréhension des activités de l'entreprise.

Les techniques d'identification des risques utilisées sont :

- identification par découpage de l'activité en tache élémentaires : il s'agit d'identifier et lister toutes les tâches élémentaires de l'activité si possible de façon séquentielle. Le découpage permettra de connaitre les risques que l'entreprise encourt si l'une des tâches n'est pas exécutée ou est mal exécutée ;

- identification prenant en compte l'atteinte des objectifs : elle débutera par une identification claire et précise des objectifs de l'entreprise, ensuite à chaque objectif sera affectée la menace qui lui correspond. Cette technique est assez complexe dans sa réalisation ;
- identification basée sur les check- lists : utilisation d'une liste préétablie et exhaustive des risques. cette liste est fonction des activités de l'entreprise et elle prend en compte

tous les risques relatifs aux différentes activités de celle-ci. Cependant l'entreprise doit veiller à une mise à jour permanente de cette liste pour éviter qu'elle ne devienne obsolète ;

- identification basée sur l'analyse historique : c'est une technique qui consiste à partir des risques déjà survenus dans l'entreprise dans le passé d'en tenir compte dans l'identification des risques.
- exposure analysis : elle consiste à identifier les risques qui ont un impact sur les actifs de l'entreprise. Les managers pour atteindre leurs objectifs utilisent les actifs de l'entreprise qui doit de ce fait se concentrer sur les risques qui touchent à ses actifs. Ces actifs peuvent être les moyens financiers, matériels, humains, immatériels. Cette techniques prend en compte la taille, le type des actifs ;
- environnemental analysis : elle consiste en une identification des risques liés aux activités de l'entreprise ;
- threat scénarios : une identification des risques basée sur les fraudes et anomalie.

Plusieurs de ces techniques peuvent être combinés pour une identification exhaustive des risques. Une fois les risques identifiés il va falloir les évaluer

2.3. Evaluation des risques

La gestion des risques ne doit pas se limiter uniquement à une simple identification, c'est-à-dire à un recensement plus ou moins exhaustif des risques potentiels et pertinents et à une analyse plus ou moins approfondie de leurs caractéristiques. Elle doit s'appuyer également sur une analyse (qualitative ou quantitative) pour mieux appréhender et estimer leurs probabilités de survenance et la gravité de leurs impacts.

2.3.1. Principes d'évaluation des risques de l'entreprise

L'évaluation des risques est une étape centrale du management des risques, mais cela nécessite certains principes non négligeables :

- l'évaluation est individuelle. Il est souhaitable que les données d'évaluation soient le produit d'une analyse personnelle ;
- l'évaluation des risques n'est pas un travail de notation ou d'appréciation des différents responsables fonctionnels ou de processus. Il faut nécessairement veiller à ce que ce travail soit le plus objectif possible ;

- l'appréciation de la probabilité est une estimation très fine des facteurs qui rendent favorable l'apparition du risque. Il peut s'agir de facteurs internes ou externes.

L'appréciation de la gravité est une estimation très fine des impacts supposés de la survenance du risque sur la réalisation des objectifs de l'organisation. Il conviendra de ne pas surestimer des risques dont les impacts sur les objectifs stratégiques ne seraient que « locaux ». De même, il faudra veiller à ne pas sous estimer des risques. Il est important que chaque évaluateur veille à ne pas tomber dans le piège du « biais cognitif » c'est-à-dire la tendance à commettre des « erreurs » d'évaluation compte tenu de facteurs subjectifs, secondaires ou erronés.

2.3.2. Technique d'évaluation du risque

Le risque se caractérise essentiellement par deux notions à savoir celle de danger (impact) et de l'incertitude (probabilité). Selon BARTHELEMY & COURREGES (2004 : 11) « le risque est fonction de sa criticité qui se mesure par : criticité égale à l'impact du risque multiplié par sa probabilité de survenance ».

Pour Bapst et Bergeret (2002 : 31), « l'évaluation est une étape qui a pour objet d'appréhender au mieux les incertitudes qui concernent une activité.
En effet, elle vise à mesurer, à affecter des valeurs aux risques identifiés en fonction de l'impact et de la probabilité d'occurrence. La probabilité d'occurrence peut provenir des facteurs internes ou externes alors que l'impact peut être financier, d'image ou matériel ».

L'évaluation des risques se fait à partir des techniques appropriées que nous présentons dans la section qui suit.

2.3.2.1. La technique qualitative

« Les techniques d'évaluation qualitative sont souvent utilisées lorsque les risques ne se prête pas à une quantification ou il n'y a pas assez de données fiable pour effectuer une évaluation quantitative ou encore lorsqu'il n'est pas possible d'obtenir ou d'analyser ces données moyennant un coût raisonnable », (COSOII REPORT, 2005: 78). Or selon Bapst et Bergeret (2002 : 11), « les actifs intangibles ou immatériels représentent aujourd'hui 2/3 de la

valeur de l'entreprise ; c'est pourquoi la technique qualitative est préférée à la technique quantitative ».

Ainsi pour ce qui est de la probabilité d'occurrence, une échelle de mesure est définie comme suit : très élevée, élevée, modérée, faible, très faible. Cette échelle est déterminée en fonction de l'efficacité du contrôle interne en place.

Tableau n°1: exemple d'échelle de probabilité des risques affectant les activités informatiques

Niveau	Qualification	Probabilité de survenance	Risques
1	Rare	Très faible	Panne prolongée des systèmes du fait des actes terroristes ou délibérés
2	Impossible	Faible	Catastrophe naturelle obligeant à avoir recours au plan de continuité
3	Possible	Modérée	Sécurité informatique attaquée par les pirates
4	Probable	Elevée	Le personnel utilise les ressources de l'organisation pour accéder à des informations non appropriées sur internet
5	Presque sûr	Très élevée	Le personnel utilise les ressources de l'organisation à des activités de messagerie privée

Source : COSOII REPORT (2005 : 208)

Quant à l'impact, il s'agit de voir quelle conséquence négative la survenance d'un risque peut avoir sur les objectifs de l'entreprise. Ces conséquences peuvent être financière, d'image, d'insatisfaction du personnel ou des clients. Pour ce qui est de sa mesure, une cotation est établie comme illustrée par le tableau ci-dessous :

Tableau n°2: exemple de correspondance d'échelle de gravité

Niveau	Impact	Risque sur les données ou informations	Description
1	Insignifiant	Accès aux données confidentielles par un agent	Pas de perte sur le CA
2	Mineur	Piratage du système informatique	Perte sur CA < 5%
3	Modéré	Vol d'informations ou des données	5%<perte de CA<10%
4	Majeur	Destruction des données	10%<perte de CA<35%
5	Catastrophique	Vol des données ou informations	35%<perte de CA<100%

Source : COSOII REPORT (2005 : 209)

2.3.2.2. La technique quantitative

La technique traite de la probabilité d'occurrence et de la mesure de la gravité du risque. Son but est de :

- hiérarchiser le risque ;
- évaluer le niveau de sécurité du système ;
- construire la sécurité du système de façon efficace et cohérente, (Desroches & al, 2003 : 59).

Cette technique rassemble les données objectives historiques et inhérentes à chaque processus provenant des sources diverses. A partir de ces éléments et pour chaque période visée, l'on calcule les coefficients et combine ces données avec leurs tendances respectives au fil du temps afin d'obtenir un indicateur statistique final pour chaque catégorie. Après pondération, ces indicateurs sont eux-mêmes regroupés pour donner un facteur de risque quantitatif global unique.

« La technique quantitative est plus complexe et nécessite des compétences dans l'élaboration des modèles mathématiques et aussi en techniques statistiques. Il est donc possible d'obtenir une mesure quantitative de l'impact d'un événement à l'échelle de l'entité lorsque toutes les évaluations individuelles des risques relatifs à cet événement sont

exprimées en terme quantitative », (COSOII REPORT, 2005 : 80). Cette technique tend vers une disparition au profit de la technique qualitative du fait qu'elle nécessite plus de qualification, de temps et aussi de ressources.

Plusieurs méthodes ont été développées dans le cadre de l'audit informatique pour évaluer les caractéristiques du risque.

2.4. Méthodes de travail de l'audit informatique

L'auditeur s'appuie sur des normes, des référentiels de bonne pratique ou des méthodes spécifiques, des standards à l'audit informatique pour mener sa mission de manière professionnelle et efficace.

2.4.1. Les normes ISO 27001 & ISO 27002

Suite à leur universalité, elles ont été reprise en partie ou en totalité dans les référentiels ou méthode « technique de l'information ».

2.4.1.1. L'ISO 27001

Publiée en 2005 par International Organisation for Standardization (ISO) et a pour titre : Technique de l'information – Technique de sécurité-Système de gestion de l'information.

La norme ISO 27001 porte sur la politique du management de la sécurité des systèmes d'informations dans une entreprise. Elle définit les contrôles de sécurité dont la mise en œuvre est exigée, (l'AFAI, 2007 & GUIDE INFORMATIQUE, 2010).

La norme ISO 27001 comprend six (06) domaines de processus qui sont :

- définir une politique de la sécurité des informations ou « données informatiques » ;
- définir le périmètre du système de management de la sécurité de l'information ;
- réaliser une évaluation des risques liés à la sécurité, gérer les risques identifiés ;
- choisir et mettre en œuvre les contrôles ;
- préparer un SoA (statement of applicability).

2.4.1.2. L'ISO 27002

Elle a pour titre : « Codes de Bonnes Pratiques pour la Gestion de la Sécurité information » et a été publiée en 2005.

La norme ISO 27002 définit la politique de sécurité de façon plus détaillée des systèmes d'informations donc des systèmes informatiques car ces derniers sont les supports des systèmes d'informations. C'est une liste annotée de mesures de sécurité. Cette norme est un guide de Bonnes Pratiques pour la sécurité d'un système d'information. Schématiquement, la démarche de sécurisation du système d'information doit passer par quatre (4) étapes de définition qui sont : périmètre à protéger (liste des biens sensibles), nature des menaces, impact sur le système d'information, mesures de protection à mettre en place.

Selon l'AFAI (2007), la norme ISO 27002 comporte 39 catégories de contrôle et 133 points de vérification repartis en 11 domaines :

- politique de sécurité ;
- organisation de la sécurité : organisation humaine, implication biérarchique, notion de propriétaire d'une information et mode classification, évaluation des nouvelles informations, mode d'accès aux informations par une tierce personne, cas de l'externalisation de l'information ;
- classification et contrôle des biens ;
- sécurité du personnel ;
- sécurité physique : organisation des locaux et des accès, protection contre les risques physiques (incendies, inondations…), système de surveillance et d'alerte, sécurité des locaux ouverts et des documents circulants ;
- communication et exploitation : prise en compte de la sécurité dans les procédures de l'entreprise, mise en œuvre des systèmes de sécurisation (anti-virus, alarmes etc.) ;
- contrôle d'accès (définition des niveaux d'utilisateurs et de leur droit d'accès, gestion dans le temps des droits) ;
- acquisition, développement et maintenance des systèmes ;
- gestion des incidents ;
- management de la continuité de service ;
- conformité (dispositions réglementaires, dispositions légales, politique interne).

« Cette norme est essentiellement pragmatique et n'impose pas d'autre formalisme que la mise en place d'une organisation qui garantie un bon niveau de sécurité au fil du temps. Elle s'intéresse à l'organisation du personnel ainsi qu'aux problèmes de sécurité physique (accès, locaux…) », (AFAI, 2007 :21&23).

2.4.2. MEHARI

MEHARI (Méthode Harmonisée d'Analyse des risques) est une méthode complète d'évaluation et de management des risques liés à l'information ou « données », ses traitements et les ressources mises en œuvre. Réduire les risques impose de connaitre les enjeux et les processus majeurs pour l'organisation afin d'appliquer les mesures organisationnelles et techniques de manière à optimiser les investissements. Cette démarche implique donc à utiliser les pratiques et solutions à la hauteur des enjeux et des types de menaces pesant sur l'information ou « données », sous toutes ses formes, et les processus comme les éléments qui la gère ou la traite, (CLUSIF, 2010a)

Selon Hugo Etiévant (2006), la méthode MEHARI s'étale sur 3 types de plans :

- le Plan Stratégique de Sécurité (PSS) qui fixe les objectifs de sécurité et les métriques et qualifie le niveau de gravité des risques encourus ;
- les Plans Opérationnels de Sécurité (POS) qui déterminent, par site ou entité géographique, les mesures de sécurité à mettre en place, tout en assurant la cohérence des actions choisies ;
- le Plan Opérationnel d'Entreprise (POE) qui permet le pilotage de la sécurité au niveau stratégique par la mise en place d'indicateurs et la remontée d'informations sur les scénarios les plus critiques.

La méthode MEHARI diagnostic 160 services de sécurité répartis en 12 domaines étudiés :

- organisation de la sécurité ;
- sécurité des sites et bâtiments ;
- sécurité des locaux ;
- réseau étendu (inter site) ;
- réseau local ;
- exploitation des réseaux ;

- sécurité des systèmes et leur architecture ;
- production informatique ;
- sécurité applicative ;
- sécurité dans les développements ;
- protection et environnement de travail ;
- juridique et réglementaire.

Selon le CLUSIF (2010 a), MEHARI donne un cadre méthodologique des outils et des bases de connaissance pour :

- analyser les enjeux majeur ;
- étudier les vulnérabilités ;
- réduire la gravité des risques ;
- piloter la sécurité de l'information ou des « données ».

L'analyse des enjeux de la sécurité est l'identification des dysfonctionnements potentiels pouvant être causés ou favorisés par un défaut de sécurité et, l'évaluation de la gravité de ses dysfonctionnements. Cette analyse se base sur les objectifs et attentes métiers de l'entreprise. Elle demande une participation des décideurs et le management stratégique de l'entité dans laquelle elle est utilisée.

L'analyse des vulnérabilités sert à identifier les faiblesses et les défauts des mesures de sécurité. En pratique, il s'agit d'une évaluation quantitative de la qualité des mesures de sécurité qui couvre l'efficacité des services de sécurité, la robustesse et la mise sous contrôle. Elle s'articule à vérifie l'absence de points faibles inacceptables, à évaluer l'efficacité des mesures de sécurité mises en place et garantir leur efficience et à se comparer à l'état de l'art ou aux normes en usage. L'analyse de vulnérabilité permet de corriger les points faibles inacceptables par des plans d'action immédiats, d'évaluer l'efficacité des mesures mises en place et garantir leur efficience, de préparer l'analyse des risques induits par les faiblesses mises en évidence et de se comparer à l'état de l'art ou aux normes en usage, (CLUSIF, 2010 a).

L'analyse des risques couvre l'identification des situations susceptibles de remettre en cause un des résultats de l'organisme en son sein. La mise en œuvre des mesures susceptibles de ramener chaque risque à un niveau acceptable.

Le pilotage de la sécurité implique un cadre ordonné pour définir les objectifs annuels ou les étapes de plan d'action, des indicateurs permettant de comparer les résultats obtenus aux objectifs et les références externes permettant un benchmarking.

Selon CLUSIF (2010 a), les modules de MEHARI peuvent être combinés, en fonction du choix de la politique de l'entreprise, pour bâtir des plans d'action ou, tout simplement, pour aider la prise de décision concernant la sécurité de l'information ou des « données ».

2.4.3. COBIT

Selon Business Technology Consulting, le COBIT comprend 318 objectifs de contrôle détaillés regroupés en 34 objectifs de contrôles de haut niveau correspondant à des processus de gestion, d'où le terme de COBIT: Control Objectifs for Information Technologie.

Les processus de COBIT sont regroupés en quatre domaines:

- planning et organisation :
  - choix de la stratégie permettant d'identifier les meilleures solutions informatiques pour permettre d'atteindre des objectifs métiers ;
  - mise en place de la stratégie, planification, communication et gestion selon différentes perspectives.
- acquisition et mise en place
  - création ou achat de solutions informatiques leur intégration aux processus métiers ;
  - gestion du changement et de la maintenance.
- fourniture et soutien
  - fourniture des services métiers disponibilité ;
  - sécurisation, disponibilité des services.
- surveillance et évaluation
  - mesure de la qualité des processus ;
  - mesure de l'atteinte des objectifs des processus ;
  - contrôle et de amélioration de l'organisation et des processus.

Pour l'AFAI (2008a), COBIT est un ensemble de ressource contenant toutes les informations dont les entreprises ont besoin pour adopter un cadre de contrôle et de gouvernance des systèmes d'information/système informatique. COBIT propose des bonnes pratiques à travers un cadre de référence par domaine et par processus, dans une structure logique facile à appréhender.

