CESAG **Centre Africain d'Etudes 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 21
(2009-2010)

Mémoire de fin d'étude

THEME

L'audit de la sécurité du système informatique : cas de la Représentation ASECNA-Cameroun.

Présenté par :

NGA ATANGANA
Simon Serge Emmanuel

Dirigé par :

OKALLA MANGA NDI
Bernardin Albert

Directeur de mission
Cabinet OKALLA AHANDA & Associés

Octobre 2010

DEDICACE

Nous dédions ce mémoire à notre mère Mme ATANGANA Dorothée Hélène et à notre père M. ATANGANA NGA René pour les sacrifices consentis, la patience et les encouragements à notre endroit. Qu'ils trouvent dans ce modeste travail l'aboutissement de leurs nombreux efforts.

REMERCIEMENTS

Nous remercions :

- Mme YAKA Rose Yvette, notre maman qui nous couve et nous porte vers le succès.
- M. MBOTTO EDIMO Frédéric, Représentant ASECNA au Cameroun qui nous a permis d'effectuer ce stage au sein de l'organisme qu'il dirige.
- M. OKALLA MANGA NDI Bernardin Albert, qui aura suscité en nous la passion pour ce métier et nous a encadré pour la réalisation de ce mémoire.
- M. YAZI Moussa, Directeur de l'ISCBF qui n'a pas hésité à mettre sa santé en péril pour la réussite de la 21^{éme} promotion du DESS audit et contrôle de gestion.
- Tout le corps professoral et administratif du CESAG pour la qualité de l'encadrement et de la formation reçus.
- L'ensemble du personnel de la Représentation ASECNA du Cameroun, particulièrement M. KUNZ MISSE Richard pour leurs grandes disponibilités.
- Nos sœurs et frères MANGA ATANGANA Marlyse, MASNDI ATANGANA Nathalie Noëlle, BIKONO ATANGANA Ernestine Renée, ABEGA Marie Salomé, ATANGANA NGA René Junior, ELOMO Parfait Thierry.
- Nos beaux-frères MM. BANGA NKOMO David Douglas, BIWOLE Jean Aloys, MVENG Pierre, pour leurs encouragements.
- Nos amis ADA BIHIHA Shirley Michelle, AMPOULIA BIWOUELE Nadia, BALLA BALLA Jean Olivier, ALIFA Barka , BELLE NGONDI Jules, BITO Eric, BEBEDE EFOMBO Mireille, EVINA Michelle, EYOUM Yves Bertrand, KOUAM Renée Manuela, KWEDI MOUDIKI Guy, MBEA Olivier, MISSE NTONE Claude, MVEINDJI BELLO Eugène, MVOM Yannick Rahmane, MVONDO Esther Noëlle, NGOUMOU MANGA Bertrand, NTOH ELOUTI Monique, ONANA Yannick Richard, OSSONO NII Edith, PONDA MPONDO Dany.
- MM. AKOTOGNONG MANDJE KOSSI Serge Eric, AWONO Théophile, BWEMBA Freddy Yannick, CHIMOUN François, pour leurs inestimables contributions.
- Mlle BEBEDE BELANG Christiane Edwige pour le soutien et le réconfort.
- Nos camarades de promotion.
- La communauté camerounaise du CESAG.
- Et tous ceux, qui de près ou de loin, ont contribué à la réalisation de ce travail.

Liste des sigles et abréviations

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

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

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ASECNA : Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar

CLUSIF : Club de la Sécurité de l'Information Français

COBIT: Control Objectives for Information and related Technology

COSO: Committee Of Sponsoring Organization of the Treadway Commission

DVD: Digital Versatile Disc

ERSI : Ecole Régionale de Sécurité Incendie

FAR : Feuille de Révélation des Risques

FRAP : Feuille de Révélation et d'Analyse de Problème

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

IGC : Infrastructures de Génie Civil

IIA: The Institute of Internal Auditors

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standardization

ITIL: Information Technology Infrastructure Library

MEHARI: Méthode Harmonisée d'Analyse des Risques

OACI : Organisation de l'aviation civile internationale

PC: Personnal Computer

POCA : Pratique d'Organisation Communément Admises

RSI : responsable de la sécurité informatique

RSSI: responsable de la sécurité du système d'information

SMI : Société de Marketing Industriel

SSLI : Section Sauvetage et Lutte Contre l'Incendie

USB: Universal Serial Bus

Liste des tableaux et des figures

Liste des tableaux

Liste des figures

Liste des annexes

Table des matières

INTRODUCTION GENERALE

L'informatique est aujourd'hui au cœur de l'activité des entreprises modernes. Aucun métier n'y échappe. Il est donc vital pour toute organisation de disposer à chaque instant d'un système informatique fonctionnel qui lui assurerait la disponibilité de son système d'information et de ses ressources informatiques.

Les catastrophes naturelles, les changements climatiques, les menaces terroristes, la cybercriminalité, la malveillance des personnes internes à l'entreprise sont des menaces qui sont susceptibles de survenir et d'avoir un impact néfaste sur le système informatique et ainsi compromettre la continuité de l'exploitation ou la bonne conduite des missions assignées à l'organisation. Des mesures de sécurité doivent être prises afin de s'assurer que de tels faits ne se produisent, et si malgré les précautions prises, il advient que l'une de ces menaces survient, l'entreprise doit être capable d'assurer la disponibilité de son système informatique en un minimum de temps. Pour ce faire, l'entreprise doit mettre en œuvre une politique spécifique de sécurité de ses actifs informatiques. Cette politique spécifique s'inscrit dans une politique globale de management du système d'information.