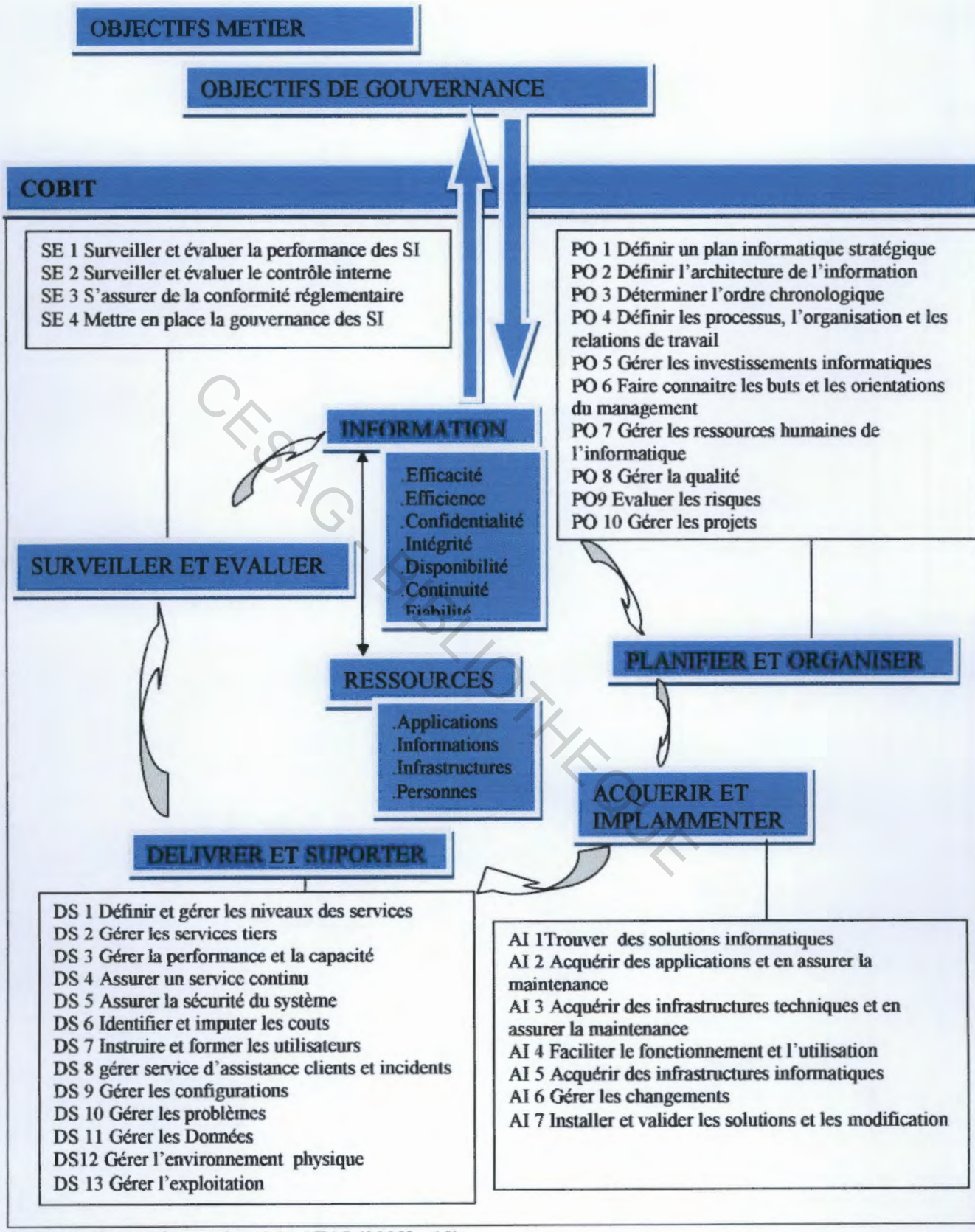
COBIT est largement utilisé sur la base de ses points de contrôle et peut trouver des compléments dans d'autres référentiels plus spécialisés tels qu'ITIL, CMMI ou l'ISO 9000. COBIT agit comme intégrateur de ces différents guides en réunissant les objectifs clés dans un même cadre de référence général qui fait aussi le lien avec les exigences de gouvernance et les exigences métiers. Dans cette perspective le COSO et d'autres référentiels semblables qui se conforment aux mêmes principes sont généralement considérés comme les référentiels de contrôle interne pour les entreprises.

Selon l'AFAI (2008a), la préférence de COBIT comme cadre de gouvernance des systèmes d'information donne les avantages qui suivent :

- une meilleure harmonisation de l'informatique et de l'activité de l'entreprise du fait de son orientation métier ;
- une compréhension partagée par toutes les parties prenantes grâce à un même langage commun ;
- une vision compréhensible de ce qu'apporte l'informatique à la gestion de l'entreprise;
- une attribution claire de la propriété et des responsabilités, du fait de l'approche par processus ;
- une adoption généralisée de la part des tiers et des organismes de contrôle,
- le respect des exigences du COSO pour le contrôle de l'environnement informatique.

Le cadre de référence de COBIT se résume dans la figure qui suit :

Figure n°2: Cadre de référence de COBIT



Source : Nous même adapté à AFAI (2008b :10)

Le référentiel d'audit et de contrôle établi à partir de COBIT permet à des auditeurs non informaticiens de mener, de façon très professionnelle, des audits informatiques du fait il permet de prendre en compte qui n'auraient pas été évoqués, faute d'y songer ou par manque de connaissance et à établir les questions à dérouler lors des entretiens.

Bon nombre de référentiels, méthodes ; et standards existent pour cadrer une mission d'audit informatique. Il s'agit du CMMI, de ITIL, de EBIOS ou encore les vingt points de contrôle critique pour une cyber-défense efficace, méthode éditée par le SANS Institute.

L'évaluation de la sécurité des données informatiques ou informations passe par l'audit de la sécurité du système informatique et des données informatique eux même. L'audit a pour but de positionner le niveau de la sécurité informatique par rapport à un standard ou par rapport à des exigences légales. L'audit de la sécurité, à l'instar de tout audit, requiert une rigueur et une démarche appropriées.

2.5. Les phases d'une mission d'audit de sécurité informatique

Pour l'ISACA in AFAI (2008 b), procéder à l'audit informatique, convient de suivre une méthodologie ou une démarche cohérente. Même si la démarche spécifique peut être propre à l'entreprise et type de mission, une approche relativement commune est utilisée. Cette approche s'articule en trois phases qui sont : la planification, le cadrage, et l'exécution.

- la phase de cadrage est particulière l'audit informatique/ l'audit des systèmes d'information/système informatique. Cette phase correspond à la mission d'audit interne. Le choix et l'utilisation d'un cadre de référence révèle ici d'une grande importance. « Le choix du référentiel COBIT permet à l'auditeur non-informaticien de mener avec efficacité une mission d'audit des systèmes d'information », (CLEUET, 2008a : 61) ;
- la phase de planification est le point de départ de chaque mission d'audit. Elle définit le périmètre d'audit/audit des systèmes d'information/système informatique. L'auditeur doit combiner la compréhension du périmètre d'audit des systèmes d'information/système informatique et la sélection d'un cadre de contrôle des systèmes d'information approprié, tel que le COBIT afin de créer un plan complet. La

réunion de ces deux éléments permet de planifier la mission d'audit en fonction des risques.

2.5.1. La phase de préparation et cadrage

Elle est encore appelée phase d'étude et se compose de l'ordre de mission, la familiarisation, l'identification et l'évaluation des risques et la définition des objectifs ; le cadrage regroupe les trois dernière étapes de cette phase.

2.5.1.1. L'ordre de mission

Pour RENARD (2010 :177), « l'ordre de mission est un droit d'accès par lequel la Direction Générale de l'entreprise donne mandat à l'Audit interne. Elle déclenche le travail de l'équipe d'audit et amorce le point de départ d'une mission. L'ordre de mission informe toutes les personnes ou entités qui seront concernées par la mission d'audit ; l'élément principal de ce document est constitué par l'objet de la mission qui doit être clairement défini ». Elle remplit à la fois la fonction de mandat et d'information.

2.5.1.2. La familiarisation

Selon RENARD (2010) et SCHIK (2007), cette étape donne une vision d'ensemble de l'entité auditée et des contrôles mis en place par des lectures, rassemblement d'une documentation, interviews, discussions avec les dirigeants. Elle permet de cibler les objectifs de la mission et à identifier les problèmes essentiels concernant le sujet la fonction objet de la mission, et surtout elle permet d'organiser les opérations d'audit.

« En plus de permettre l'identification des objectifs de contrôle et des procédures en place, elle permet de définir le périmètre de l'audit qui sera communiqué en même tant que les objectifs à toutes les parties prenantes et approuvées par celle-ci », (AFAI, 2008b :73).

La familiarisation ou prise de connaissance permet de situer le système informatique dans son contexte, de rencontrer ses utilisateurs, d'apprécier le contrôle interne et de se placer dans un repère provisoire de points forts et des points faibles

2.5.1.3. L'identification et l'évaluation des risques

« Cette étape conditionne le dosage et la nature des contrôles à effectuer. L'auditeur interne construira son référentiel et son programme de travail en tenant compte des risques inhérents identifiés », (SCHIK, 2007 :93).

2.5.1.4. La définition des objectifs

Cette phase est encore appelée rapport d''orientation ou plan de mission. La stratégie d'audit doit être définie, les objectifs et le périmètre de la mission d'audit doivent être formalisés. Le champ d'investigation, les objectifs généraux et les objectifs spécifiques sont définis dans le rapport d'orientation. Il assure la pertinence des travaux par la concertation avec les responsables audités et le commanditaire, c'est un contrat passé avec l'audit interne ; de plus l'objectivité de la démarche : découpage, objectifs, risques, bonnes pratiques, analyse des risques, ciblage/choix est une garantie d'objectivité et de transparence. Le choix du cadre de référence COBIT offre la possibilité de choisir parmi ses 34 processus celui ou ceux correspondant à la mission d'audit.

La phase de préparation est très importante et nécessite un budget temps conséquent.

2.5.2. La phase de réalisation

Encore appelée phase de vérification, c'est la phase des travaux sur le terrain.
« C'est une phase primordiale de la mission qui à pour objectifs de fournir aux auditeurs des preuves concernant les points faibles présumés et surtout les dysfonctionnements de l'organisation ou des systèmes visités pouvant ainsi mesurer l'impact des conséquences », (LY, 2005 : 72).

2.5.2.1. La réunion d'ouverture

Pour RENARD (2010 :191), « C'est une réunion qui se tient juste avant le début des travaux de vérification, et se tient sur les lieux des travaux ainsi son objet est de présenter le référentiel de l'auditeur. Elle regroupe les auditeurs internes et les responsables audités ».

Il s'agit de la présentation des parties prenantes, de faire des rappels sur l'audit interne, de prendre des rendez-vous et des contacts, de définir les condition matérielles de la mission et de faire un rappel sur la procédure d'audit.

2.5.2.2. Le programme de vérification

Il est établi sur la base d'un référentiel d'audit. Il permet de définir, de répartir, planifier et suivre les travaux des auditeurs. Il indique la liste des tâches à effectuer, des investigations à mener, des questions à poser, les points à voir, des procédures à rechercher.

Selon l'AFAI (2008 b :99), « le programme d'audit permet d'évaluer, de vérifier que ceux-ci sont appliqués et d'évaluer l'efficacité opérationnelle des contrôles. Ces tests et évaluations peuvent aussi porter sur l'efficacité des contrôles ». Différents vérifications et tests peuvent aussi être appliqués dans cette phase.

2.5.2.3. Le travail sur le terrain

« Il consiste à conduire les contrôles prévus dans le programme de vérification. Son point de départ est l'évaluation du contrôle interne. Cette étape permet de garantir que les mesures de contrôle mises en place fonctionnent comme prévu, de façon homogène et continue et d'émettre une conclusion sur le bien-fondé de l'environnement de contrôle », (AFAI, 2008b : 37). Pour RENARD (2010 :132), « l'auditeur doit réaliser sur chacun des points soumis à son jugement critique, une observation complète ; c'est un guide, un fil conducteur qui se compose de toutes les questions potentielles ». Il permet d'identifier pour chaque fonction quels sont les dispositifs spécifiques de contrôles essentiels.

Pendant la phase de réalisation ou d'exécution devra s'informer et confirmer, inspecter, observer, ré exécuter et/ou recalculer, tracer des diagrammes, réaliser des observations physiques, effectuer des rapprochements et reconstitutions et établir des papiers de travail. Ces opérations doivent être précises, cohérentes et fiables. Il faudra dissiper les contradictions apparentes par recoupements. Les feuilles de révélation et d'analyse des problèmes (FRAP) et les feuilles de révélation de risques (FAR) sont élaborées pendant cette phase. Le contenu des FRAP et des FAR permettent de rédiger le rapport d'audit après leur exploitation.

2.5.3. La phase de conclusion

« La rédaction du projet de rapport, la réunion de clôture, la rédaction du rapport définitif, et le suivi des recommandations constituent cette dernière phase », RENARD (2010 :134).

2.5.3.1. Le projet de rapport

Selon RENARD (2010) et THORIN (2000), il porte sur la synthèse des constats et des recommandations qui pourront être discutés avec les audités, cela permet d'affiner le travail et facilite la meilleure acceptation du rapport final par les audités. Cela favorise donc une excellente mise en œuvre des recommandations qui seront formulées par l'auditeur.

2.5.3.2. La réunion de clôture

Il porte sur l'analyse des différents points du projet de rapport.
Elle a pour objet de collecter l'avis des audités sur les constats, raisonnements faits par l'équipe d'audit. Seulement après cette étape que le rapport final est élaboré, (RENARD, 2010 et SCHICK, 2007).

2.5.3.3. Le rapport définitif

Il regroupe les résultats des étapes précédentes. « Le rapport doit communiquer les actions recommandées pour atténuer les faiblesses du contrôle, le comparatif de performance par rapport aux normes et aux meilleurs pratiques pour une vue relative des résultats et le niveau de risque associé au processus », (AFAI, 2008b :157).

Le rapport doit être concis puis faire l'objet d'une rédaction rapide pour qu'il soit déposé à temps. Les recommandations du rapport doivent être économiques et réalistes afin d'être mise en œuvre rapidement et à moindre cout pour l'entité ou l'organisation. L'auditeur présentera pour ce faire un plan d'action. Le suivi des recommandations est donc nécessaire.

2.5.3.4. Le suivi des recommandations

« Bien que l'auditeur ne participe pas à la mise en œuvre de ses propres recommandations, il doit être informé de la suite donnée à celle-ci afin de mesurer l'efficacité, d'alimenter les dossiers et de parfaire les audits ultérieurs », (RENARD, 2010 :189). Pour une logique d'amélioration et de démarche qualité, l'auditeur interne doit effectuer un suivi du plan d'action adopté, des questionnaires peuvent être administrés aux prescripteurs de la mission et aux auditeurs internes.

2.6. Les objectifs de la mission d'audit

La sécurité vise à protéger les actifs informatiques et immatériels de l'entreprise contre les risques et ce d'une manière qui est adaptée à l'entreprise, à son environnement et à l'état de son outil informatique. Les missions d'audit de la sécurité visent à présenter les objectifs recherchés, la revue de l'organisation générale de la sécurité, l'analyse générale des risques, l'évaluation de la sécurité physique, l'évaluation de la sécurité des données et des traitements informatiques et l'examen des dispositifs de protection contre les risques et attaques venus du réseau (interne ou externe). L'audit de la sécurité des données informatiques ou information cherche à déterminer les risques encourus, les analyser et les classer selon leur niveau de gravité. Cet audit porte sur les données informatiques et les composantes du système informatique à travers les points suivants.

Le cadre de référence COBIT pris comme base de référence pour notre étude nous permet d'avoir comme objectifs en audit de sécurité ce qui suit :

2.6.1. La revue de l'organisation générale de sécurité

L'objectif de la l'organisation générale de la sécurité vise à évaluer l'organisation informatique mise en œuvre pour assurer la sécurité et cela ne peut se concrétiser qu'en mettant en place :

- la politique générale et les plans de sécurité ;
- le management et le pilotage de la sécurité ;
- la charte de sécurité ;
- les procédures de gestion opérationnelle de la sécurité ;
- la sensibilisation et la formation du personnel à la sécurité informatique.

Cela correspond à SE 4, DS 7 du cadre de référence de COBIT

2.6.2. L'évaluation de la sécurité physique et environnementale

Cette évaluation permet la mesure du dispositif mis en place pour assurer la sécurité physique et environnementale. Cela se passe par :

- la protection de l'accès physique à l'environnement informatique et lieux de stockage des bandes ou cartouches magnétiques ;
- la protection des locaux contre les catastrophes naturelles ;
- couverture de contrat d'assurance ;
- protection contre la hausse de température et la poussière.

L'objectif de contrôle est de protéger les actifs informatiques et de réduire les risques d'interruption des activités, (processus DS 12 de COBIT). Cela se fait par la maintenance, la fourniture d'un environnement physique adapté afin de protéger l'accès aux ressources informatiques.

2.6.3. L'évaluation de la sécurité des dounées

Il s'agit de faire :

- l'évaluation de la production informatique ;
- l'évaluation des procédures de gestion des accès aux applications et aux données ;
- l'évaluation de la protection et de la confidentialité des données ;
- l'évaluation des autres dispositifs de sécurité.

Cet objectif de contrôle qui correspond au processus DS 11 de COBIT a pour but de protéger les données métiers et de réduire les risques liés à la non confidentialité, la non disponibilité…

2.6.4. L'examen des dispositifs de protection

Cela nécessite :

- l'évaluation des dispositifs de contrôle des accès au réseau de l'entreprise et internet ;
- l'évaluation des mesures et des dispositifs de sécurité de l'exploitation de réseau ;

- l'évaluation des mesures et des dispositifs de protection contre les programmes malveillants ;
- l'évaluation des dispositifs de détection des intrusions ;

Cet objectif de contrôle (processus DS 13 et DS 5 du cadre de COBIT) exige de maintenir l'intégrité du réseau tout en réduisant les attaques ou programmes malveillants de tout genre.

2.6.5. L'aualyse et la gestion du risque

L'analyse du risque a pour objectif la prise en compte de l'environnement informatique sur le risque inhérent et le risque lié au contrôle, cela consiste à évaluer les risques en tenant compte de l'indentification potentielle et du système de contrôle interne mis en place par l'entreprise, et à en déduire la nature des contrôles substantifs à mener avec ou non l'aide de technique d'audit assistée par ordinateur.

Ce processus traduit l'exigence d'analyser et communiquer sur le risque informatique, de même de leur impact potentiel sur les objectifs et les processus métiers. Cela passe par le développement d'un cadre de gestion des risques. Ce cadre doit être intégré à celui de la gestion des risques opérationnels, de l'évaluation des risques, de leur réduction et de la communication sur les risques résiduels. « La gestion des risques doit être intégrée au processus de management, en interne et en externe pour favoriser l'évaluation des risques tout en recommandant, en communiquant des plans d'action pour réduire ces risques », (AFAI, 2008a :122). Par rapport au cadre référence COBIT, cet objectif correspond au processus PO 9.aux auditeurs internes.