Le plan de modernisation des équipements et installations et la mise en œuvre des premières applications opérationnelles des nouvelles technologies de navigation et de gestion du trafic CNS/ATM débutés en 2006 à l'ASECNA accroissent la probabilité que des risques liés au système informatique se matérialisent. De plus l'activité aéronautique voit peser sur elle la menace terroriste. Ces attaques peuvent survenir sur le site informatique ou viser les données et les applications de guidage ; les attaques chinoises du 15 janvier 2010 sur le moteur de recherche GOOGLE nous démontrent que de tels faits peuvent se produire à tout moment[1].

La technicité quasi ésotérique du domaine informatique et l'organisation administrative et fonctionnelle de la Représentation ASECNA du Cameroun place la sécurité informatique sous la seule responsabilité du Bureau Informatique. De plus, la vacance du poste d'Agent Informatique en charge de la sécurité (antivirus, système d'application) et de la surveillance de l'environnement informatique fait reposer le poids de cette tâche stratégique sur une seule personne : le Chef du Bureau Informatique. Le site sur lequel les installations abritant les composants du système informatique sont construites peut être la cible d'individus ou

[1] Dans le même ordre d'idée le film de Penny HARLIN « 58 minutes pour vivre » (die hard 2) avec Bruce WILLIS et William ARTERTON sortie le 02 juillet 1990 montre comment des terroristes prennent le contrôle du centre informatique d'une tour de contrôle pour faire se crasher des avions par la transmission de données erronées.

d'organisation malveillants. Cet état de fait augmente la probabilité qu'un risque majeur se matérialise et menace l'intégrité de ce système.

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

- l'absence de risk manager ;
- l'absence d'un responsable de la sécurité informatique ;
- le manque de contrôle de l'accès aux locaux informatiques ;
- l'ignorance de certains risques pouvant affecter le système informatique ;
- l'absence d'une unité d'Audit interne pour évaluer la sécurité informatique ;
- le cumul de tâches incompatibles au sein du Bureau Informatique ;
- l'effectif inadéquat au Bureau Informatique (profil et nombre) ;
- l'absence d'une charte de sécurité informatique.

Les conséquences découlant des problèmes ci-dessus mentionnés peuvent être :

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

Afin d'y faire face, nous pensons que les dispositifs suivants peuvent être envisagés :

- la sensibilisation des acteurs en matière de sécurité ;
- la mise en place d'une politique de sécurité informatique ;
- le recrutement de personnel supplémentaire et compétent au Bureau Informatique ;
- la nomination d'un risk manager ;
- la création du poste de responsable de la sécurité informatique
- l'élaboration d'une cartographie des risques du système informatique ;
- l'audit de la sécurité du système informatique.

La dernière solution paraît la plus opportune car un audit de sécurité permet de s'assurer que la politique de sécurité informatique adopte les bonnes pratiques. Il est d'usage de comparer une politique de sécurité avec un standard, un cadre de référence ou aux bonnes pratiques en

vigueur[2]. Le résultat de l'évaluation consiste en un ensemble de recommandations qui visent à adapter des processus, des procédures ou des configurations aux standards.

Au regard de ce qui précède, la question principale à laquelle ce mémoire permettrait de répondre est la suivante : « Comment la sécurité du système informatique est-elle assurée » ?

Elle conduit aux questions sous-jacentes suivantes :

- Quelles sont les risques informatiques auxquels la Représentation de l'ASECNA-Cameroun doit faire face afin de s'en prémunir ?
- Quelles sont les dispositifs de sécurité qui doivent être mis en place pour limiter l'impact des risques informatiques ?
- Comment est-ce que les dispositifs de sécurité choisis sont-ils mis en œuvre au quotidien ?

L'audit de la sécurité du système informatique permettra de répondre à ces questions à travers les trois objectifs spécifiques suivants :

- s'assurer de l'existence d'un processus d'évaluation et de gestion des risques informatiques ainsi que l'impact potentiel des risques sur les objectifs et les processus métiers[3] ;
- s'assurer de la sécurité des systèmes en évaluant les dispositifs mis en place pour maintenir l'intégrité de l'information et de l'infrastructure technologique et réduire au maximum les conséquences des failles et des incidents de sécurité[4] ;
- s'assurer de la gestion de l'environnement physique en évaluant les mesures de protections des actifs informatiques et les données métiers et réduire le risque d'interruption de l'activité[5].

L'audit de la sécurité informatique couvre un large champ qui comprend les applications, les données, les hommes, les réseaux, le matériel, les installations, les procédures…

Cette étude sera limitée aux :

- dispositifs mis en place pour la sauvegarde du matériel informatique (hardware) ;

[2] CLEUET & al (2008a) et ISACA in AFAI (2008b).
[3] COBIT 4.1 PO9
[4] COBIT 4.1 DS5
[5] COBIT 4.1 DS12

- 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).

L'intérêt d'une telle étude pour l'entreprise est de pouvoir évaluer et situer sa maîtrise 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.

L'intérêt pour le lecteur est qu'il constituerait une aide à la connaissance des risques informatiques et des moyens de prévention de même qu'une aide à la connaissance des méthodes d'audit informatiques pour l'aspect sécurité.

Notre intérêt sera la mise en pratique des enseignements reçus tout au long de notre formation. Cette étude est pour nous le point culminant de notre formation d'une année.

Ce sujet sera traité en deux parties.

La première concernera les aspects théoriques de l'audit de sécurité informatique et comprend trois chapitres repartis ainsi qu'il suit : le premier présentera Le système informatique et la sécurité, le second sera consacré à l'audit de la sécurité informatique et le troisième à la méthodologie de recherche. La deuxième présentera l'aspect pratique et se composera de trois chapitres : le premier concernera la présentation de l'ASECNA Cameroun, le second sera consacré à la Description de la sécurité informatique et le troisième présentera et les travaux d'audit et les résultats obtenus.