Conclusiou

L'évaluation des risques passe par des techniques qualitative et quantitative. L'audit de la sécurité informatique permet à une organisation ou une entité de situer sa maitrise et la gestion des risques pesants sur les données informatiques puis sur le système informatique. L'apport des méthodes, référentiels, standards, normes, tels que MEHARI, COBIT, ISO 27002, ITIL et autres est d'une importance capitale pour prendre des mesures correctives et de se fixer des objectifs en matière de sécurité informatique afin d'aboutir à une meilleure

certification du degré d'assurance de sécurité acceptable. Nous utiliserons le cadre référence COBIT pour notre étude.

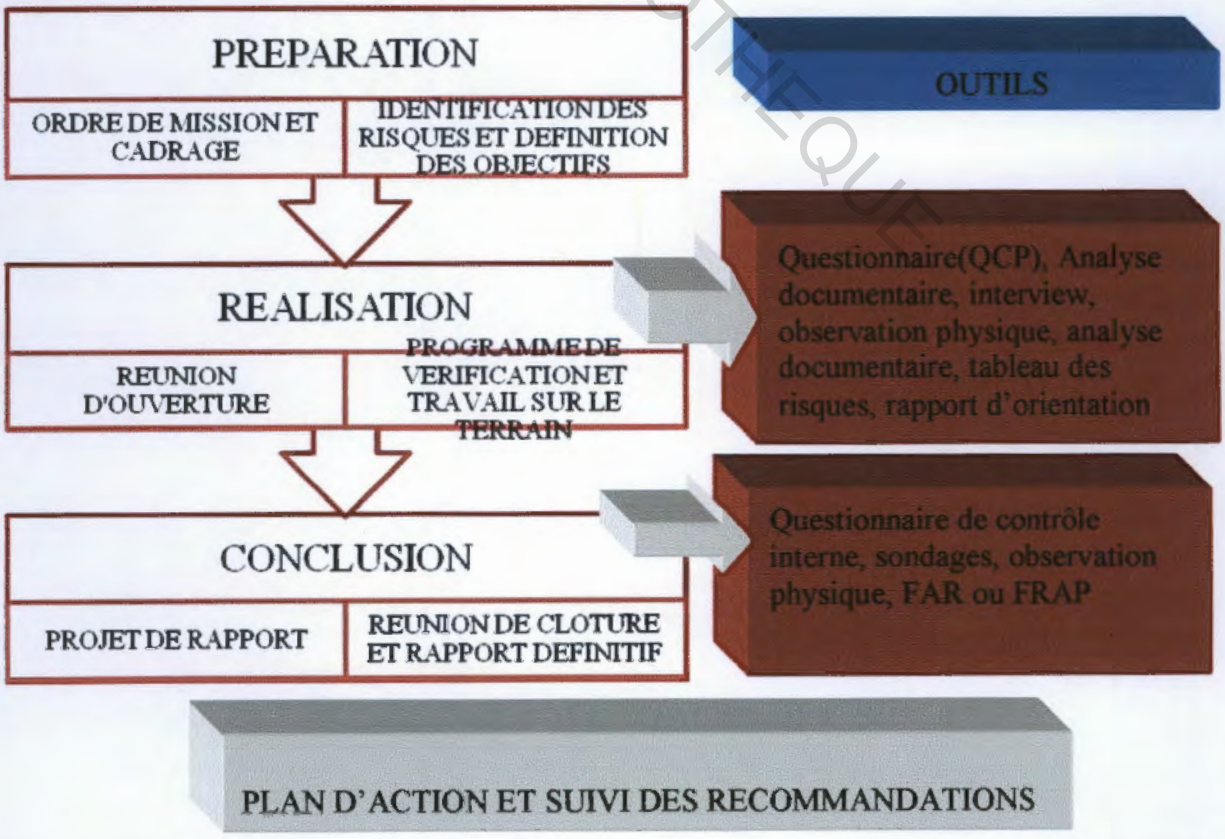
CHAPITRE III : APPROCHE METHODOLOGIQUE

Les chapitres précédents nous ont permis de présenter les données informatiques, leurs supports de stockage donc du système informatique ainsi que l'évaluation du risque informatique en terminant par l'audit de la sécurité informatiques. Notre modèle d'analyse qui nous permettra de mener à bien la partie pratique de notre étude sera présenté dans ce chapitre ; cela se fera par l'élaboration d'une démarche référentielle d'audit de la sécurité des données informatiques. Le travail comportera deux parties. La première portera à la présentation de la démarche référentielle, la seconde mettra en exergue les outils de collecte et d'analyse des données nécessaires à la conduite d'une mission d'audit de la sécurité informatique.

3.1. La démarche référentielle

Le référentiel proposé est basé sur l'approche par les risques et se caractérise par les différentes phases et étapes ainsi que les outils qui y sont associés. Cela se résume par la figure qui suit.

Figure n° 3 : Modèle d'analyse



Source : Nous même

3.2. Les outils de collecte et d'analyse des données

L'objectif de notre étude est de collecter le maximum d'informations sur le processus de sécurité des données informatiques, ainsi nous rabanterons aux responsables intervenant dans ce processus pour collecter les données. Le contrôle interne s'apprécie grâce à divers outils qui sont, soient des outils de collecte d'information ou d'analyse des données.

3.2.1. Les outils de collecte

Ils sont constitués du questionnaire de prise de connaissance, de l'interview, de l'observation physique et des sondages.

3.2.1.1. L'interview

Il permet de collecter des informations auprès de l'interlocuteur relatera les activités qu'il mène. Il contribue à connaitre et comprendre les activités au cœur de l'entreprise ; aussi, il permet avoir connaissance des procédures de fonctionnement de sécurité et déterminer les procédures de contrôle qui gouverne le domaine audité. L'interview permet d'obtenir des explications détaillées sur des faits ou manquements observés.

3.2.1.2. L'observation physique

L'observation physique est outil d'application universelle. On peut observer les processus, les biens, les documents ou les comportements et permet de s'assurer de la réalité, de la permanence ou de conformité des dispositifs du contrôle interne.

Il permet d'identifier et d'observer la mise en application des différents dispositifs de sécurité logique et physique, le contrôle de la sécurité et l'accès aux locaux sensibles.

3.2.1.3. Le questionnaire de prise de connaissance (QPC)

Il permet de à l'auditeur d'avoir une vision de l'ensemble de l'entité et du secteur audité. Il facilite à définir le champ d'application de la mission, de prévoir le travail à accomplir et de concevoir le questionnaire de contrôle interne. Le dépouillement des

informations obtenues permettra de faire une présentation de l'entreprise, de se familiariser avec les procédures et les intervenants dans la sécurité des données informatiques.

3.2.1.4. Le sondage

Le sondage utilisé en audit permet d'extrapoler à partir d'un échantillon prélevé sur l'ensemble de la population les observations faites sur l'échantillon. Il permet de mettre à découvert les dysfonctionnements. Cet outil permettra d'approuver les réponses positives du contrôle interne afin de s'appréhender de l'utilisation des mesures de sécurité.

3.2.2. Les outils d'analyse et diagnostique

Dans cette liste, on a l'analyse documentaire, le tableau des risques, le questionnaire du contrôle interne, les FRAP et les FAR.

3.2.2.1. L'analyse documentaire

Elle porte sur l'exploitation des documents de l'entité faisant l'objet de l'étude. La consultation des documents permettra de tirer le maximum des informations afin d'avoir une connaissance approfondie de l'entité sur lequel porte l'audit. Elle facilite le rapprochement des données pour les vérifications et elle est permanente pendant l'audit.

3.2.2.2. Le questionnaire du contrôle interne

Il porte sur chaque fonction et objectif de l'entreprise, et se présente sous forme de questionnaire préétabli. Il s'intéresse aux différents points du contrôle interne en relevant les mesures existants, en constatant les forces et les faiblesses du processus de sécurité informatique mis en place.

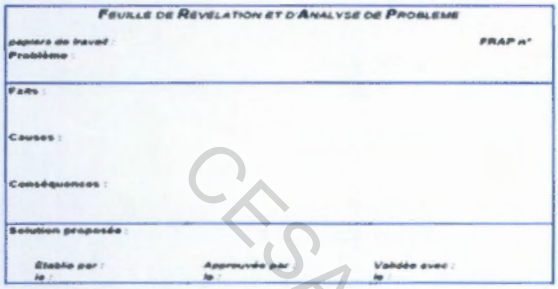
3.2.2.3. La FAR et La FRAP

Ce sont les outils d'analyse des problèmes rencontrés(FRAP) et des risques identifiés(FAR) pendant la mission d'audit. La FAR est constituée des éléments qui suivent : types de risque identifié, faits constatés, causes explicatives, conséquences réelles ou

potentielles puis les recommandations ; quand à la FRAP, elle a pour éléments : problèmes, faits, cause, conséquences enfin les solutions.

L'assemblage des FAR ou des FRAP de façon ordonnée constitue la structure même du rapport.

Figure 4 : FRAP


FEUILLE DE REVELATION ET D'ANALYSE DE PROBLEME

papiers de travail :
Problème :
FRAP n°

Faits :

Causes :

Conséquences :

Solution proposée :

Etablie par : le :
Approuvée par : le :
Validée avec : le :

Source : Cabinet A.S Consulting

Conclusion

Dans ce chapitre, nous avons déroulé la démarche référentielle que nous allons pratiquée sur le terrain. Nous avons aussi présenté les outils que nous utiliserons pendant la mission d'audit de la sécurité des données informatiques de la S.N.E. C'est sur ce chapitre que nous mettons fin la revue de littérature.

CONCLUSION DE LA PREMIERE PARTIE

La première partie nous a permis de présenter les données informatiques, les éléments du système informatique, les risques qui y sont liés ainsi que les dispositifs de sécurité.
La mise en œuvre d'une politique de sécurité, par la Direction Générale, est capitale pour la survie de l'organisation ; sa mise en œuvre nécessite le respect des normes et lois internationales.

Les données informatiques constituent le capital immatériel de la SNE dans la mesure où toutes les entreprises ont la tendance actuelle d'informatiser la quasi-totalité de leur activité. La sécurité des données informatiques est d'actualité et s'impose à toute organisation.

Connaitre le niveau de sécurité des données informatiques impose un audit adéquat car cela attirera l'attention des dirigeants de la S.N.E sur les dangers qui pèsent sur les données et le système informatique puis favorisera la détermination des axes d'amélioration afin d'accroitre la performance.

DEUXIEME PARTIE : CADRE PRATIQUE

La modernisation des entreprises suite à la mondialisation implique la croissance de leur performance. Pour cela, elles sont dans la procédure d'informatiser la quasi-totalité des processus d'activités. Cette informatisation les expose à des nouveaux risques.
La maitrise des risques des données informatiques est jugée suite aux mesures sécuritaires mises en place.

La sécurité informatique se justifie par la mise en place des mesures technique et organisationnelle affinées.

L'activité qu'exerce la SNE ne l'exclut pas à des risques informatiques du fait de l'informatisation de ses processus et surtout l'importance de sa clientèle. Il est par conséquent important, de procéder à un audit de la sécurité des données informatiques. Cet audit représentera ainsi l'objet de cette deuxième partie.

Nous présenterons dans cette partie la SNE, la structure de ses données informatiques, le système informatique et les dispositifs de sécurité informatique ; ensuite nous présenterons nos travaux d'audit afin de clôturer à la présentation des résultats de notre étude.

CHAPITRE IV : PRESENTATION DE LA S.N.E

La société Nationale d'Electricité découle de la volonté politico-économique en ce qui concerne le besoin de l'énergie électrique. Il est important pour nous de présenter la structure qui nous a reçu pour le stage ainsi que les données informatiques, le socle de notre étude.

4.1. Présentation succincte de la S.N.E

Cette section portera sur l'histoire, les missions, son statut juridique ainsi que son organisation afin de bien comprendre le rôle de la S.N.E.

4.1.1. Historique

L'histoire de la S.N.E remonte pendant la décennie 1930-1940.
En effet, c'est en pleine colonisation française qu'une société dénommée Union Electrique d'Outre Mer UNELCO s'est installée à Brazzaville son but essentiel est la production, la distribution et la commercialisation de l'énergie au profit des usagers.
En 1938, UNELCO signe un contrat de partenariat avec la société Force Bas Congo du Congo Belge. Un câble sous fluviale est posé entre Brazzaville et Léopoldville actuelle Kinshasa.

En 1953, une autre société, la société Equatoriale d'Energie Electrique (S.E.E.E) s'installe à Brazzaville et met en service la centrale hydroélectrique de Djoué. Dans le cadre l'amélioration de la qualité de l'énergie fournie, en 1953, la SEEE et l'UNELCO signent un contrat de mise en valeur des réserves d'énergie électrique avec la société Force Bas Congo qui exploite la centrale hydroélectrique de Zongo d'une puissance de 61MW et les deux rives du fleuve Congo (Brazzaville et Léopoldville) sont connectées.

Sous le régime du socialisme scientifique des années soixante, l'Etat congolais initie et s'engage dans la nationalisation de nombreuses entreprises jadis privées issues de la colonisation. Celles-ci deviennent ainsi entreprise d'Etat.
La société Nationale d'énergie crée le 15 juin 1967 par la loi n° 06/67 du 15juin 1967 puis débaptisée en Société Nationale d'Electricité par la loi n° 67/84 du 11 septembre1984, la SNE devient ainsi une entité paraétatique.

4.1.2. Statut juridique

La SNE est un organisme d'Etat à caractère technique, industriel et commercial doté de la personnalité civile et jouissant d'une autonomie financière. Elle est régie par une convention collective adoptée en 1991 établie conformément à la loi n° 45/75 du 16 Mars 1975 instituant le code du travail en République populaire du Congo et la loi n°06/96 du 6 Mars 1996 modifiant et complétant certaines dispositions de la loi n° 07/72 du 1er Février 1972, portant statut général des entreprises d'Etat est crée. Elle a la qualité de commerçant, son capital est constitué par des apports en espèces ou en nature fait par l'Etat et les collectivités publique, que ses biens sont considérés comme une partie de l'Etat, qu'elle est placée sous la tutelle d'un ministère ou organisation spécialisée de l'Etat, ou d'une collectivité publique expressément dotée du pouvoir de tutelle.

4.1.3.. Missions

La SNE a pour mission de produire, de transporter, de distribuer et de commercialiser l'énergie électrique sur l'ensemble du territoire national. A ce titre, l'étude et la réalisation des ouvrages en vue de la production et de la distribution de l'énergie électrique font partie intégrante de ses attributions.

La SNE possède trois barrages hydroélectriques :

- le barrage hydroélectrique de Moukoukoulou avec une puissance de 74MW;
- le barrage hydroélectrique d'Imboulou, il fournit une puissance de120 MW;
- le barrage hydroélectrique du Djoué avec une puissance 15MW; il n'est plus en activité depuis l'année 2007 suite à une noyade
- et une centrale à gaz qui a une capacité de production de 450 MW.

La SNE distribue et commercialise aux usagers la moyenne et la basse tension.

4.1.4. Organisation

Située sur l'avenue Denis SASSOU NGUESSO, la SNE est dirigée par un Directeur Général nommé lors d'un conseil de ministres. Il a sous sa direction un secrétariat général, un secrétariat particulier, l'assistant du Directeur Général et différent départements.

A ceux-là s'ajoutent les directions centrales détenant le monopole d'exploitation des activités de la SNE qui, engagent la société dans l'initiative des décisions stratégiques à moyen et long terme, qui sont :

- la direction de la production et du transport,
- la direction des ressources humaines et du patrimoine,
- la direction financière et comptable,
- la direction de la distribution et de la commercialisation.

Sur le plan territorial, la Direction Générale dispose de cinq directions départementales, et dispose également de deux secteurs, telle que présenté dans l'annexe n°1. Nous avons passé notre stage au département d'audit et contrôle de gestion dirigé par un chef de département et qui se compose du :

- secrétariat ;
- service Audit et Contrôle de Gestion Financier et Comptable ;
- service Audit et Contrôle de Gestion Administratif ;
- service Audit et Contrôle de Gestion Commercial, approvisionnement et stock.

Nous avons collecté les informations au département informatique.

4.2. Les données informatiques

Les données informatiques de la SNE issues des traitements automatiques sont essentiellement comptables, commerciales et gestion des ressources humaines et bientôt la gestion des stocks. Les données comptables sont gérées par l'application Sage et les données commerciales et des ressources humaines sont gérées par des applications développées à partir du logiciel Windev.

4.3. Le système informatique

La SNE est équipée d'un système informatique qui assure le traitement des données de ses activités (comptabilité, gestion de la clientèle, facturation et paie) ; ce système est géré par le centre informatique.

4.3.1. Le réseau informatique

Le Centre informatique ou service informatique a la charge de gestion du réseau informatique qui comporte deux réseaux indépendants à savoir :

- le réseau de comptabilité de la direction de Brazzaville-Pool. Le serveur se trouve dans le bureau du chef de service comptabilité et le logiciel sage y est installé;
- le réseau reliant le département informatique, le bâtiment du centre informatique et les différentes directions et départements du siège social.

  Ce réseau a quatre serveurs qui sont logés dans le bâtiment du centre informatique dont trois déploient l'application sage qui gère la comptabilité et le GDC qui est une application pour la gestion de la clientèle et la GRH.L'application GRH a servi grâce au logiciel windev à développer les applications GRHS (gestion des ressources humaines- solde) et GRHP (gestion des ressources humaine- personnel). Les applications GDC et GRH ont été développées grâce au logiciel windev. Le quatrième serveur, configuré sous le système linux est celui de l'internet. Les serveurs et applications utilisent les mêmes canaux et les mêmes switch ; tous les signaux des différents serveurs passent dans un même switch mais la plage d'adresse est scindée.

Les postes des agences se connectent au serveur à partir d'une liaison télécom (liaison à boucle radio) ; seule l'application GDC se déploie dans ces agences.

Dans l'avenir, le serveur qui se trouve dans le bureau du chef de service administratif et financier de Brazzaville-Pool sera ramené au centre informatique et le réseau internet sera isolé.

Les serveurs et les systèmes de gestion des réseaux que l'on trouve à la SNE sont résumés dans le tableau qui sui.

Tableau n° 3 : Les serveurs et les applications

Modèle	Système d'exploitation réseau
HP Proliant ML 350G6 (Comptabilité)	Windows Server 2008
HP Proliant DL 370G6(Gestion de la clientèle)	Windows Server 2008
Server Super7 Proxy internet	Système Linux
HP proliant ML 350(Gestion de paie)	Système Linux
DELL Power Edge 440(Comptabilité)	Windows Server 2003

Source: Nous- même

En l'absence de l'état récapitulatif du matériel informatique, nous avons pus comptabilisé en faisant de porte à porte au siège :

- 82 ordinateurs de bureau dont 45 seulement se connectent au réseau informatique avec accès sélectif;
- 43 imprimantes ;
- 21 ordinateurs portables.

Conclusion

Nous venons de faire une brève présentation de la S.N.E, de ses données informatiques et des éléments constituants son système informatique.

Cette présentation terminée, nous allons effectués une description des mécanismes ou processus de sécurité et des acteurs ou services participants à la sécurité informatique et nous finirons par présenter le déroulement de nos travaux d'audit.

CHAPITRE V : PRESENTATION DES MECANISMES DE SECURITE INFORMATIQUE A LA SNE

Dans ce chapitre, nous présenterons les acteurs qui interviennent dans la sécurité informatique et les dispositifs de sécurité informatique que nous avons pus identifier à la SNE tout en suivant les objectifs de notre recherche.

5.1. Les protagonistes de la sécurité informatique

Il est question des services, des départements, des directions ou des personnes qui concourent à la sécurité des données informatiques.

5.1.1. Le département informatique

Ce département est animé par le chef de département informatique. Il a sous sa tutelle plusieurs collaborateurs qui sont repartis en plusieurs services, divisions et section comme présenté dans l'annexe n°2 à la page 100.

5.1.1.1. Le chef de département informatique

Il a pour attributions prioritaires de :

- veiller à l'application des stratégies informatiques de la SNE,
- veiller à ce que la SNE soit à la pointe de l'éveil technologique,
- veiller au bon fonctionnement du système informatique,
- veiller à la sécurité des données ou de l'information,
- assurer le rôle de conseil en équipement informatique,
- veiller et mettre en place les politiques de sauvegarde de l'information.

5.1.1.2. Le chef du service ou centre informatique

Il a pour rôle :

- d'assurer l'interface entre le bureau d'étude et d'exploitation,
- de veiller sur l'organisation des équipes d'exploitation,

- de veiller à la sécurité du matériel (serveurs et autres machines)
- de veiller à la sécurité du personnel,
- de veiller et mettre en place les dispositifs de sécurité du bâtiment abritant le centre informatique

5.1.1.3. La division exploitation

Elle a pour rôle :

- d'assurer la sécurité des données,
- d'assurer l'exploitation et la maintenance des logiciels,
- d'assister les utilisateurs.

5.1.1.4. La division maintenance et réseau

Elle comme attributions de :

- veiller au bon fonctionnement du réseau,
- veiller au bon fonctionnement des équipements informatiques,
- assurer la maintenance des équipements informatiques,
- assurer la maintenance et l'installation du courant onduleur et du générateur électrique.

5.1.2. Le service de protection du patrimoine

Il a pour rôle de:

- veiller à la surveillance et le gardiennage du patrimoine de la S.N.E ;
- veiller à la protection et la prévention contre l'incendie ;
- veiller à l'hygiène et l'assainissement des installations de la S.N.E ;
- produire les statistiques des accidents.

5.1.3. Le département Audit et contrôle interne

Selon la charte d'audit de la SNE, ce département a pour objectif général de donner à la Direction Générale l'assurance raisonnable que la SNE est gérée de manière saine et efficace. Pour ce faire, il s'assure que :

- les ressources et actifs de la SNE sont dûment enregistrés dans ses grands livres et préservés comme il convient ;
- les données financières, opérationnelles, comptables et autres qui sont générées par la SNE ou utilisées pour sa gestion sont exactes et fiables ;
- l'application des procédures et méthodes de gestion et de fonctionnement du contrôle interne sont efficaces et respectées ;
- les opérations de la SNE, ainsi que diverses fonctions et activités, sont réalisées de façon efficace et rentable.

Il couvre les domaines suivants :

- les activités financières et comptables, techniques et auxiliaires y compris leur suivi, la gestion du portefeuille et de la trésorerie ;
- les activités de production, transport et distribution d'électricité ;
- les systèmes d'information de gestion et des technologies d'information, y compris les aspects relatifs à la sécurité et au contrôle des systèmes d'informatiques ;
- toutes les autres activités, y compris les ressources humaines et les fonctions administratives.

5.2. Les dispositifs de sécurité informatique à la S.N.E

Le processus de sécurité implique plusieurs services. Il se trouve, qu'il n y a pas de manuel de procédure précisant des mesures à prendre en matière de sécurité informatique dans son ensemble. Nonobstant, en s'appuyant sur les interviews et les observations sur le terrain, nous allons décrire dans cette section, les mesures de sécurité que nous avons pu relever.

5.2.1. La gestion et l'évaluation des risques

Nous avons constaté qu'au niveau de la S.N.E, qu'il n'y a pas un processus de gestion et d'évaluation des risques informatiques.

5.2.2. La sécurité du système

Ici, nous présentons des mesures mis en place pour assurer la sécurité logique et la protection des données.

5.2.2.1. La gestion des identités et des comptes utilisateurs

La gestion des habilitations dans GDC, GRH et Sage se fait au niveau d'une table de paramétrage de GDC, GRH et Sage.
L'administrateur de base de données octroie des droits en fonction des responsabilités de chaque utilisateur. La liste non exhaustive des droits des utilisateurs liés à la gestion des clients sont les suivants selon que l'opération concerne la facturation, le recouvrement, portefeuille : création échéancier BT, annulation factures impayées, annulation avoir, régularisation d'un paiement, mise à jour des soldes client, visualisation paiement client, visualisation factures, insertion frais de coupures, saisie/correction de la relève, résiliation police. Un login ou code utilisateur et un mot de passe sont exigés avant le lancement des applications GDC, GRH et Sage. Le mot de passe renferme au moins six caractères avec une durée limitée. Certaine machine qui utilise les applications GDC, GRH, et Sage oblige l'utilisateur un mot de passe pendant le démarrage.

Le Serveur de données clients est arrêté en fin de journée et relancé en début de matinée pour des raisons d'intempéries. Le démarrage du Serveur des données exige un mot de passe Root, puis le démarrage du service Smb qui exige un code enfin on démarre le Shmod 777/hod/données.

5.2.2.2. Prévention, détection, neutralisation des logiciels malveillants

La S.N.E utilise le logiciel anti-virus McAfee version 8.7i avec licence et mis à jour, aussi, dans certaine machine, le logiciel KAPERSKI est installé.

5.2.2.3. Sécurité du réseau, échange des données

Le réseau dispose d'un serveur super 7 PROXY Internet avec un système d'exploitation Linux sans anti-virus qui reçoit la connexion internet.

5.2.2.4. La sauvegarde et l'archivage des données

Les sauvegardées de la base de données sont journalières, hebdomadaires et mensuelles :

- la sauvegarde journalière a pour but de garder une image fidèle des données d'exploitation. La sauvegarde des données se fait avec un disque amovible et les serveurs ;
- la sauvegarde hebdomadaire vise à garder une image fidèle des données. La sauvegarde se fait dans un disque amovible ;
- la sauvegarde mensuelle permet de conserver une image fidèle des données (exploitation et back up). La sauvegarde se fait dans un disque amovible.

Suivant la capacité du disque amovible, les données peuvent être sauvegardées jusqu'au plus 3mois. Les sauvegardes de la comptabilité et de la paie se font sur les serveurs.
L'archivage des données de la comptabilité et de la paie se fait à la direction financière et comptable.

5.2.3. La gestion de l'environnement physique

Nous allons présenter ici, les mesures de sécurité physique que nous avons pu identifier pendant la phase de prise de connaissance.

5.2.3.1. Mesures de séeurité physique/ Accès physique

Les employés ont des obligations qui cadrent dans la sécurité, ainsi l'article 32 et 33 du règlement intérieur de la S.N.E stipulent que :

- tout travailleur à le devoir de préserver le patrimoine de l'entreprise,
- Il est formellement interdit au personnel de fumer dans l'entreprise, d'intervenir pour toute opération de dépannage ou de maintenance sur tous les matériels en service dans l'entreprise lorsqu'il n'y est pas habilité.

Les éléments de la force publique assurent la garde à l'entrée du bâtiment administratif et dans le bâtiment qui abritait les ateliers, la relève des équipes se fait mensuellement. De plus, une société de gardiennage G.B.S sous contrat assure la protection des locaux. Deux agents sont placés aux deux entrées sur les quatre du bâtiment administratif. Une entrée est réservée spécialement pour le Directeur général et la quatrième est celle occupée par les éléments de la force publique cités ci haut. Deux éléments de la compagnie de gardiennage occupent les deux entrées du siège et un est posté à l'entrée du domicile Directeur Général. Les agents de la société de gardiennage en poste au bâtiment administratif et du domicile du Directeur Général disposent de registres où ils doivent inscrire la date, les noms des personnes qui accèdent dans ces bâtiments, le service de destination, l'heure d'arrivée et l'heure de départ.

Un agent est placé à l'entrée du centre informatique qui, interdit toute personne hors de la S.N.E d'y entrer et il est tenu d'assurer la liaison entre les visiteurs du centre informatique et les agents du centre informatique. Les fenêtres du centre informatique sont protégées par des grilles métalliques qui prennent support dans les murs du bâtiment.
Le centre informatique dispose de deux entrées :

- la première sert d'entrée principale, elle dispose de deux portes, une en planche avec des grilles métalliques, la deuxième est faite en métal et les deux portes ferment à clé ;
- la deuxième sert d'issue de secours, la porte est faite en métal en plus elle ferme à clé et crochet.

Certains composants du système informatique disposent d'un numéro d'immatriculation. Les câbles réseaux se trouvant dans les bureaux sont abrités dans des

goulottes. Les câbles électriques et les câbles réseaux reliant les différents bâtiments sont enterrés. Les liaisons radio qui relient les agences et le centre informatique disposent des antennes à vis-à-vis.

5.2.3.2. Protection contre les risques liés environnement

Le nettoyage du centre informatique est assuré par un agent du centre informatique par contre dans le bâtiment administratif, le nettoyage est assuré par la société BALAI MAGIQUE qui est sous contrat. Les appareils et serveurs se trouvant dans la salle des machines sont habituellement soufflés par un souffleur qui se trouve dans le centre informatique. La salle des machines qui abrite les serveurs dans le centre informatique dispose de trois climatiseurs Split réglés à dix huit degré Celsius mais il ya absence des outils de mesure de la température.

Le centre informatique dispose aussi de sept climatiseurs qui assurent le conditionnement de l'air dans son ensemble.

5.2.3.3. La gestion des installations matérielles

Le centre informatique dispose de trois extincteurs rangés dans trois bureaux différents du centre informatique. L'arrivée du courant électrique passe par un onduleur de 70 KVA avec des batteries d'une autonomie de 30 minutes qui le distribue à tous le matériel du réseau informatique. Le courant électrique arrive au centre informatique par une seule arrivée puis passe par un tableau électrique avant d'alimenter les équipements. La salle des machines dispose d'un dispositif de détection/extinction d'incendie. Sur le bâtiment administratif un paratonnerre est installé pour protéger les installations électriques contre la foudre.

Conclusion

Nous sommes passés en revue sur un ensemble d'éléments pour avoir un aperçu sur la sécurité informatique à la Société Nationale d'Electricité à travers la présentation des acteurs ou services intervenant dans ce domaine et la description des mesures de sécurité existantes,

ceci pour se faire connaitre l'état des lieux. Nous passerons au prochain chapitre qui portera sur les travaux et les résultats de notre audit à la S.N.E.

CHAPITRE VI : LES TRAVAUX ET LES RESULTATS DE L'AUDIT

Suite à la non réalisation des missions d'audit informatique par le département d'audit de la SNE, nous avons mis en œuvre nos connaissances acquises pendant la formation pour la réalisation de cet audit. L'entretien, la revue documentaire, l'inspection des locaux et des appareils, l'observation et les tests de validation ou de confirmation sont les diligences ou activités mises en œuvre pour la réalisation de nos travaux. Ici, nous présenterons le déroulement de nos travaux d'audit et nous ferons une synthèse des forces et faiblesses qui en ressortent. Les faiblesses et/ou forces constatées conduirons à des recommandations afin de corriger les faiblesses et de renforcer les dispositifs existants.

6.1. Les séquences de la mission d'audit

La mise en œuvre de notre modèle ici nous emmène à étaler les outils retenus et de retenir les points les plus capital.

6.1.1. La préparation et le cadrage de la mission

C'est l'étape où interviennent l'ordre de mission, l'établissement du questionnaire de prise de connaissance, la définition du champ d'action, le choix de l'échelle de l'évaluation des risques.

6.1.1.1. L'ordre de mission

Il doit émaner de la plus haute autorité de la SNE donc la Direction Générale ; elle à pour objet ici, l'audit de la sécurité des données informatiques. Son objectif principal est de s'assurer du niveau de sécurité des données informatiques dans l'optique de réduire l'exposition aux vulnérabilités et sinistre et de minimiser les risques ; ses objectifs spécifiques sont :

- s'assurer de la gestion et de l'évaluation des risques informatiques;
- s'assurer de la mise en place des dispositifs de sécurité logique des données ;

- s'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques ;
- s'assurer de la mise en place d'un système de droit d'accès aux données informatique ;
- s'assurer d'une bonne sauvegarde des données issues des traitements informatiques.

Les destinataires de cet ordre de mission sont : le département informatique, la direction financière et comptable, la direction commerciale, département sécurité et les utilisateurs tout en précisant la date de la mission.

6.1.1.2. Le questionnaire de prise de connaissance

Il nous a permis de nous acclimater de l'environnement interne ou externe de la SNE. Il nous a permis de faire une présentation de la SNE, elle a le monopole sur le marché de l'électricité et de repérer les services ou acteurs impliqués dans la sécurité informatique (données). La revue des documents de travail interne nous a permis de nous familiariser avec l'activité informatique. La visite des locaux nous a permis d'avoir un premier contact avec les responsables et le personnel intervenant dans l'activité informatique et la sécurité en général. Ce questionnaire se résume dans l'annexe n°3

La compréhension du fonctionnement des services ou départements de la SNE ou familiarisation s'est faite grâce à des interviews ou entretiens que nous avons eu avec certains responsables et agents (voir annexe n°4). Une visite des locaux abritant les serveurs était faite en compagnie d'un agent informatique, ceci pour localiser le centre informatique et la salle des machines.

Vu l'indisponibilité du chef de département informatique à cause de son état de santé, nous avons eu un entretien avec le chef de service études et maintenance des logiciels pour prendre connaissance des dispositifs de sécurité existants. Les tests de confirmation ou de validation on été réalisés, nous avons procédé à l'observation, à l'inspection des locaux et du matériel informatique. Le tableau ci-après résume notre entretien, les tests de confirmation et de validation, les observations, l'inspection des locaux et du matériel informatique.

Tableau n°4 : Identification et évaluation des dispositifs de sécurité informatique

Section	Oui/Forces	Non/Faiblesses
Sécurité physique		
Infrastructure physique		
Qualité des murs et des fenêtres	✓	
Détection d'intrusion (alarme, gardiennage)		✓
Protection incendie		
Dispositif détection/extinction	✓	
Etat du dispositif détection/extinction		✓
Protection électrique		
Onduleur avec batterie est en place sur chaque serveur	✓	
Climatisation	✓	
Contrôle des accès		
Contrôle des accès (jour)	✓	
Condition de fonctionnement		
Hygiène-propreté	✓	
Rangement des locaux informatiques		✓
Maintenance du matériel		
Existence des contrats pour les serveurs		✓
Un personnel spécial de la SNE	✓	
Plan de secours informatique		
Existence et documentation		✓
Sécurité logique		
User-id et mot de passe au démarrage		✓

User-id et mot de passe à l'entrée des applications	✓	
User-id et mot de passe sont personnels	✓	
Renouvellement régulier des mots de passe	✓	
Gestion des profils d'accès sur les données bureautiques		✓
Antivirus sur serveur et postes	✓	✓
Mise à jour antivirus		✓
Verrouillage des configurations système		✓
Procédure de sauvegarde		
Stockage externe		✓
Sauvegarde des postes individuels(PC)		✓

Source : Nous même

L'évaluation des dispositifs de sauvegarde se présente dans le tableau ci-après

Tableau n°5: Evaluation des dispositifs de sauvegarde

Cycle	**Contenu**	**Jeux**	**Stockage** (lieu, condition, accès…)
Quotidienne	Données et applications	1	Disque amovible
Hebdomadaire			

Source : Nous même à partir de CLEUT & al (2008a : 57-59)

Le disque amovible n'a pas de lieu de conservation fixe et est souvent gardé le soir à la maison du responsable de la gestion de la base des données.