PREMIERE PARTIE : CADRE THEORIQUE

Introduction

Le système informatique est l'un des domaines de l'entreprise devant bénéficier d'une gestion de sécurité optimale. La montée en puissance de la cybercriminalité, les menaces de l'environnement internes et externes font peser des risques sur ce système stratégique de l'entreprise. En effet, du fait de sa particularité de dispositif transversal, l'impact éventuel des risques qui l'affectent se répercutent dans toute l'organisation. Sa sécurité doit donc être mise en place de façon pointilleuse, et être évaluée régulièrement.

L'évaluation de la sécurité du système informatiques 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.
Ainsi, nous consacrerons cette partie au système informatique et à la sécurité, puis à l'audit de sécurité informatique et nous terminerons par notre méthodologie de recherche.

Chapitre 1. Le système informatique et la sécurité

Les entreprises modernes dépendent aujourd'hui pour l'atteinte de leurs objectifs de l'outil informatique. L'ensemble de ces outils et des procédures de mise en œuvre est appelé système informatique. Quelques fois, le même ensemble prend le nom de système d'information. Il s'agit là de deux notions connexes que nous allons décrire pour mieux en cerner la nuance. Nous allons ensuite présenter les risques pouvant affecter ce système puis nous terminerons ce chapitre par la description des dispositifs relatifs à la sécurité de ces outils.

1.1. Description d'un système informatique

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 ».

Nous pouvons donc affirmer dans ce cas que le système informatique en est la colonne vertébrale, car il est le support du système d'information.

1.1.1. Le système informatique comme support du système d'information

Pour DAYAN & al (2004), le système d'information ne se réduit pas au système informatique. En effet, dans l'esprit de nombreuses personnes s'est installée une confusion entre système d'information et système informatique. L'informatique reste un support et un véhicule privilégié de l'information formalisée. Elle est un moyen et seulement un moyen parmi d'autres.

Selon LAUDON & al (2002), bien que les systèmes d'information informatisés se fondent sur la technologie informatique pour traiter des données brutes et pour les transformer en informations ayant une signification, il faut bien distinguer un ordinateur et un logiciel, 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.

Un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures…permettant d'acquérir, de traiter, de stocker des informations dans les organisations, (REIX, 2005).

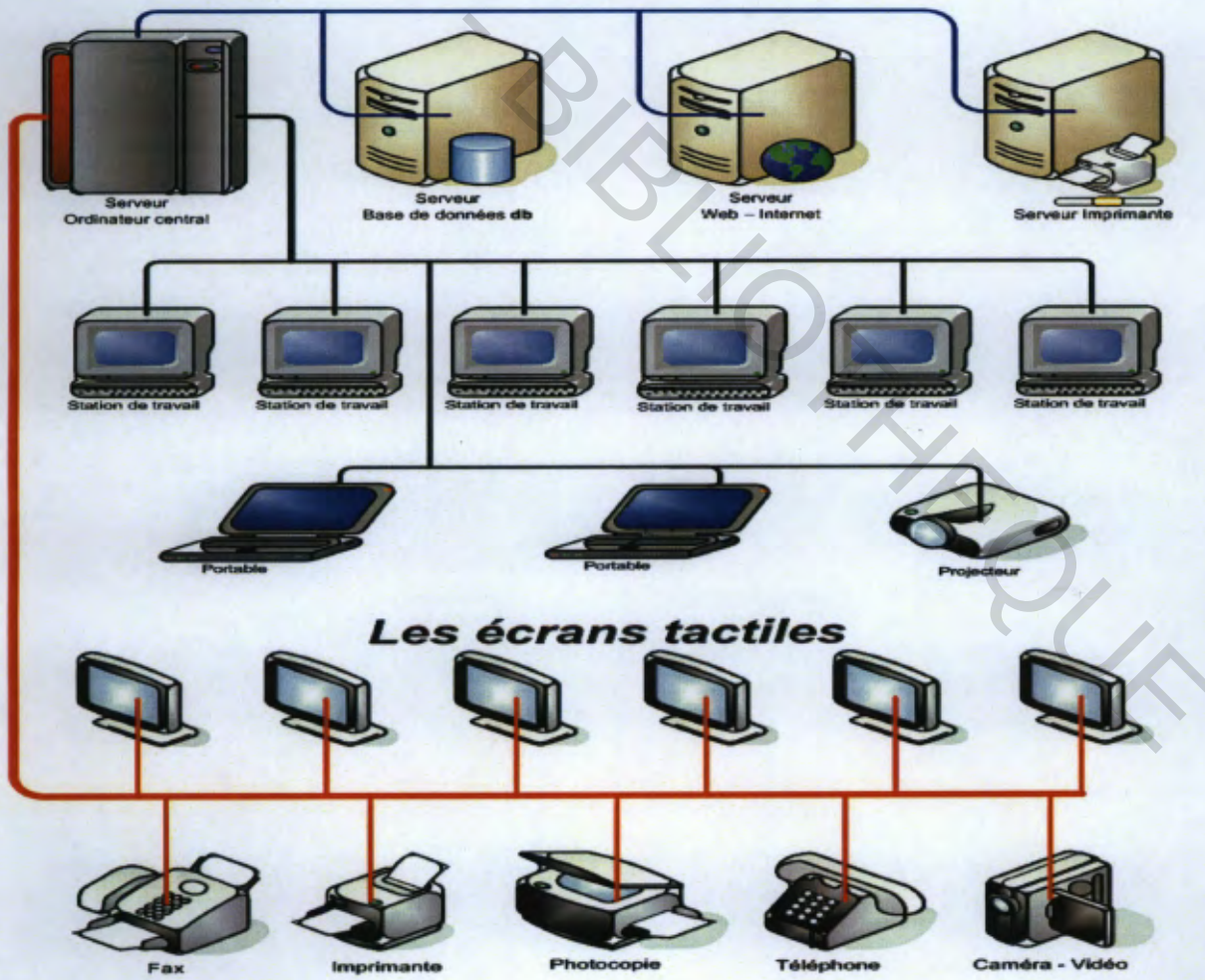
1.1.2. Architecture d'un système informatique

Selon DAYAN & al (2004 : 1075), « le système informatique est le support technique du système d'information de l'entreprise. Cela regroupe les moyens informatiques (serveurs et poste 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 regroupe les postes de travail, les supports de stockage, les serveurs et les réseaux sans lesquels cet ensemble serait inopérant. La figure ci-après nous donne une vue de ces différents composants en réseau.