Du fait de la non réalisation des missions d'audit informatique et d'une matrice d'évaluation des risques par le département d'audit et contrôle de gestion malgré ses attributions, nous proposons une matrice d'évaluation des risques dans le tableau suivant :

Tableau n° 6 : Matrice d'évaluation des risques

Niveau du risque	Evaluation de l'impact	Nature des travaux
1	Faible	Contrôle par intermittence
2	Moyen	Sondage et inspection
3	Elevé	Contrôle exhaustif

Source : Nous même adapté à l'approche de RENARD (2010)

La recherche des éléments probants passera par des tests à base de ce tableau.
Suite aux objectifs de notre mission d'audit, les travaux se focalisent sur les éléments que contient le tableau qui suit :

Tableau n° 7 : Champ d'action des travaux d'audit

Lieu et local	Population
Centre informatique	Ordinateur du réseau
Salle des machines	Tous les serveurs
Bloc administratif	DRHP, DFC, DS
	Responsables impliqués dans la sécurité

Source : Nous même

Après la définition du champ d'action, l'exécution de la mission ou travaux d'audit s'amorce.

6.1.2. Les travaux d'audit sur le terrain

L'achèvement du questionnaire de contrôle interne et son administration aux acteurs potentiels cimentent cette étape ; puis nous avons conçu un planning de travail qui intègre aussi des travaux d'expérimentation ou de vérification sur le terrain. Nous signalons qu'une note de service était initiée par le Directeur des ressources humaines et de la gestion du patrimoine puis envoyée dans les directions ou services qui sont dans notre champ d'action ; cela a eu comme conséquence, la non tenue de la réunion d'ouverture classique.
Le programme d'audit est consolidé dans le tableau qui suit.

Tableau n°8: Programme d'audit

Objet	Département, service/Lieu	Type de taches
Questionnaire du contrôle interne	-Affaire juridique et gestion du patrimoine, -Service méthode et maintenance des logiciels, -Service client (caisses) -Service paie, budget, comptabilité	-S'informer et valider - Observer
Sécurité logique	-PC utilisateurs -Serveurs	-Inspecter -Observer
Sécurité physique	Centre informatique	-Inspecter -Observer

Source : Nous même

Ici, nous procédons à l'établissement des FRAP et des FAR suite à des réponses négatives du questionnaire du contrôle interne. La réponse négative du questionnaire de contrôle interne constitue une faiblesse et la réponse positive constitue une force qui devra être validée.

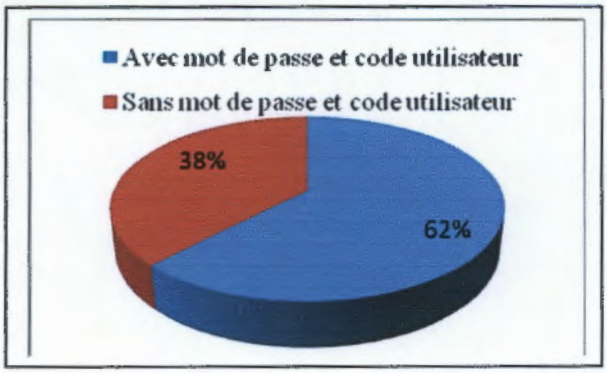
Les tests de la confirmation du questionnaire de contrôle interne qui suivent, découlent du programme de travail conçu à partir des réponses positives du questionnaire du contrôle interne.

II-a-1- Sélectionner un échantillon d'utilisateurs (GDC, GRH, Sage), vérifier qu'un mot de passe et code utilisateur sont exigés pour procéder aux traitements des données.

Figure n° 5: Exigence de mot de passe et code utilisateur pour tout traitement des données

Population : 62

Echantillon : 45



Source : Nous même

II-a-2-Sélectionner un échantillon de PC, vérifier que l'anti-virus McAfee ou KARSPESKY est installé.

Figure n°6 : Antivirus McAfee ou KARSPESKY est installé sur les PC

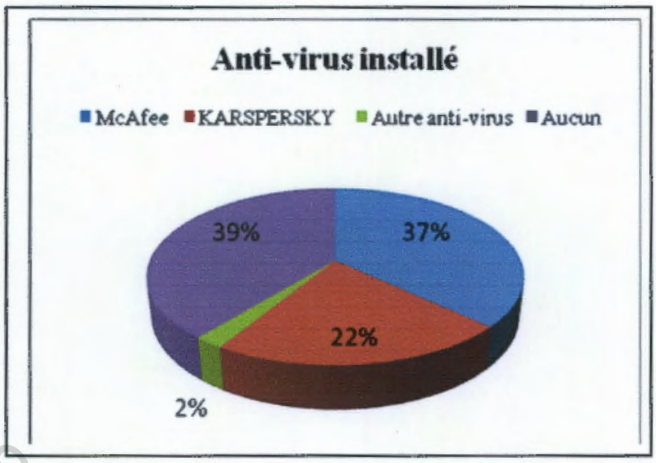
Population : 45

McAfee : 17

KARSPERSKY : 10

Autre anti-virus : 1

Aucun :18



Source : Nous même

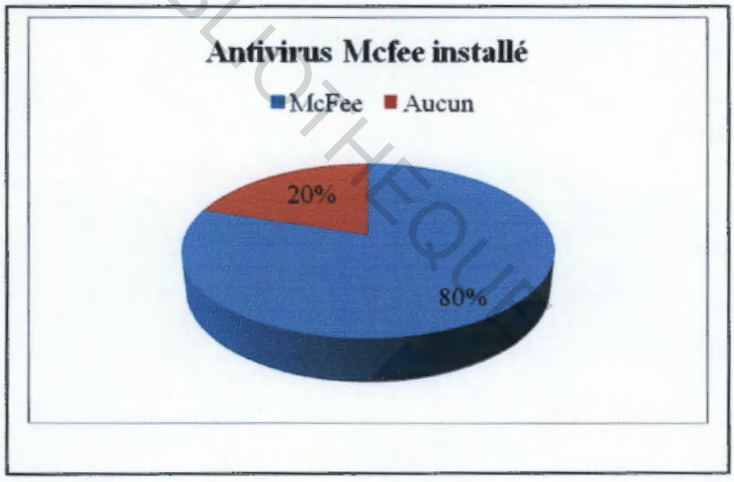
II-a-2-1-Vérifier que l'anti-virus McAfee est installé dans les serveurs.

Figure n° 7: Anti-virus McAfee installé

Population : 5

Installé : 4

Aucun :1



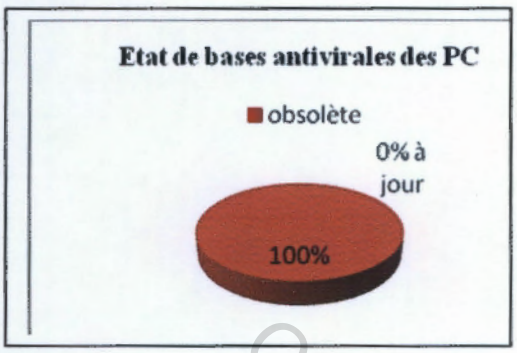
Source : Nous même

II-a-2-1-Vérifier que les bases des antivirales sont à jour.

Figure n°8 : Etat de bases antivirales des PC et des serveurs

Population : 45

(Issue de II-a-2)



Population serveur : 5

Source : Nous même

V-c-1-Vérifier que sur les serveurs, PC et Switch les onduleurs sont installés

Population serveur : 5

Population PC : 45

Population Switch : 11

Echantillon : 7

Figure n°9 : Etat des PC, serveurs, et switch reliés à l'onduleur principal et/ou à un onduleur secondaire

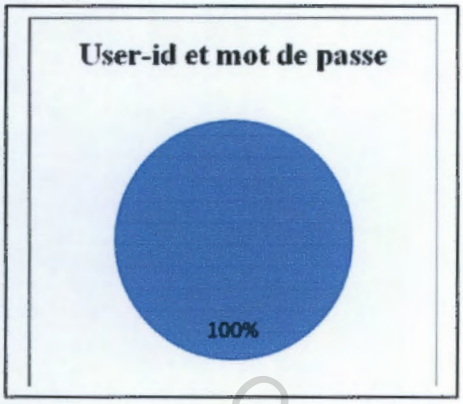
Source : nous même d'après les réponses positives du questionnaire de contrôle interne.

Le test (II-a-2-1) nous à permis de constater qu'un seul serveur possède un anti-virus et le test (II-a-2-1) à montré que les bases antivirales sont obsolètes.

III-Vérifier qu'un User-id et mot de passe sont exigés à l'entrée des applications

Population : 45

Figure n°10 : Exigence d'user-id et mot de passe à l'entrée des applications

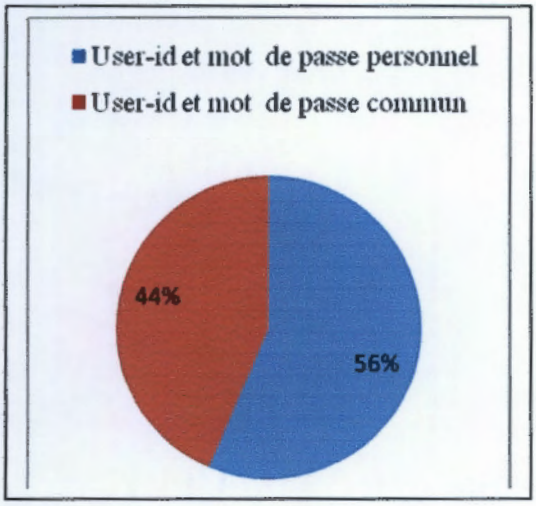


Source : Nous même

Vérifier que l'User-id et le mot de passe sont personnels

Population : 45

Figure n°11 : User-id et mot de passe sont personnels



Source : Nous même

Les vérifications ont permis de constater que les utilisateurs ont des habilitations précises suivant les fonctions et les responsabilités

L'inspection du bâtiment du centre informatique, l'observation et le contrôle des dispositifs de sécurité ont conduit aux constats suivants:

- état et qualité des portes : double portes métalliques à l'entrée principale et une porte de secours en métal. Les trois portes en vitre du couloir qui mène à la salle des machines n'existent plus et sont entreposées contre le mur dans le couloir. La porte qui mène à la salle des machines est en vitre et se ferme hermétiquement. Trois bureaux reliés au couloir n'ont plus de portes.

- qualité des fenêtres et vitrage: vitrage avec lamelle de vitre hermétique, grille métallique à l'extérieur.

- qualité des murs: murs extérieurs solides doublés à l'intérieur d'un contre plaqué, les cloisons intérieurs sont en partie en contre plaqué.

- état du plafond: double plafonds (un en contre plaqué et l'autre est un faux plafond), le faux plafond est en état de délabrement et laisse les câbles réseaux à porté de vue, de plus cet état de délabrement peut conduire à la variation de la température dans la salle des machines.

- système de détection incendie: présence d'un système de détection/extinction qui n'est plus en état de fonctionner.

- alarme automatique ou manuel: aucune alarme ou de dispositif (alarme, téléphone) reliant aux sapeurs pompiers.

- extincteurs: aucun extincteur à porter de vue au couloir, mais présence de trois extincteurs en poudre en poudre repartis et rangé dans les coins de trois bureaux distincts.

- extincteurs entretenus: aucun.

- protection des câbles: câbles dans les goulottes, présence des câbles de l'ancien réseau à même le sol sur plus de huit mètres. Une grande partie du câblage du bâtiment passe dans le plafond.

- arrivée unique du courant: oui, avec double disjoncteurs (un disjoncteur principal à l'arrivée du courant dans le bâtiment et un autre qui est relié à la sortie du courant onduleur qui alimente tous les appareils connectés au réseau.

- onduleurs et batterie de relai: un onduleur principal pour tous les appareils connectés au réseau et un onduleur secondaire relié à un seul serveur.
- climatisation redondant: oui, deux climatiseurs dans la salle des machines réglés à 17° C.
- réfrigération: température constante dans la salle des machines mais peut aussi varier à cause de l'état de délabrement du faux plafond.
- présence de poussière: non, présence d'un souffleur dans le bureau de la division maintenance et réseau.
- rangement des locaux: présence des cartons et des caisses remplis du matériel informatique abimés, de papiers dans le couloir et certain bureau, présence d'une poubelle dans la salle où se trouve l'onduleur central du réseau.
- protection des supports de sauvegarde : aucun dispositif.
- lieu de stockage des sauvegardes : aucun dispositif.
- dispositif d'assurer la permanence de l'électricité : présence d'un groupe électrogène qui a cesser de fonctionner depuis des mois.

Après les constats de l'inspection ou de la visite du centre informatique, nous-nous sommes amenés de vérifier la ponctualité à son poste de travail de l'agent qui contrôle et assure la liaison entre les visiteurs du centre informatique et les agents de ce centre.

Pendant 10 jours, vérifier entre 10h et 11h que l'agent qui assure le contrôle d'accès et la liaison entre les visiteurs du centre informatique et les agents de ce centre est à son lieu de service.

Figure n°

Nombre de présence au poste : 3

Nombre d'absence au poste : 7

Figure n°12: Assiduité de l'agent de contrôle d'accès

Source : Nous même

Les FAR, FRAP sont montées à partir des réponses négative du questionnaire du contrôle interne et des disfonctionnements constatés pendant l'inspection des locaux.

6.2. Synthèse de l'audit de la sécurité des données informatiques

Ici, nous allons présenter les forces et les faiblesses constatées pendant l'audit, en cela nous retenons les points les plus marquants. Nous présentons ces points dans la logique de la section 2 du chapitre v.

6.2.1. Les points forts de la sécurité informatique

- **Gestion des identités/Gestion des comptes utilisateurs/Applications :** l'accès aux applications professionnelles est protégé par un processus d'authentification avec code utilisateur et mot de passe. L'architecture de la base de données présente une bonne fixation des index.
- **Prévention, détection, neutralisation des logiciels malveillants et Sécurité du réseau/Echange de données sensibles :** la SNE dispose des anti-virus McAfee et KARSPERSKY avec licence et mise à jour sur internet. Le système informatique de la SNE est compartimenté.
- **Sauvegarde et archivage des données :** les données du serveur renfermant le logiciel GDC sont sauvegardées tous les jours dans un disque dur externe. Les données de la comptabilité et de la paie sont archivées à la direction financière et comptable
- **Mesures de sécurité physiques/Accès physique et agencement des locaux :** double portes métalliques à l'entrée principale du centre informatique de même la porte de secours. La salle des machines est bien aménagée et rangée.
- **Protection contre les risques liés à l'environnement :** la salle des machines dispose de deux climatiseurs et chaque bureau du centre informatique dispose d'un climatiseur, un agent est chargé à assurer l'entretien des bureaux du centre informatique, le bureau de la division maintenance et réseau dispose d'un souffleur pour éliminer la poussière sur les équipements.

- **Gestion des installations matérielles :** présence d'un onduleur central qui régule le courant de tout le système informatique, les câbles hors bâtiments sont enterrés, le centre informatique a de trois extincteurs. Le centre informatique n'est pas facilement identifiable de l'extérieur, les câbles du centre informatique et du bâtiment administratif sont dans des goulottes.

6.2.2. Les points faibles et les risques informatiques associés

Nous présentons ici, les faiblesses recensés ou comptabilisés pendant nos travaux d'audit ainsi que les risques qui y sont associés. A ces risques, une cotation est associée suite du fait que nous l'avons adapté par rapport au tableau n°9, cette cotation est présentée entre parenthèses.

➢ **Gestion et évaluation des risques :**

Les risques sont : non détection des conséquences d'un risque informatique sur l'entreprise (3), perte d'actifs informatique (3), réaction aux risques non efficace (3), assurance excessive dans les vérifications existantes insuffisantes (3).

Ces risques existent des faits qui sont :

- aucun dispositif ou mécanisme n'est mis en place pour la gestion ou l'évaluation des risques informatiques à la SNE,
- le risque informatique n'est pas compris dans son ensemble,
- la non réalisation d'audit informatique dans son ensemble.

➢ **Gestion de la sécurité informatique.**

Nous avons recensé comme risques : dissimilitude entre dispositions de sécurité prévues et appliquées (3), données et actifs informatiques non protégés (3), dispositions de sécurité mises en échec par les parties prenantes et les utilisateurs(2).

Les causes de ces risques sont :

- aucun poste n'existe à la SNE qui est en charge de la gestion de la sécurité informatique,
- l'inexistence de procédures précises et détaillées de sécurité informatique,

- absence générale des procédures de secours et de reprise en cas de sinistre,
- absence de police d'assurance couvrant la sécurité informatique,
- absence de la charte informatique et de la politique de sécurité informatique,
- les utilisateurs ne connaissent pas le risque informatique.

➢ **Gestion des identités/Gestion des comptes d'utilisateurs/Applications.**

Les risques identifiés sont : perte de confidentialité (3), dénie de service (3), modification ou suppression non autorisée des données (3), reconfiguration non autorisée des systèmes (2), compromission de la sécurité logique (3), fraude (3), cassure des index de la base de données (3), impossibilité d'accéder à la base de données et application (3).

Ces risques ont pour source :

- absence de procédures d'évaluation régulière et réauthentification des droits d'accès aux applications et aux systèmes,
- les mots de passe ne sont pas personnels et ne sont pas renouvelés régulièrement,
- les PC connectés au serveur de la comptabilité générale n'exigent pas une authentification (mot de passe et code utilisateur) au lancement de l'application Sage,
- incompatibilité entre l'architecture des applications développées à partir du logiciel windev qui ne sont pas de type clients/serveur alors que le réseau est de type clients/serveur.
- les PC des utilisateurs ne sont pas protéger par un mot de passe au démarrage ou en sortie d'éveil.

➢ **Prévention, détection, neutralisation des logiciels malveillants.**

Comme risques, nous avons : attaques des cybers pirates (3), divulgation des informations (3), systèmes et données exposés aux virus (3), contre mesures inefficaces (3), faille de sécurité(3).

Les origines de ces risques sont :

- l'antivirus McAfee ou KARSPRSKY n'est pas installé sur tous les PC,

- la difficulté d'acquisition d'antivirus avec possibilité d'installation sur l'ensemble des PC
- aucun antivirus n'est installé dans les serveurs de l'internet, de la comptabilité générale et celui de la comptabilité de Brazzaville,
- la mauvaise configuration système du serveur et PC associés de la comptabilité générale refuse tout installation d'antivirus,
- aucune base antivirale de l'antivirus installé n'est à jour,
- pas de connexion internet, la SNE ne paie pas régulièrement ses factures d'abonnement internet à son fournisseur du fait que le débit fourni ne facilite pas l'accès à l'internet ce qui ne facilite pas la mise à jour de la base antivirale,
- les clés USB et câble de téléphone régulièrement connectés aux unités centrales des PC par les utilisateurs favorisent des attaques virales,
- les utilisateurs méconnaissent le risque informatique.