Figure 1: Exemple d'éléments constitutifs d'un système informatique.



Source : GUARDIAN-SOFT (2010).

Au vu de la figure 1, le système informatique est composé d'éléments divers.

1.1.2.1. Les serveurs

Selon YADAV & SINGH (2009), 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 le serveur de 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 d'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 de courrier est utilisé pour stocker et transmettre du courrier électronique. Un serveur web stocke et manipule les pages d'un site Web et les transmets sur demande de l'utilisateur. Un serveur de jeu arbitre et suit l'évolution d'un jeu en mettant en communication les différents joueurs. Un serveur d'applications effectue les traitements d'un ou plusieurs logiciels applicatifs à architecture client/serveur. Un serveur proxy (mandataire) reçoit des demandes, les contrôle, puis les transmet à d'autres serveurs, (YADAV & SINGH, 2009).

1.1.2.2. Les postes utilisateurs ou ordinateurs

Ce sont les ordinateurs de bureau et leurs périphériques d'entrée/sortie, les ordinateurs portables, les ordinateurs de poche, les tablettes et les Smartphones qui permettent de se connecter de n'importe quel lieu où une connexion réseau est disponible, (DAYAN & al, 2004).

1.1.2.3. Les équipements électroniques

Selon CARPENTIER (2009), c'est l'ensemble constitués par tous les appareils électroniques qui peuvent être intégrés au système informatique. Il s'agit principalement des imprimantes, des scanners, des vidéo projecteurs, des appareils fax, des téléphones, des photocopieurs, des caméras numériques, des clés USB, des lecteurs MP3, des disques durs externes…

1.1.2.4. L'infrastructure réseau

L'infrastructure réseau ou supports 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 propagent 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).

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).

1.1.2.5. La salle informatique ou data center

Selon la SMI[6] (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 plupart 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...).

1.2. Les risques informatiques

Tous les systèmes informatiques, quelles que soient leurs tailles, leurs structures, sont confrontés à des risques. Nous définirons donc la notion de risque et nous présenterons les risques informatiques.

1.2.1. Définition du risque

Le risque opérationnel défini par le « nouvel accord de Bâle » est le risque de perte directe résultant d'une inadéquation ou d'une défaillance attribuables à des personnes, des procédures, des systèmes mis en place et à des évènements extérieurs.

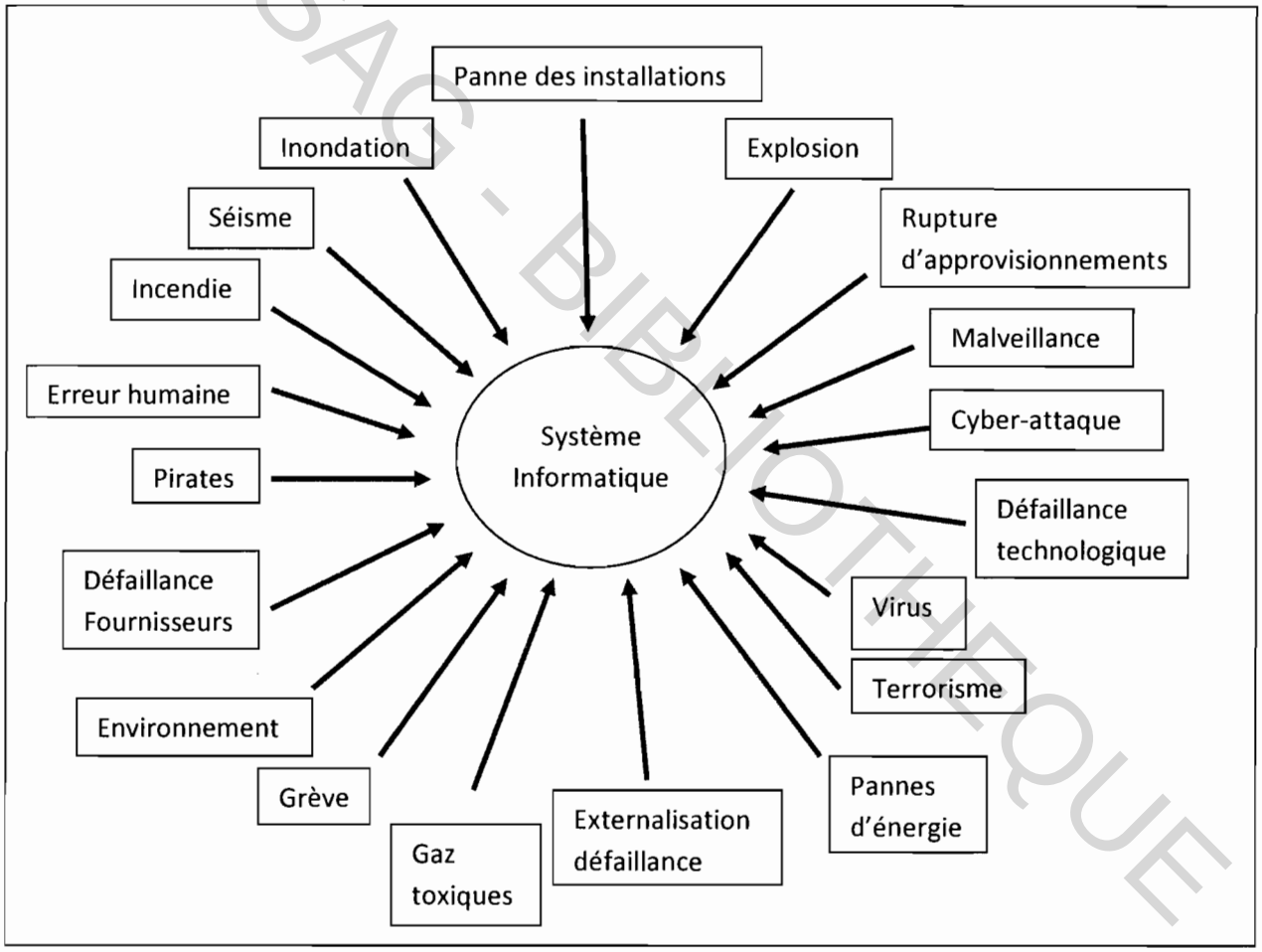
Selon l'IFACI (in RENARD 2010 : 155), « le risque est un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont

[6] SOCIETE DE MARKETING INDUSTRIEL

notamment pour mission d'assurer autant que faire se peut la maîtrise », pour 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).

Figure 2: Les risques inhérents du système informatique de l'entreprise



Source : Nous même, à partir de DUGELAY (2003 : 17).

Comme nous le voyons sur la **figure 2**, les risques propres au système informatique ou risques inhérents sont d'une part les risques physiques, qui affectent le matériel informatique et d'autre part les risques logiques qui eux sont relatifs à la partie immatérielle du système informatique (logiciels, données, informations), et ceci sans tenir compte du contrôle interne

qui pourrait exister dans l'entité. Ces risques sont présentés dans les paragraphes suivants de cette section.

1.2.2. Les risques physiques

Selon GODARD (2002) & ACISSI (2009), sans être exhaustif, les plus envisageables sont :

- les dégâts des eaux ;
- le feu ;
- l'électricité ;
- les défauts de climatisation ;
- les intrusions physiques ;
- les phénomènes électrostatiques.

Il existe plusieurs modes de classification des risques informatiques. Nous retenons pour la présentation des risques physiques la nomenclature qui distingue les risques humains, environnementaux, électriques et les sinistres, (CALE & TOUITOU, 2007).

1.2.2.1. Les risques humains

Selon CARPENTIER (2009), la circulation des personnes non autorisées dans les locaux peut entraîner divers incidents : vols, pertes de confidentialité, sabotages, etc., avec des conséquences aisément imaginables (pertes de temps, pertes financières, pertes de réputation, indisponibilité du système informatique, etc.).

La menace d'une attaque terroriste sur des sites stratégiques est hélas d'actualité. Elle entrainerait la destruction de l'infrastructure technologique.

1.2.2.2. Les risques environnementaux

Ici il s'agit des fluctuations de température, de l'hygrométrie et de la poussière. Ces éléments peuvent entrainer des incidents techniques de nature à ralentir l'activité. La survenance d'un tremblement de terre est une éventualité qui pourrait gravement affecter le système informatique du fait de la destruction des bâtiments et de la rupture des câblages, (CLEUET & al, 2008b).

1.2.2.3. Les risques électriques

Selon ROYER (2004), les risques liés à l'électricité proviennent surtout de : surtension, sous-tension, coupures de courant. Malgré la qualité du fournisseur, ces incidents sont difficilement prévisibles et ont un impact sur le système informatique (pertes de données, pannes d'équipements, etc.). La foudre peut également être classée dans cette catégorie.

1.2.2.4. Les sinistres

Les sinistres sont principalement dût à l'eau et au feu.
Pour l'eau, il s'agit de : rupture de conduite, infiltration, déclenchement de systèmes anti-incendie, obstruction des évacuations d'eaux usagées, inondation... Les causes sont nombreuses, tout comme les conséquences : courts-circuits, dangers d'électrocution, détérioration des équipements, corrosion des câbles et connecteurs, (GODART, 2002).

Les dégâts du feu peuvent entraîner la destruction partielle ou totale des équipements informatiques (centre informatique, câblage, atteinte physique aux équipements informatiques, etc.) et donc l'indisponibilité de tout ou partie de l'architecture durant une assez longue période. A noter qu'ils s'accompagnent souvent des dégâts liés à l'eau du fait des tentatives d'extinction, (CARPENTIER, 2009) & (CLEUET & al, 2008b).

1.2.3. Les risques logiques

Ce sont les risques qui affectent les personnes (*social engineering*), les logiciels, les données et les informations du système informatique. Ils sont le fait soit de personnes internes à l'organisation, soit le fait de personnes externes à travers les réseaux (internet, Wifi).
Selon CALE & TOUITOU (2007) et ROYER (2004), l'être humain est le maillon le plus faible du système d'information, il représente ainsi la plus grande menace pour la sécurité informatique. L'ignorance des menaces et des techniques des cybercriminels est un facteur aggravant des risques informatiques.
De nouvelles menaces apparaissent chaque jour. Nous allons présenter les risques les plus significatifs.

1.2.3.1. Les malwares

Selon ACISSI (2009), CALE & TOUITOU (2007), les malwares sont des programmes malveillants qui sont utilisés par les pirates pour commettre leurs forfaits. Ils sont de plusieurs types :

- Le virus informatique comme son équivalent biologique, s'installe au sein des programmes légitimes pour se reproduire et contaminer le plus de fichiers possible et ensuite déclenche l'action pour laquelle il a été crée.
- Le ver informatique est différent du virus en ce sens qu'il est un programme autonome qui se déplace dans les réseaux informatiques 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 de données, l'établissement d'une connexion à travers un pare-feu. Il permet à son concepteur de faire du chantage, de l'espionnage industriel et commercial, des détournements de 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 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 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 de plusieurs sortes :
    - le spyware est un petit logiciel qui s'installe à l'insu de l'utilisateur pour transmettre des données et des fichiers ;
    - 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 ;
    - l'adware collecte des informations personnelles (habitudes de navigation, configuration de l'ordinateur, etc.), il permet d'afficher des publicités

ciblées ou de rediriger automatiquement vers des serveurs web lorsque l'utilisateur tape certains mots clés.

- le rootkit ou "kit de démarrage" est un programme malveillant qui est utilisé par une personne malintentionnée et qui dissimule la présence de programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, firewall).
- Le dialer est un programme composant un numéro de téléphone pour se connecter à un site ou vers des numéros surtaxés, (CALE & TOUITOU, 2007).

1.2.3.2. Les spam

Selon ACISSI (2009), le spam encore appelé pourriel, désigne l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques à des personnes ne souhaitant pas recevoir ce type d'information. Il est de plus en plus utilisé pour effectuer du *social ingeenering* (technique que nous décrirons dans le présent mémoire).

1.2.3.3. Les facteurs humains

Selon ACISSI (2009), CALE & TOUITOU (2007) et GODART (2002), il s'agit ici :

- des erreurs humaines commises par les informaticiens qui peuvent être lourdes de conséquence. Ces erreurs sont notamment des erreurs de conception, des erreurs de programmation, des erreurs de configuration ou des erreurs par négligence ;
- du social engineering ou ingénierie social qui consiste à exploiter la confiance humaine pour obtenir des informations (numéros de téléphone, organigramme, mot de passe, 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 (service sécurité, administrateur système, etc.) ;
- du *phising* ou hameçonnage qui est une technique qui consiste à créer une réplique presque 100 % parfaite d'un site Web qui entreprend subrepticement d'extorquer à des utilisateurs leurs données d'accès personnelles (nom d'utilisateur, mot de passe, code PIN, etc.) au moyen d'un formulaire présenté sur le site Web contrefait.

1.2.3.4. Les atteintes à la disponibilité ou déni de service

Le déni de service est un type d'attaque qui a pour but de rendre indisponible un service ou d'en détériorer la qualité afin de l'empêcher de répondre aux demandes légitimes. Cette technique permet à son auteur de ne pas rentrer par effraction dans le système cible, il utilise des canaux de communications généralement ouverts, (ROYER, 2004).

1.2.3.5. Les compromissions de l'information et les usurpations d'identité

Selon GODART (2002) , il s'agit ici de vol d'informations confidentielles par cassage de messages crypté ou cassage de mots de passe, le *snifing* ou encore la récupération de données effacées. L'information peut également être manipulée en modifiant le contenu des pages d'un site Web.

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

1.2.3.6. Les nouvelles menaces

Pour CALE & TOUITOU (2007), l'usage de la téléphonie sur IP et du Wifi sont désormais des cibles potentielles pour les cybercriminels faisant appel au déni de service. Les logiciels P2P (*peer-to-peer*), l'usage des clés USB, des iPOD, des disques durs externes ainsi que le téléchargement de fichiers (image, audio, vidéo etc.) sont également de grands vecteurs de risque. Les usurpations d'identités, les intrusions, les attaques par des vers, les écoutes et l'enregistrement des communications sont les risques associés à ces technologies. La possibilité de mettre en place un point d'accès Wifi pirate est aisé, il s'agit de la technique du « *man in the middle* ».

Nous classerons également dans cette catégorie les menaces liées à l'utilisation de logiciels sans licence d'exploitation et l'usage des copies de logiciel illégales.

A travers cette présentation non exhaustive des risques inhérents au système informatique, force est de constater que les menaces sont nombreuses et de diverses natures. Afin de s'en prémunir l'entreprise doit mettre en place des dispositifs et des procédures de sécurité que nous allons présenter dans la section suivante.

1.3. La sécurité informatique : le contrôle interne de la fonction informatique

Selon le COSO in RENARD (2009 : 137) « le contrôle interne est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation destiné à fournir une assurance raisonnable quant à la réalisation des objectifs »

Le contrôle interne de la fonction informatique provient du fait que dans la plupart des grandes entreprises, la quasi-totalité des procédures et processus reposent sur des traitements informatiques ; cela conduit au respect des cinq composants du contrôle interne qui sont l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication et enfin le pilotage. Le respect de ces conditions implique donc la mise en place d'un dispositif spécifique dédié au système informatique : la sécurité informatique.

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

« 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 », (GODART, 2002 : 16-17).

La sécurité informatique consiste aussi à s'assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Selon ACISSI (2009), CARPENTIER (2009) et GODART (2002), la sécurité informatique est caractérisée par cinq principes :

- 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 de la protection contre la consultation de données stockées ou échangées. Les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- L'intégrité : ce principe garantit à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au

cours de la communication ; la mise en œuvre de ce principe doit permettre de valider l'intégralité, la précision, l'authenticité et la validité des données.

- La disponibilité : il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment et que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement.
- La non-répudiation : cette caractéristique 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 prouvent que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée. L'élément de la preuve de non-répudiation doit permettre l'identification de celui qu'il représente ; il doit être positionné dans le temps (horodatage), il doit présenter l'état ou le contexte dans lequel il a été élaboré.
- L'authentification : c'est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système. Elle assure l'identification d'un individu, d'une entité mais également l'origine de l'information ou de l'opération traitée par le système.

A ces cinq principes communs, CARPENTIER (2009) et GODART (2002) définissent un sixième principe qui est :

- La journalisation ou la preuve : elle assure que tout accès à un système, tout accès à une information ainsi que toute opération exercée sur ceux-ci soit toujours enregistrée et répertoriée.

Ces caractéristiques doivent être mises en œuvre dans le cadre de la politique de sécurité qui est définie par les dirigeants de l'entreprise et la Direction Informatique et dont le rôle est le choix des solutions organisationnelles et techniques aux problèmes de sécurité informatique.

1.3.1. La politique de sécurité informatique

La politique de sécurité est le principal document de référence en matière de sécurité informatique ou sécurité des systèmes d'information. Elle a pour objectif de définir la protection des systèmes d'information. Elle reflète la vision stratégique de l'organisation et montre l'importance qu'accorde le manager à son système d'information, (ANSSI, 2010).