➢ **Sécurité du réseau/Echange des données**

Les risques sont : attaques des cybers pirates (3), divulgation d'information (3), systèmes et données exposés aux virus (3), faille de sécurité (3), contre mesures inefficaces (2), indisponibilité du réseau (2).

On a constaté qu'aucune méthode de chiffrement n'est utilisée.

➢ **Sauvegarde et archivage des données**

Les risques recensés sont : perte d'image (3), risque financier(3), arrêt de l'activité (3), reprise de l'activité compromise (3).

Les causes sont :

- aucun écrit précis des procédures de sauvegarde des supports de sauvegarde n'existe,
- les supports de sauvegarde ne sont pas protégés contre une éventuelle destruction volontaire ou accidentelle,
- aucune sauvegarde externe n'est faite à la SNE,

- la sauvegarde est faite en un seul disque amovible,
- l'archivage n'est qu'à la comptabilité et à la solde.

➢ **Agencement des locaux**

Le risque est la vulnérabilité accrue vis-à-vis des risques de sécurité résultant de l'emplacement ou de l'agencement des locaux (2).

Nous avons constaté :

- la salle qui abrite le serveur du département Brazzaville est remplie de cartons de document et des papiers à même le sol,
- le plafond du bâtiment du centre informatique est en état de délabrement ce qui peut favoriser la variation de la température jusque dans la salle de machines et laisse à vue les câbles du réseau
- la présence d'une poubelle dans la salle abritant l'onduleur central, des cartons contenant les accessoires informatiques et feuilles dans les bureaux de la division maintenance et réseau peut faciliter l'installation des rongeurs,
- la mauvaise conception du bâtiment (carreaux au sol) a fait que la quasi-totalité des câbles du réseau passe dans le plafond et la présence des rongeurs accroit le danger,
- la présence d'un poteau où passent des fils électriques nus conduisant un courant de moyenne tension à moins de 12 mètres du bâtiment du centre informatique,
- les cloisons en contre plaqué augmentent la vulnérabilité de destruction en cas d'incendie.

➢ **Mesures de sécurité physique/Accès physique**

Les risques décelés sont : sabotage des supports de sauvegarde (3), accès non autorisé aux sites sensibles (3), vol de matériel informatique (3), système reconfiguré sans autorisation (3), perte financière (2)

Les causes sont :

- absence des mesures définies ou écrites sont appliquées pour assurer la sécurité physique et les contrôles d'accès,
- absence de système d'alarme ou de détection d'intrusion,

- les personnes visitant le centre informatique ne sont pas facilement identifiables,
- l'agent assurant le contrôle d'accès au centre informatique n'est pas souvent à son poste.

➢ **Protection contre les risques liés à l'environnement**

Les risques sont : poussière (1), chaleur (1), humidité (1).
Les causes sont le délabrement du faux plafond dans l'ensemble du centre informatique peut entrainer une augmentation de la température, certain bureau du centre informatique présente des lieux où le balai ne passe pas à cause de l'encombrement des bureaux.

➢ **Gestion des installations matérielles**

Les risques identifiés sont : destruction des bâtiments (3), destruction du système (3), panne machine (3), incendie/feu (3), risques électriques (3), risque magnétique (2), coupure d'électricité (3), fraude (3).
Les causes en sont :

- beaucoup d'ordinateurs ont leur unité centrale à même le sol,
- aucun PC n'est connecté à un onduleur secondaire,
- quatre serveurs ne sont pas connectés à un onduleur secondaire,
- les batteries de l'onduleur central ont plus de 5ans sans être changées,
- la caducité du matériel informatique et des applications,
- absence de contrat de maintenance des équipements informatiques,
- les extincteurs du centre informatique sont disposés dans des bureaux du centre informatique à même le sol, derrière les équipements et ne sont pas entretenus.
- le dispositif de détection/extinction est en panne,
- aucun dispositif téléphonique reliant la SNE et la caserne des sapeurs pompiers,
- le groupe électrogène devrait prendre le relai pour la fourniture de l'électricité est en panne depuis plus de 2ans.

Quand tenue de l'absence des audits informatiques surtout dans l'aspect sécurité, de l'inexistence d'un responsable de sécurité informatique, d'une entité d'identification d'évaluation et de gestion des risques informatiques ; tous les risques relevés ou identifiés ont une échelle de cotation forte donc une évaluation de l'impact élevée.

Nous allons maintenant lister les risques informatiques cités ci-haut qui se sont déjà ou se sont réalisés pendant notre stage. La liste est la suivante : panne machine, perte de confidentialité des données (information), dénie de service, coupure d'électricité, perte d'image, risque financier, risque magnétique, systèmes et données exposés aux virus, faille de sécurité, réaction aux risques informatique non efficace, dispositions de sécurité mises en échec par les parties prenantes et les utilisateurs, fraude, cassure des index de la base de données et impossibilité d'accéder à la base de données et applications.

Après que nous avons présenté les points forts et les points faibles, nous allons récapituler dans le tableau qui suit les risques qui découlent des points faibles constatés en fonction des objectifs poursuivis afin de ressortir le niveau du risque et les bonnes pratiques admises.

Tableau n°9 : Tableau des risques

Taches	Objectifs	Risques	Evaluation	Pratiques d'organisation communément admises
Gestion et évaluation des risques	-Protéger l'atteinte des objectifs informatiques ; -Protéger le matériel de stockage et en être capable ; -Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et ressources informatiques	-Non détection des conséquences d'un risque informatique sur l'entreprise ; -Perte d'actifs informatique ; -Réaction aux risques non efficace ; -Assurance excessive dans les vérifications existantes insuffisantes	-Elevé -Elevé -Elevé -Elevé	-Plan d'action de gestion de risques, -Cartographie des risques, -Fonction de gestion de risques, -Mise en place d'une action de sensibilisation à la valeur des actifs informatiques, -Approche élargie de la gestion des risques informatiques
Gestion de la sécurité informatique	-S'assurer que les règles et les procédures de sécurité sont clairement définies et connues de tous ; -Maintenir l'intégrité des données ou informations et de l'infrastructure de traitement et de stockage	-Dissimilitude entre dispositions de sécurité prévues et appliquées ; - Dispositions de sécurité mises en échec par les parties prenantes et les utilisateurs ; -Données et actifs informatiques non protégés	-Elevé -Moyen -Elevé	-Protection des actifs de stockage et autres actifs informatiques critiques ; -Plan de sécurité informatique -Charte de sécurité informatique
Gestion d'identité/gestion des comptes d'utilisateurs/ Applications	S'assurer que les données confidentielles ne sont pas accessibles à ceux qui ne doivent pas y accéder	-Perte de confidentialité(3), -Dénie de service (3), -Modification ou suppression non autorisée des données(3), -Reconfiguration non autorisée des systèmes(2), -Compromission de la sécurité logique (3), -Fraude (3), -Cassure des index de la base de données (3), -Impossibilité d'accéder à la base de données et application (3).	Elevé(3) Moyen(2)	-Mot de passe, outil de gestion d'accès ; -Verrouillage de configuration ; Limitation de l'accès au panneau de configuration, -Existence de procédures d'attribution, de suppression et de mise à jour de mot de passe, -Même architecture de configuration entre le réseau et applications

Prévention, détection, neutralisation des logiciels malveillants	S'assurer de la protection des accès logiques au système et données	-Attaques des cybers pirates, -Divulgation des informations, -Systèmes et données exposés aux virus, -Contre mesures inefficaces, -Faille de sécurité.	-Elevé -Elevé -Elevé -Elevé -Elevé	-Pare-feux -Logiciel anti-virus -Compartimentage du système informatique -Application des correctifs et patchs de sécurité -Sonde réseau
Sécurité du réseau/ Echange des données sensibles	S'assurer que les transactions automatisées et les échanges des données sont fiables	-Attaques des cybers pirates, -Divulgation d'information, -Systèmes et données exposés aux virus, -Faille de sécurité, -Contre mesures inefficaces, -Indisponibilité du réseau.	-Elevé -Elevé -Elevé -Elevé -Moyen -Moyen	-Pare-feux -Logiciel anti-virus -Compartimentage du système informatique -Application des correctifs et patchs de sécurité -Sonde réseau Cryptographie
Sauvegarde et archivage des données	S'assurer que les services et les infrastructures informatiques peuvent résister à une panne due à une erreur, à une attaque délibérée ou à un sinistre et se rétablir	-Perte d'image, -Risque financier, -Arrêt de l'activité, -Reprise de l'activité compromise.	-Elevé -Elevé -Elevé -Elevé	-Procédure de sauvegarde des données définies, -Procédure d'archivage des données définie, -Armoires sécurisés de protection des supports de sauvegarde, -Plan de secours et de reprise, -Conservation des données aux délais légaux d'archivage

Agencement des locaux	S'assurer que les services et les infrastructures informatiques peuvent résister à une panne due à une erreur, à une attaque délibérée ou à un sinistre et se rétablir	-Vulnérabilité accrue vis-à-vis des risques de sécurité résultant de l'emplacement ou de l'agencement des locaux	-Moyen	-Bâtiment solide et salles rangées, -Murs intérieurs pleins, -Dispositif de détection d'ouverture relié à une alarme, -Service de nettoyage, -Dispositif de détection de fumée/extinction, -Fenêtres à double vitrage, -Portes extérieure blindées -Barreaux sur les fenêtres extérieures
Mesures de sécurité physique/Accès physique	S'assurer que les données critiques et confidentielles ne sont pas accessibles à ceux qui ne doivent pas y accéder	-Sabotage des supports de sauvegarde, -Accès non autorisé aux sites sensibles, -Vol de matériel informatique, -Système reconfiguré sans autorisation, -Perte financière	-Elevé -Elevé -Elevé -Elevé -Moyen	-Inventaire physique, -Service de gardiennage, -Système de détection d'intrusion, -Protection des câbles du réseau, -Contrôle d'accès aux bâtiments, -Gardiens armés et sensibilisés
Protection contre les risques liés à l'environnement	S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'ait qu'un impact minimum sur l'activité	-Poussière, -Chaleur, -Humidité	-Faible -Faible -Faible	-Service de nettoyage, -Vitrage hermétique, -Climatisation/réfrigération redondante
Gestion des installations matérielles	Protéger les actifs informatiques et en être capable	-Destruction des bâtiments(3) -Destruction du système(3), -Panne machine(3), -Fraude (3) -Incendie/feu, -Risques électriques (3), -Risque magnétique (2), -Coupure d'électricité (3),	-Elevé(3) Moyen(2)	-Contrat d'assurance du matériel -Plan de reprise -Groupe électrogène -Onduleurs avec batteries-relais -Capteurs de fumée -Extincteurs à poudre -Extincteurs automatique d'incendie

6.3. Recommandations

Les recommandations qui vont suivre, vont à l'attention de Monsieur le Directeur Général, à monsieur le chef de département informatique et à monsieur le chef du centre informatique.

➢ **Recommandations à Monsieur le Directeur Général**

La SNE bénéficierait à :

- commander des missions régulières d'audit informatique,
- commander un audit organisationnel et fonctionnel du département informatique,
- lancer un avis de vacance de poste pour le recrutement d'un agent responsable de la sécurité informatique,
- créer un comité en appuis du département sécurité qui jouera le rôle de Risk Manager,
- faire élaborer une cartographie de risque pour évaluer tous les risques,
- élaborer un plan de réhabilitation du centre informatique et instruire les services généraux à réparer le faux plafond et toutes les portes en mauvais états de ce centre,
- acquérir un groupe électrogène pour relai en cas de coupure d'électricité,
- élaborer un plan d'acquisition de nouveaux matériels informatiques à la pointe de la veille technologique,
- instruire l'achet d'une police d'assurance du risque informatique,
- élaborer une politique de sécurité conforme aux normes ISO 27000, ISO 27001, ISO 27002,
- instruire un inventaire physique du parc informatique,
- élaborer un plan de formation des auditeurs en audit informatique,

- élaborer un manuel de procédure qui prendra en compte l'aspect sécurité informatique tout en précisant les tâches et les responsabilités des parties prenantes du processus sécurité,

- négocier un nouveau contrat de fourniture d'internet auprès d'un autre fournisseur avec des avenants précis,

- faire suivre les instructions ci-dessous.

➢ **Recommandations à monsieur le Chef de Département Informatique**

Pour une maitrise de la sécurité informatique, il serait judicieux de :

- Proposer un plan de secours informatique et de sauvegarde à Monsieur le Directeur Général pour parer à un scénario de destruction des données informatiques en particulier et du système informatique en général,

- proposer à Monsieur le Directeur général l'acquisition de nouveaux matériels informatique en respectant la qualité afin que la SNE reste à la pointe de la veille technologique,

- procéder un plan d'acquisition d'un antivirus avec licence et capacité d'installation sur un grand nombre de poste (maximum de poste),

- faire migrer ou évoluer l'architecture des applications développées à partir de windev vers un profil de type clients/serveur,

- redéfinir les règles de création de mot passe des utilisateurs pour tenir compte de la longueur, du nombre de caractères, du délai d'utilisation,

- élaborer une charte informatique et la communiquer à tous les utilisateurs de PC,

- organiser des ateliers pour sensibiliser les utilisateurs aux risques informatiques,

- choisir un référentiel de gestion de risques et un référentiel de management de l'informatique et le soumettre à Monsieur le Directeur Général canevas pour l'élaboration d'un manuel de procédure qui formalisera les tâches et les objectifs de sécurité informatique

➢ **Recommandation à monsieur le Chef du Centre Informatique**

Pour une bonne sécurité, il serait mieux de :

- Procéder à l'installation de l'antivirus sur tous les PC et serveurs,
- procéder à la mise à jour des bases antivirales sur tous les PC et serveurs,
- acquérir des armoires ignifuges pour conserver les supports de sauvegarde,
- acquérir et remplacer des nouvelles batteries de l'onduleur central,
- installer deux arrivées du courant électrique dans le bâtiment du centre informatique,
- réparer et réinstaller le dispositif de détection/extinction,
- installer les extincteurs dans les bureaux ou au couloir sur des supports muraux et à porté de vue,
- instruire le nettoyage et l'arrangement des bureaux du centre informatique,
- redéfinir les attributions et veiller à assiduité de l'agent de sécurité ou de liaison de l'entrée principale du centre informatique,
- installer un dispositif de détection de fumée ou d'alarme dans le bâtiment du centre informatique.

6.4. Plan d'action et mise en œuvre des recommandations

Certaines conditions devront être prises en compte avant la mise en œuvre de ces recommandations, notamment la programmation budgétaire, des délais, de la disponibilité des différents acteurs. Nous proposons dans le tableau qui suit le plan d'action de la mise en œuvre des différentes recommandations aux responsables cités ci-haut, mais cela n'a pas un caractère impératif ou impérieux.

Tableau n°10 : Plan d'action de la mise œuvre des recommandations

Responsable	Actions	Délai de mise en œuvre
Directeur Général	Suivi des recommandations	Immédiat
	Avis de vacance de poste	05jours
	Comité de sécurité, politique de sécurité, plan de secours	3semaines
	Audit organisationnel et fonctionnel du département d'audit	Février 2012
	Réhabilitation des locaux, manuel de procédure, cartographie des risques, achat groupe électrogène, contrat d'internet, formation auditeurs, inventaire physique	Budget 2012
Chef de Département informatique	Plan de secours et de sauvegarde, charte informatique, acquisition d'antivirus	2 semaines
	Faire évoluer les applications, redéfinir les règles de création de mot de passe	Immédiat
	Choix du référentiel, ébauche de scénario de reprise de l'activité	2 semaines
	Atelier de sensibilisation	45 jours
Chef de Centre Informatique	Installation d'antivirus, mise à jour base antivirale, achat, nettoyage locaux, redéfinir les attributions de l'agent gardien	Immédiat
	Achat batteries, réparation et installation du dispositif détection/extinction, alarme, installer les extincteurs sur les murs, installer deux arrivées du courant électrique	2 semaines

Source : Nous-mêmes

Conclusion

Ce chapitre nous a permis de faire un état des lieux sur les dispositifs de sécurité informatique de la SNE, de dégager les points forts et les points faibles de la sécurité ; par la nous avons formulé des recommandations aux acteurs clés capables d'apporter des améliorations, pour terminer, nous avons proposé un plan d'action de la mise en œuvre des recommandations.

Conclusion de la deuxième partie

Nous venons de présenter dans cette partie l'historique, le statut, les activités, les données informatiques et le système informatique de la SNE dans le chapitre IV. Dans le chapitre V, nous avons mis à jour les dispositifs de sécurité informatique et les acteurs intervenant dans ce processus. Au dernier chapitre, nous avons mis notre démarche méthodologique qui nous a permis de collecter des éléments pour mettre à jour les forces et les faiblesses tout en énumérant les risques qui y sont liés ; nous avons proposé un plan action pour la mise en œuvre des recommandations.

CONCLUSION GENERALE

La destruction ou l'altération des données informatiques peut entrainer des pertes financières ou même l'arrêt de l'activité pour les établissements comme la SNE dans les cas où elles seraient exposées à œuvres malveillant de l'homme et d'autres menaces. C'est pourquoi nous avons porté notre choix sur le thème « audit de la sécurité des données informatiques », qui permet de contribuer à améliorer la sécurité des données, à garantir la continuité de l'exploitation, une bonne sauvegarde des supports de sauvegarde.

Ce travail est constitué de deux parties, à savoir :

- la première partie dite théorique définie les données et le système informatique, explique comment évaluer un risque, étale les dispositifs de sécurité informatique, les outils d'audit informatique, les étapes d'un audit informatique et le référentiel retenu pour mener à bien notre méthodologie.
- la seconde partie est pratique, porte sur la prise de connaissance, de la présentation de la SNE et l'expérimentation de l'audit de la sécurité des données informatiques.

D'une manière générale la question fondamentale à la quelle nous apportons un élément de réponse est celle de savoir si les données informatiques ont un niveau de sécurité optimal les mettant à l'abri des attaques, menaces et autres vulnérabilité pouvant affecter la pérennité de l'entreprise?

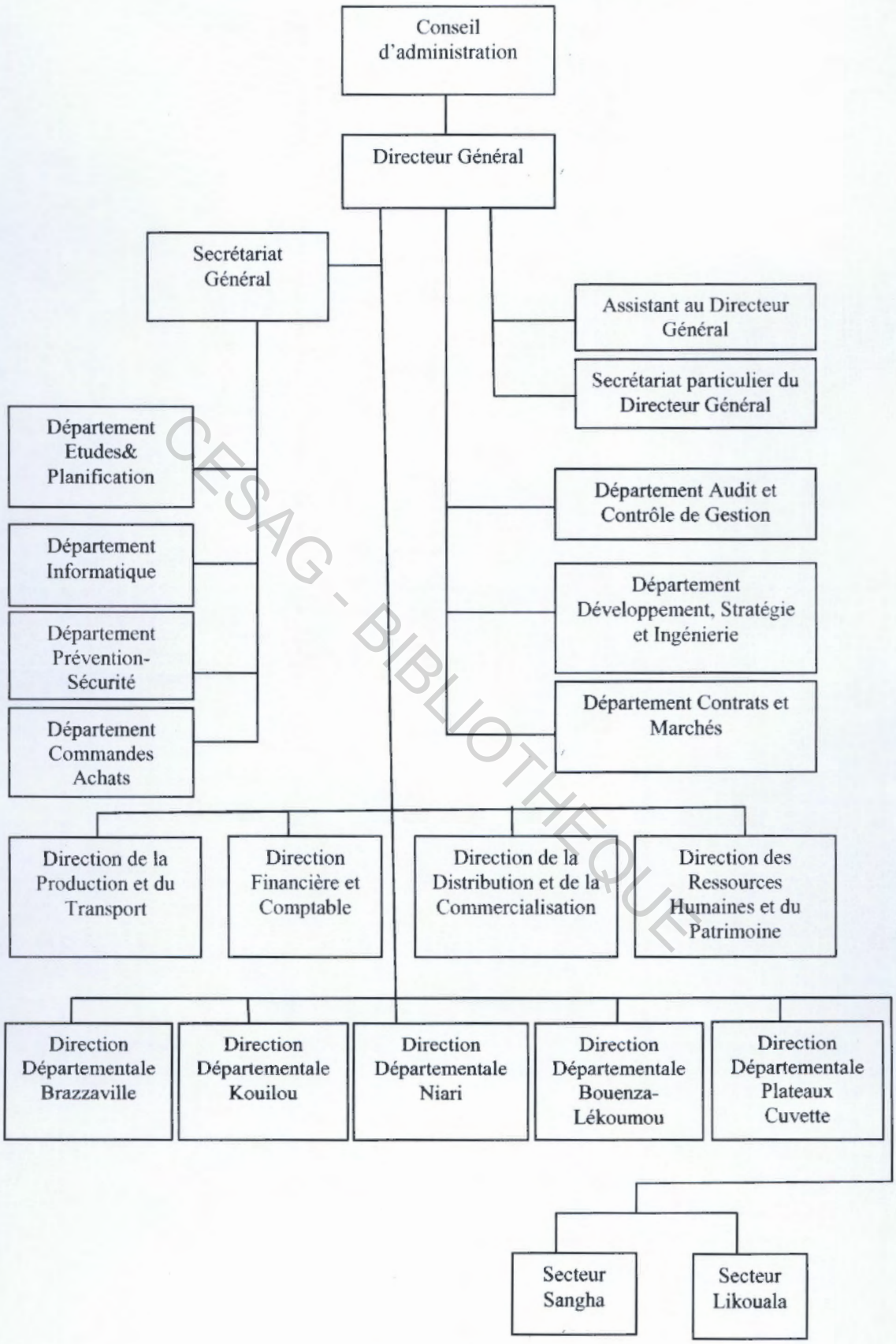
Le recours croissant au stockage des données sur disque dur, bande magnétique, CD, la généralisation progressive de l'usage des terminaux de saisie ou de consultation, l'extension des réseaux de transport de données ouverts sur l'extérieur sont autant d'accès nouveaux à l'information qui à l'origine de nouveaux risques pour l'entreprise. C'est ainsi une prise en compte insuffisante de la sécurité peut générer avec une ampleur des risques tels que les malveillances de toute nature, vol, divulgation des données confidentielles, destruction des données enfin l'organisation insuffisante de moyen de sauvegarde et de secours ne mettent pas la SNE à l'abri de risque. Aucune disposition ne peut garantir en toute certitude l'absence de risques informatiques. De ce fait, l'objet de la sécurité est de contenir ces risques acceptables au moyen d'un ensemble de protection technique et opérationnelle.

Les règles de sécurité s'appliquent à tous acteurs de l'entreprise et à tout niveau; ainsi donc, à travers l'audit de la sécurité des données informatique de la SNE, nous avons pu faire

l'état des lieux, l'analyse des risques, proposer des recommandations et un plan d'action de la mise en œuvre des recommandations, ceci pour répondre à la question si haut, aussi, permettra à la SNE de corriger certaines défaillances constatées sur le plan organisationnel, fonctionnel et pratique.

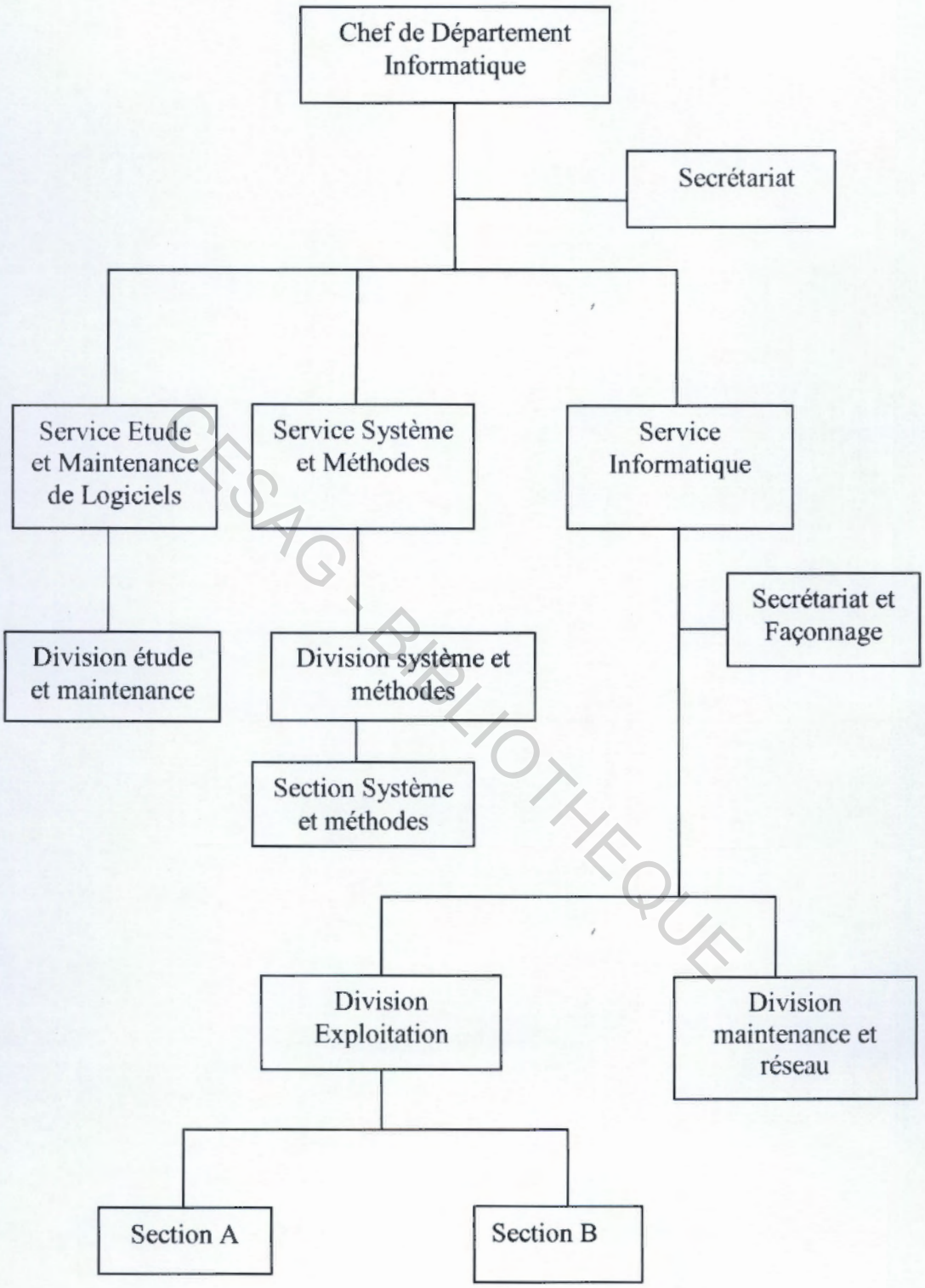
ANNEXES

Annexe n° 1 : Organigramme général de la SNE



Source : SNE

Annexe n° 2 : Organigramme du Département informatique



Source : SNE

Annexe n°3: Questionnaire de prise de connaissance

QUESTIONNAIRE DE PRISE DE CONNAISSANCE	
Objectif : Avoir une idée sur l'ensemble de l'entité, des données, système et sécurité informatique	**Observations**
Se présenter l'entité	
Mission, activités, statuts, organisation	OK
Historique	OK
Organigramme général	OK
Acquérir connaissance des données, du système informatique et de la sécurité informatique	
Organisation générale	OK
Visite des locaux et matériels	Centre informatique, et bâtiment administratif
Examiner le manuel de procédure	Pas de manuel de procédure
Document à obtenir	
Manuel de procédure	Pas de manuel
Statuts et règlement intérieur	OK
Rapport d'activité	OK, rapport des trois premiers trimestres de 2011
Charte informatique	Pas de charte informatique
Organigramme détaillé	Partiel, à compléter

Source : Nous même

Annexe n°4 : Proposition de l'ordre de mission

Ordonnateur : Directeur général	Date : 15 septembre 2011
Service : Direction Générale	Réf :

Objet : **Audit de la sécurité des données informatiques**

Dans le but de matérialiser la fin de sa formation pour l'obtention du Diplôme d'Etudes Supérieures Spécialisées en Audit et contrôle de Gestion au Centre Africain d'Etudes Supérieures en Gestion(CESAG) du Sénégal, Monsieur MOUAMANA SOUAMI Hugues se propose de réaliser un audit de la sécurité des données informatiques du point de vue de l'auditeur interne.

L'objectif principal de cet audit est de s'assurer du niveau de sécurité des données informatiques dans l'optique de réduire l'exposition aux vulnérabilités et sinistre et de minimiser les risques.
La mission débutera dès approbation du thème de la mission et s'achèvera le 31 octobre 2011.

Cette étude a pour but d'analyser la sécurité des données informatiques de la SNE, identifier les forces et les faiblesses afin d'émettre les recommandations en vue de son amélioration.
Les objectifs spécifiques de la mission sont :

- S'assurer de la gestion et de l'évaluation des risques informatiques
- s'assurer de la mise en place d'un système de droit d'accès aux données informatiques
- S'assurer de la mise en place des dispositifs de sécurité logique des données
- S''assurer d'une bonne sauvegarde des données issues des traitements informatiques
- S'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques.

Cette se déroulera auprès des utilisateurs de l'outil informatique et du département informatique/centre informatique à la SNE.

Vous voudrez bien en informer les personnes concernées et prêter votre concours actif au bon déroulement de cette mission/étude.

Le Directeur Général de la SNE

Destinataires : Département informatique, département prévention et sécurité, utilisateurs de l'outil informatique des directions et départements.

Source : Nous même à partir de SCHLIK(2007)

Annexe n°5 : Questionnaire du contrôle interne

QUESTIONNAIRE DE CONTROLE INTERNE	DONNEES INFORMATIQUES	Folio 1/9

AUDIT DE LA SECURITE DES DONNEES INFORMATIQUES

OBJECTIFS DE CONTROLE :

I-S'assurer de la gestion et de l'évaluation des risques informatiques
II- s'assurer de la mise en place d'un système de droit d'accès aux données informatiques
III- S'assurer de la mise en place des dispositifs de sécurité logique des données
IV- S''assurer d'une bonne sauvegarde des données issues des traitements informatiques
V- S'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques

Source : Nous même, selon les approches de CLEUET& al, COBIT

QUESTIONNAIRE DE CONTROLE INTERNE	Département informatique	Folio 2/9

OBJECTIF DE CONTROLE :
I-S'assurer de la gestion et de l'évaluation des risques informatiques

I-a Gestion de la sécurité informatique

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Un référentiel de gestion des risques existe-t-il dans l'entreprise ?		✓			
2. Existe-t-il un référentiel de gestion des risques informatiques ?		✓			
3. Le contexte de risque informatique est-il compris : a) compris ? b) communiqué ?	✓	 ✓			
4. Les principales menaces sont-ils identifiées ?	✓			La foudre et l'électricité	
5. Existe-t-il un processus d'identification et de mesure des risques informatiques qui tient compte : a) de la probabilité ? b) des conséquences ?		 ✓ ✓			
6. Existe-t-il un processus de réponse aux risques informatiques ?	✓				
7. Un plan de gestion des risques est-il mis en place ?		✓			

QUESTIONNAIRE DE CONTROLE INTERNE	Département informatique	Folio 3/9

OBJECTIF DE CONTROLE :
I- S'assurer de la gestion et de l'évaluation des risques informatiques

I-a : Gestion de la sécurité informatique

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Existe-t-il dans le département informatique un responsable de la sécurité informatique?		✓			
2. Existe-t-il dans l'entreprise un comité de pilotage de la sécurité informatique ?		✓			
3. Est-ce que l'entreprise dispose d'une charte informatique ?		✓			
4. La politique de sécurité couvre-t-elle : a) la responsabilité du conseil d'administration ? b) la direction générale ? c) les cadres intermédiaires ?	✓	✓ ✓			
5. Existe-t-il des procédures et standards de sécurité détaillés ? a) Politique de sécurité des ordinateurs de bureau, serveurs ? b) Politique d'utilisation d'internet ? c) Politique de sécurité du courrier électronique ? d) Contrat de conformité aux règles de sécurité informatique ?		✓ ✓ ✓ ✓ ✓		Aucun écrit n'existe mais les agents travaillent avec des procédures dictées par leur hiérarchie	
6. Existe-t-elle dans l'entreprise une structure organisationnelle et hiérarchique de la sécurité informatique ?		✓			

QUESTIONNAIRE DE CONTROLE INTERNE	Département informatique	Folio 4/9

OBJECTIF DE CONTROLE :
II- s'assurer de la mise en place d'un système de droit d'accès aux données informatique

II-a : Gestion des identités/gestion des comptes utilisateurs

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Les actions des utilisateurs (internes, externes, stagiaires) sont-elles identifiables sans confusion?	✓				
2. Les systèmes sont-ils configurés pour imposer l'authentification avant d'autoriser l'accès ?	✓			L'authentification est exigée au lancement des logiciels d'exploitation	
3. Lors de l'attribution d'une identité, les droits sont-ils validés par le management responsable du processus?	✓				
4. Des mécanismes de fourniture d'accès et de contrôle d'authentification sont-ils utilisés pour contrôler : a) l'accès logique sur tous les utilisateurs? b) les processus système et les ressources informatiques?	✓ ✓				
5. Est-ce qu'il existe une procédure pour évaluer régulièrement et ré authentifier les droits et accès aux systèmes et applications?	✓				
6. Les politiques, standards et procédures de gestion des comptes utilisateurs s'étendent-ils à tous les processus et utilisateurs des systèmes?	✓				

QUESTIONNAIRE DE CONTROLE INTERNE	**Département informatique**	**Folio 5/9**

OBJECTIF DE CONTROLE :
III- S'assurer de la mise en place des dispositifs de sécurité logique des données
III-a: Prévention, détection, neutralisation des logiciels malveillant/Sécurité des réseaux/Echange des données sensibles

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Une politique de prévention contre les logiciels malveillant a-t-elle été mise en place ? Est-elle documentée et communiquée dans l'ensemble de l'entreprise?		✓		Pas d'écrits, le supérieur hiérarchique décide sur quoi faire	
2. Un logiciel de protection est-il distribué ?	✓			Difficulté d'acquisition et distribution limité	
3. L'usage des mots de passe est-il généralisé sur tous les postes et sur l'ensemble des utilisateurs ?	✓				
4. Les fonctions de conception de la sécurité facilitent-elles les règles de mot de passe : a)longueur maximum ? b) caractères ? c) expiration ? d) réutilisation ?	 ✓ ✓ ✓				
5. Une politique de sécurité réseaux a) est-elle mise en place ? b) est-elle à jour ?		 ✓ ✓			
6. Les données sont-elles chiffrées avant leur transmission hors de l'entreprise ?		✓			
7. Le logiciel de gestion des autorisations d'accès permet-il de distinguer entre l'autorisation de consultation des donnés et l'autorisation de mise à jour des données ?	✓			L'accès aux données est personnalisé avec des droits définis	

QUESTIONNAIRE DE CONTROLE INTERNE	Département informatique	Folio 6/9

OBJECTIF DE CONTROLE :
IV- S''assurer d'une bonne sauvegarde des données issues des traitements informatiques