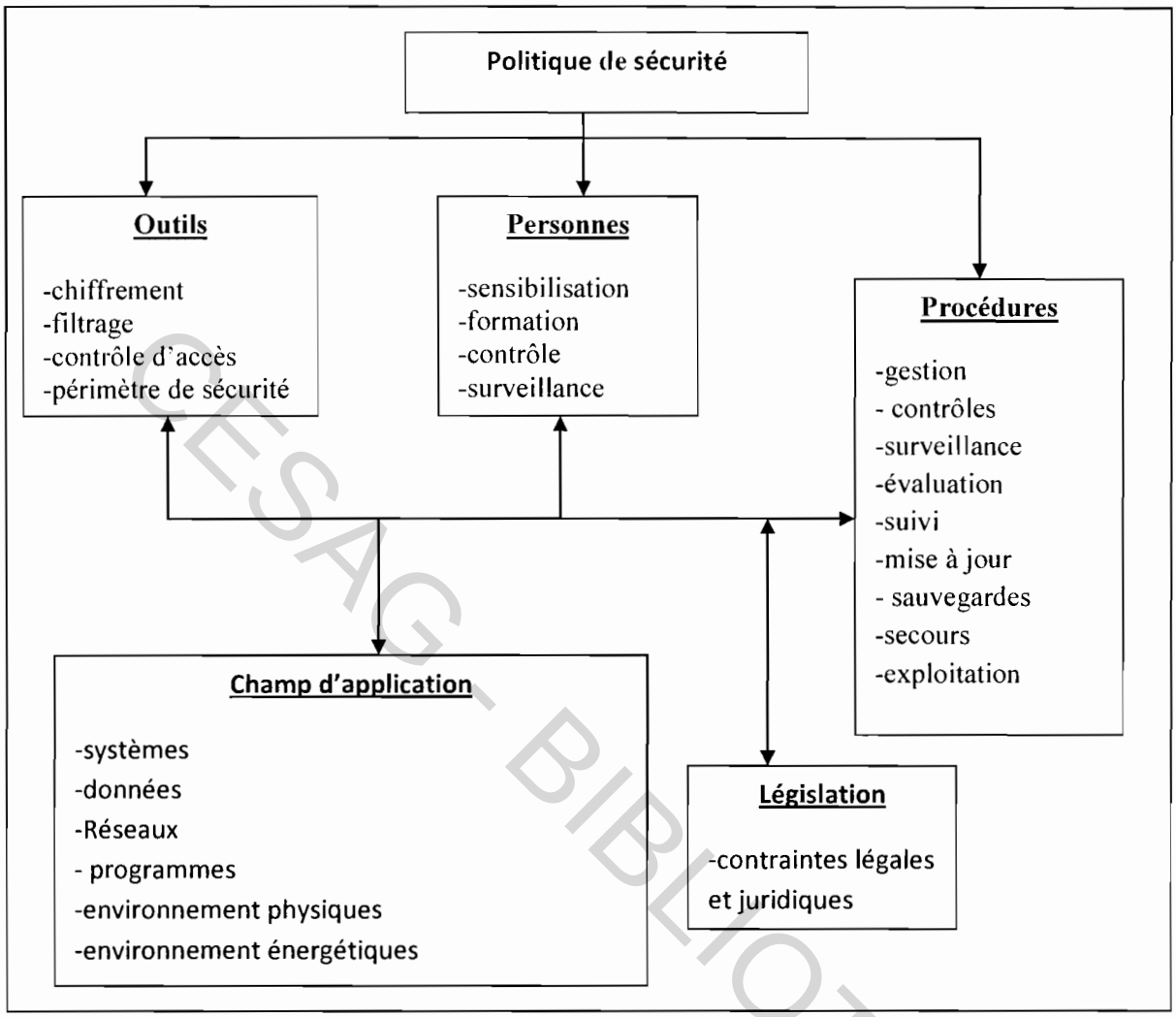
La politique de sécurité se présente sous la forme d'un ensemble de documents qui présentent de manière ordonnée les règles de sécurité, les directives, procédures, règles organisationnelles et techniques à appliquer et à respecter. Ces règles sont généralement issues d'une étude des risques des systèmes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

Selon ANSSI (2007) et SUPRALOGIC (2010), les éléments essentiels de la politique de sécurité sont :

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

La figure ci-après nous donne une idée claire de la politique de sécurité dans toutes ses composantes.

Figure 3: La politique de sécurité informatique



Source : Nous même, à partir de CARPENTIER (2009 : 34).

1.3.2. La charte informatique

Selon EOX-PARTNERS (2009), c'est un document à forte connotation juridique qui est souvent associé au règlement intérieur de l'organisation. Elle est inspirée de la politique de sécurité du système informatique. La charte définit les règles d'utilisation de l'outil informatique ; elle définit aussi les responsabilités et les droits des utilisateurs (interne et externe).

Selon CALE & TOUITOU (2007), la charte informatique a comme objectifs de fixer les droits et obligations des utilisateurs concernant l'usage des ressources informatiques en définissant les règles d'usage et de fonctionnement, d'informer les utilisateurs des moyens de

contrôle mis en place pour surveiller et limiter l'utilisation des ressources informatiques et de permettre une meilleure gestion des coûts et des risques liés à cette utilisation notamment en termes de sécurité, de responsabilité, d'image et de réputation.

1.3.3. Les acteurs de la sécurité informatique

Ce sont toutes les personnes qui jouent un rôle dans la prévention et la gestion des risques informatiques.