IV-a: Sauvegarde et archivage des données

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Est-ce qu'il existe une procédure de sauvegarde des données clairement définie?	✓				
2. Disposez-vous d'armoire appropriée pour la conservation des supports de sauvegardes ?		✓			
3. Procédez-vous de façon périodique à des tests de relecture ?	✓				
4. Les supports sont-ils conservés dans des lieux suffisamment éloignés des sites sensibles ?		✓			
5. Est-ce qu'il existe un plan de secours et de reprise en cas de sinistre important ?		✓		Malgré l'absence du plan de secours, les sauvegardes facilitera la reprise de l'activité	
6. Un périmètre de sauvegarde est-il défini ? a)concerne t-il les données ? b) les applications et logiciels ? c) la fréquence de sauvegarde ?	 ✓ ✓ ✓				
7. La sauvegarde concerne-t-elle : a) les serveurs ? b) les postes individuels ?	 ✓	 ✓			

QUESTIONNAIRE DE CONTROLE INTERNE	Département sécurité, Département informatique et Département gestion du patrimoine	Folio 7/9

OBJECTIF DE CONTROLE :
V- S'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques

V-a: Mesures de sécurité physique

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Est-ce qu'une politique a été définie et mis en place pour contraindre les sites informatiques de respecter les mesures de sécurité physique et de contrôle d'accès? Cette politique est-elle régulièrement étudiée pour s'assurer qu'elle demeure pertinente et à jour ?	✓	✓			
2. Les mesures de sécurité physique incluent-t-elles : a) des systèmes d'alarme ? c)une protection des câbles ? d) des systèmes de détection de fumée ?		✓ ✓ ✓			
3. Est-ce que des séances de formation ou d'assistance en sécurité sont régulièrement organisées aux agents du département informatiques ?	✓			La dernière séance date de l'année 2006	
4. Les supports de stockage des données sont-ils conservés dans des lieux suffisamment éloignés des sites ou lieux sensibles ?		✓			
5. Est-ce qu'il est régulièrement organisé des tests d'application des mesures de sécurité imposée à la société privé de gardiennage et aux agents de l'armée qui assurent la sécurité des cites du siège social ?	✓			Le chef de service protection du patrimoine réalise des visites nocturnes pour s'assurer de l'assiduité des agents de sécurité	

QUESTIONNAIRE DE CONTROLE INTERNE	DRP- Département informatique	Folio 8/9

OBJECTIF DE CONTROLE :
V :- S'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques

V-b: Accès physique

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Est-ce qu'un processus a été mis en place pour gérer les demandes et l'octroi d'accès au centre informatique?	✓			Les procédures sont sous forme de projet qui n'est pas réalisé et vulgarisé	
2. Est-ce qu'un processus permet de journaliser et de surveiller les accès des sites informatiques et d'enregistrer tous les visiteurs, les fournisseurs et les sous traitants?		✓		L'accès est contrôlé à la salle des machines	
3. Existe-t-il une garde à l'entrée du centre informatique avec des taches précises ?		✓			
4. Est-ce qu'un règlement impose aux visiteurs du centre informatique d'être accompagnés ?		✓			
5. Est-ce qu'un règlement impose au personnel de porter en permanence un signe d'identification visible?		✓			
6. Evite-t-on l'émission des cartes d'identification ou de badges sans autorisation appropriée?	✓				
7. Est-ce que l'accès au centre informatique est limité par le biais d'une protection périmètre (ex : clôtures/ murs et dispositifs de sécurité sur les portes intérieures ?	✓			Présence d'un mur de clôture.	

QUESTIONNAIRE DE CONTROLE INTERNE	DRP- Département informatique	Folio 9/9

OBJECTIF DE CONTROLE :
V- s'assurer de la sécurité physique des outils de stockage des données informatiques à l'épreuve des risques

V-c: Gestion des installations matérielles et protection contre les risques liés à l'environnement

QUESTIONS	OUI	NON	N/A	COMMENTAIRE	F.T
1. Est-ce qu'il existe une procédure ou mécanismes étudiant la nécessité de protéger les installations informatiques contre les conditions extérieures et les pannes de courant et incendie électriques?	✓			Installation des onduleurs et détecteur d'incendie	
2. Est ce que l'entreprise se procure des onduleurs ? -Est-ce qu'ils répondent aux exigences de disponibilité et de continuité des activités ?	✓ ✓			L'onduleur principal n'a plus que 30min d'autonomie du fait que le remplacement des batteries de relai ne se fait pas.	
3. Est-ce que dans le centre informatique plusieurs entrées d'alimentation électrique sont disponibles?		✓		Il existe une seule entrée du courant électrique	
4.Est-ce qu'il y a un groupe d'alimentation électrique qui assure la production du courant en cas de coupure d'électricité?	✓			Le groupe est en panne il y a plusieurs années	
5. Est-ce que les câbles extérieures au centre informatique sont enterrés ou disposent d'une protection adaptée?	✓				
6.Est-ce qu'il existe des schémas et des plans ? - les câbles situés dans les sites informatiques sont-ils contenus dans des conduites sécurisées? - les câbles sont-ils renforcés et	✓ ✓			Les câbles blindés qui résistent même à l'interférence	

protégés contre les risques environnementaux ? -le câblage et la connexion physique (données) sont correctement structurés et organisés ?	✓ ✓				
7.Est-ce qu'un processus a été mis en place pour s'assurer que la maintenance du matériel et du centre informatique est effectuée selon les spécifications et la périodicité recommandée par les fournisseurs ?		✓		Il y a plus une organisation interne	
8. Est-ce que la maintenance est uniquement assurée par le personnel autorisé ?	✓				
9. Est-ce qu'une politique décrit comment le matériel informatique est protégé contre les menaces environnementales ?		✓		Aucun document écrit, présence de 4extincteurs et d'un souffleur.	
10. Est-ce qu'une politique à été mis en place pour garantir un nettoyage régulier à proximité des activités informatiques ?	✓			Un agent est en charge du nettoyage du centre informatique.	

Annexe n°6 : Guide d'entretien des acteurs à la sécurité informatique

Service paie

I. Quelle application utilisez-vous pour traitement de vos données ? Comment est –elle utilisée ?

II. Comment est-elle sécurisée ?

III. Comment vos données sont-elles sauvegardées ?

IV. Connaissez-vous les risques informatiques ? Les quelles sont susceptibles de se matérialiser ?

Direction financière et Comptable

I. Quel usage fait-vous de l'outil informatique ?

II. Quelle application utilisez-vous ? Comment est-elle sécurisée ?

III. Comment vos données sont-elles sauvegardées et archivées ?

IV. Connaissez-vous les risques informatiques auxquels vous êtes exposés ?

Service de protection du patrimoine

I. Quelles sont vos missions ?

II. Comment assurez-vous la prévention contre le feu ou l'incendie des bâtiment, du personnel et du matériel de la SNE ?

III. La SNE se procure-t-elle des extincteurs ? Qui est à la charge de l'entretien de vos extincteurs ?

IV. Y a-t-il un dispositif qui vous relie à la caserne des sapeurs pompiers ? Si oui, lequel ?

V. Quel appui votre service apporte au département informatique ?

VI. Est-ce que la SNE est couverte par une assurance ?

VII. Connaissez-vous le risque informatique ?

Vigile du bloc administratif

I. En quoi consiste votre travail ?

II. Vous enregistrez toutes les entrées dans le registre ?

III. Contrôlez-vous tout le matériel qui sort du bloc administratif ?

Agent de liaison ou de garde du centre informatique

I. Quelle sont vos attributions ?

II. Avez-vous une note administrative qui vous nomme à ce poste ?

III. Pouvez-vous expliquer comment vous assurez vos taches ?

IV. Contrôlez-vous toutes les entrées et les sorties du matériel et du personnel ?

V. Quelles difficultés rencontrées en accomplissant votre fonction ?

Chef du centre informatique

I. Quelles sont vos missions ?

II. Quelles sont les dispositifs de sécurité qui existent dans le centre informatique ?

III. Etes-vous souvent assister par les agents du service protection du patrimoine en matière de sécurité ?

IV. Comment travaillez-vous avec le département informatique en matière de politique de sécurité informatique ?

V. Comment vous vous procurez l'antivirus ?

VI. Disposez-vous d'une police d'assurance couvrant le risque informatique ?

VII. Existe-t-il un plan de secours informatique ?

VIII. Pouvez-vous nous faire visiter le centre informatique ?

Division maintenance et réseau

I. Quelles sont vos missions ?

II. Existe-t-il des contrats de maintenance du matériel informatique ?

III. Qui vous fourni l'électricité ?

IV. Pouvez-vous nous décrire le réseau informatique de la SNE ?

V. Comment est sécurisé le réseau informatique ?

VI. Quelles difficultés rencontrez-vous dans l'accomplissement de vos tâches ?

Division exploitation

I. Quelles sont vos attributions?

II. Disposez-vous de combien d'applications ? Comment fonctionnent-elles et comment sont-elles protégées ?

III. Comment est protégé l'accès à la base de données ?

IV. Comment gérez-vous les habilitations ?

V. Respectez-vous les conditions de création de mots de passe (longueur, durée, nombre caractères) ?

VI. Quelles sont les difficultés que vous rencontrez dans la sécurité de la base de données ?

VII. Existent-t-ils des écrits qui détaillent les procédures de sauvegarde et d'archivage ? Si non, expliquer-nous comment vous procédez aux sauvegardes et à l'archivage des données ?

Ouvrages

1. ACISSI (2009), *Sécurité informatique : ethical harking, apprendre l'attaque pour mieux se défendre*, Editions ENI, Paris, 355 pages

2. AFAI(2008), *Cobit 4.1.*, IT Gouvernance Institute, Paris, 196 pages.

3. AFAI (2008) Guide *d'Audit des Systèmes d'informations: Utilisation de cobit*, IT Gouvernance Institute, Paris 269 pages.

4. BARTHELEMY, Bernard et COURREGES, Philippe (2004), *Gestion des risques: Méthode d'optimisation globale*, 2ème édition, Edition d'organisation, Paris, 471 pages.

5. BUTEL, Annie(2008), *Continuité d'activité : Plan de secours*, CLUSIF/BNP PARIBAS, Paris 33 pages.

6. - CALE, Stéphane et TOUITOU, Philipe(2007), La *sécurité informatique : réponses techniques, organisationnelles et juridiques*. Lavoisier, Paris, 282 pages.

7. CARPENTIER, Jean-François(2009), *La sécurité informatique dans la petite entreprise : état de l'art et bonne pratique*, Edition ENI, Paris, 277 pages

8. CLEUET, Fabien, et al. (2008 a), *Audit des systèmes information*, Vol. 1 INTEC/CNAM, Paris, 162 pages

9. CLUSIF(2010), *Menace informatique et pratique de sécurité informatique en France*, Edition 2010, Paris, 102pages.

10. CLUSIF(2010), *MEHARI 2010 : Manuel de référence de base de connaissance Méhari 2010*, CLUSIF, Paris, 16pages.

11. COSOII Report (2005), *Le management des risques de l'entreprise*, édition les organisations, 523 pages.

12. DAYAN, Armand, et al (2004), *Manuel de gestion* Vol. 1, 2e édition, ELLIPSES/AUF, Paris, 1088 pages.

13. DESROCHES, Alain, LEROY, Alain et VALLEE, Frédérique (2003), *La gestion des risques : Principes et Pratiques,* Edition Lavoisier, Paris, 286 pages.

14. Gildas Avoine, Pascal Junod et Philippe Oechslin (2004), *Sécurité informatique*, Edition Vuibert, Paris, 157 pages

15. GODART, Didier (2002), *Sécurité informatique : risques, stratégie et solutions*, Edipro, Paris, 334 Pages

16. GRAEVE, Jean de et POITIER, Jean (2001), *Système d'information, Management et Acteurs*, Les Editions SAIENTIA, Paris, 135 pages.

17. - HAMZAOUI, Mohamed(2005), *Audit : gestion des risques d'entreprise et contrôle interne : normes ISA 200, 315, 330, et 500*, Edition Village Mondial, Paris, 242 pages

18. LAUDON, C., Kenneth, LAUDON, P., Jane et GINGRAS, Lin (2000), *les systèmes d'information de gestion,* Pearson Education/Village Mondial, Paris, 784 pages

19. LY, Henri (2005), *L'Audit technique informatique*. Edit. LAVOISIER/HERMES SCIENCE, Paris, 230 pages.

20. MENTHONNEX, Jean(1995), *Sécurité et qualité informatique. Nouvelles orientations,* Presses Polytechniques et Universitaires Romandes, Lausanne, 422 pages

21. MOREAU, Franck (2002), *Comprendre et gérer les risques*, Edition d'Organisation, Paris, 222 pages.

22. REIX, Robert (2002), *Système d'information Management des organisations*, 2è édition, LIBRAIRIE VUIBERT, Paris, 443 pages

23. REIX, Robert(2005*), Système d'information et management des organisations*, 5è édition, LIBRAIRIE VUIBERT, Paris, 486 pages

24. RENARD, Jacques(2010), *Théorie et pratique de l'audit interne*, 7e édition, Edition d'Organisation, Paris, 470 pages

25. ROYER, Jean Marc (2004), *Sécuriser l'informatique de l'entreprise : enjeux, menaces, prévention et parade,* Editions ENI, Paris, 422 pages

26. - SCHICK, Pierre, (2007), Mémento d'audit interne. Méthode de conduite d'une mission d'audit, DUNOD, Paris, 217 pages.

27. SNE (2006), *Charte d'audit de la SNE*, DIRECTION GENERALE SNE, 37 pages.

28. SNE(1996), *Règlement intérieur SNE*, DIRECTION GENERALE SNE, 34 pages.

29. SNE(2011), *Rapport d'activité des trois premiers trimestres 2011*, SECRETARIAT GENERAL SNE, 18 pages.

30. STALLINGS, William (2002), *Sécurité des réseaux, Applications et standards*, Edition Vuibert, 382 pages

31. VOLLE, Michel (2004), *Lexique du système d'information*. Club des maitres d'ouvrages des systèmes d'information & Michel VOLLE, GNU Free Documentation, Paris, 23 pages.

32. -YADAV, Subhash Chandra et SINGH, Sanjay Kunar (2009), *An Introduction to Client/Server Computing*, New Age Internationnal, Varanasi, 212 pages.

33. YANN, Derrien (1992), *Les techniques de l'audit informatique,* Edit. DUNOD, 239 pages.

Articles

34. AFAI (2007), Rappel sur les normes et méthodes en matière de sécurité des systèmes d'information, *La revue Française de l'Audit et du conseil informatique*, Vol. 85 :21-23

35. DUGELAY, Eric (2003), Quels enjeux et quelles approches pour un plan de continuité global, *Revue Française de l'Audit interne*, Vol. 163 : 16-17

36. Pierre Alexandre Bapst et Florence Bergeret, Pour un management des risques orientés vers la protection de l'entreprise et la création de la valeur, *Revue Française d'audit* n° 162, Décembre 2002.

Sources internet

37. Alexei Lesnykh (2009), Périphérique-de stockage[En ligne][Citation :2 Juillet 2011] http://wwwZataz.com/news/19190/peripherique-de stockage Actualit

38. - Business Technology Consulting, *Introduction à COBIT* [Enligne] [Citation : 16Juillet 2011], http://www.btcweb.com/btc/fr/services/organisation/cobit/index.html

39. CLUSIF (2010 b), www.clusif.asso.fr. [En ligne] [Citation : 2 Aout 2012], http//www.clusif.asso.fr/fr/production/mehari/.

40. DEVICE LOCK Inc, Proactive Network Security [EN ligne][Citation: 6mai2011] http://www.athena.gs.com/Livre_blancs/devicelock

41. - FAURE, Jean-Baptiste, (2009), Dossier spécial stockage- Stockage magnétique, Dataligence.COM,[En ligne] [Citation : 29Juin 2011]

http//:www.dataligence.com/site/dossier-special-stockage-données/stockage-magnetique/les-bandes-magnetiques.htlm

42. FAURE, Jean-Baptiste, (2009), Les NAS, les SAN et les architecture réseaux, Dataligence.COM. [En ligne][Citation :5Juin 2011] http://www.dataligence.com/site/dossier-spécial-stockage-données.html.
43. Gartner group, www.techno-science[En ligne][Citation: 28 Mai 2011] http//www.techno-science.net/?onglet=glossaire&definition=162
44. GUIDE-INFORMATIQUE (2010), Sécurité des informations, normes BS7799, ISO17799, EBIOS, MEHARI. www.guideinformatique.com. [En ligne] [Citation 22 Juillet 2011], http//guideinformatique.com/fiche-securite_des_informations-441.htm.
45. Hugo Etiévant (2006) *Normes de sécurité : les méthodes d'analyse des risques* [En ligne] [Citation 17Juillet2011], http://cyberzoide.developpez.com/securite/methodes-analyse-risques/
46. KOMAR, Mancel,(2006), Les solutions de stockage NAS et SAN [En ligne] [Citation 5juillet 2011] http://wwwguideinformatique.com/fiche-nas-339.htm.
47. LESSAUVEGARDES(2007), Construire son plan de sauvegarde, [En ligne] [Citation :10 Juin 2011], http//www.lessauvegardes.com/Iscom/2007/10/15/construire-son-plan-de-sauvegarde/
48. PILLOU, Jean-François(2010), Mise en place d'une politique de sécurité. Linux Plus-Value. [En ligne] [Citation: 19 Juin 2011] ; http/www.linuxplusvalue.be/mylpv.php?id=184
49. SOCIETE DE MARKETING INDUSTRIEL (2010), Sécurité : Eviter aussi les risques physique, *ACHETEURS INFO. COM.* [En ligne] [Citation : 7 juin 2011] http/www.acheteursinfo.com/actualites_securite.html.
50. WIKIPEDIA(2011), Données [En ligne][Citation : 2Juin 2011] ;wikipedia.org