1.3.3.1. La Direction Générale

Selon GRAEVE & POTIER (2001), la Direction Générale est le maitre d'ouvrage de la sécurité informatique. C'est la direction générale qui définit la politique de sécurité, affecte les budgets et définit toute la stratégie de sécurité de l'entreprise. De plus, elle est responsable du respect des prescriptions légales et réglementaires relatives à l'information, au respect et à la protection des propriétés intellectuelles et des œuvres produites et/ou utilisées au sein de l'entreprise. Il en est de même pour le respect des prescriptions fiscales. Nous reviendrons sur ces points dans le paragraphe qui traite des contraintes légales et réglementaires.

1.3.3.2. Le responsable de la sécurité du système d'information

Selon CARPENTIER (2009) et REIX (2005), désigné par la Direction Générale, le responsable de la sécurité du système d'information (RSSI) ou le responsable du système informatique (RSI) est le maitre d'œuvre de la politique de sécurité informatique. Il établit des procédures spécifiques, limite les accès au réseau en cas d'informations stratégiques, s'assure de l'intégrité des données et veille régulièrement à ce que le réseau ne présente aucune faille. Il contribue à garantir la disponibilité du système d'information de l'entreprise, préserve son intégrité et sa confidentialité et assure la sécurité des transactions électroniques. En cas d'inexistence de ce dispositif, cette tâche peut être dévolue au responsable de l'informatique. Le RSI possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique. C'est une fonction essentiellement managériale qui consiste à encadrer une équipe d'ingénieurs et de techniciens d'exploitation, dont il organise et contrôle le travail.

1.3.3.3. Le risk manager

Selon GRAEVE & POTIER (2001), le risk manager est le gestionnaire des risques de l'entreprise. Il est en charge de l'application générale des politiques, processus et pratiques de traitement des risques. Son rôle peut inclure l'identification, l'évaluation, les mesures de réponse, la surveillance, l'examen et la communication des risques. Le Risk Manager doit réduire au maximum la variabilité des risques et leurs coûts par des mesures appropriées de prévention, de protection ou de transfert (maîtrise des risques). Pour EFFI-SOFT (2010), « on définit la gestion du risque comme le processus d'intégration des résultats de l'analyse des risques dans un contexte global de considérations sociales, économiques, politiques visant à établir la décision. Il est évidemment nécessaire que les critères de choix (ou d'élimination) aient été définis préalablement ».

1.3.3.4. L'audit interne

« L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise et en faisant des propositions pour renforcer son efficacité » (IIA in RENARD, 2010 : 73).

L'audit interne, à travers ses missions de conseil et d'assurance joue un rôle d'aide au management. Son rôle est donc primordiale dans l'évaluation de la politique de sécurité et des différents processus et procédures y relatives.

1.3.3.5. Le personnel

Selon REIX (2005), GRAEVE & POTIER (2001), le personnel est l'utilisateur des ressources informatiques. Son rôle est d'appliquer les règles et principes définis dans la charte de sécurité informatique qui est un dispositif de contrôle interne. Une bonne sensibilisation du personnel aux problèmes de sécurité informatique réduit les risques qui pèsent sur le système informatique.

1.3.4. Les dispositifs de sécurité informatique

Nous présentons dans ce paragraphe les dispositifs qui peuvent être mis en place afin d'assurer la sécurité des actifs informatiques, du point de vue physique et du point de vue logique. Nous allons reprendre la nomenclature utilisée pour la présentation des risques dans la section 2 afin d'associer chaque dispositif de sécurité au risque qu'il permet de maitriser.

1.3.4.1. Les dispositifs de sécurité physique

Ces dispositifs protègent le matériel de façon physique.

- Les risques humains : les ordinateurs portables doivent être équipés de câble en titane qui permettent de les fixer à une table, une armoire ou à une chaise. Une protection des bâtiments doit être mise en place notamment des dispositifs de contrôle d'accès (badges, biométrie, clé, etc.) et de détection des déplacements et des intrusions. Les fenêtres doivent être en double vitrage blindé et les portes donnant sur l'extérieur doivent être blindées et disposées d'une détection d'ouverture reliée à une alarme. Le premier rempart peut être un service de gardiennage qui identifie et filtre les visiteurs. La solidité des bâtiments et une bonne police d'assurances sont le dernier recours à une attaque terroriste, (CALE & TOUITOU, 2007).

- Les risques environnementaux : un double système de climatisation (principal et secondaire) doit être installé avec un contrat de maintenance 24h/24 et 7j/7. Des dispositifs de contrôle d'alerte pour les températures doivent être installés. La salle informatique doit être propre et correctement rangée, (CLEUET & al, 2008a).

- Les risques électriques : les bâtiments doivent être équipés de systèmes évitant les remontées de foudre (paratonnerre, puits de terre, fusibles). Une double alimentation doit être prévue (groupe électrogène) et tous les postes doivent être équipés d'onduleurs adaptés. Les circuits d'alimentation du câblage électrique doivent également être redondants, (SMI, 2010).

- Les sinistres : les dégâts des eaux se préviennent par le choix judicieux de la salle informatique qui ne doit pas être située en sous-sol (inondations) ou au dernier étage (infiltrations). Les équipements doivent être surélevés et des tubes hermétiques

doivent être utilisés pour les câblages d'alimentations et de réseaux. Le plancher doit être compartimenté de façon à contenir et à diriger l'eau vers les systèmes d'évacuation, (ROYER, 2004).

Les dégâts du feu se préviennent en évitant de disposer au voisinage de la salle informatique des produits inflammables, en évitant des kyrielles de blocs de multiprises et en vérifiant régulièrement les circuits électriques. Des armoires ignifugées doivent être prévues pour le stockage des supports informatiques. Un système de détection d'incendie qui déclenche une alarme et/ou un mécanisme d'extinction (de préférences au gaz halon, Co2, FM200, etc.). Ce système doit couper l'alimentation électrique avant de déclencher le dispositif d'extinction. Des extincteurs doivent être disposés dans les bâtiments. Les installations stratégiques et complexes doivent être reliées par un dispositif d'alerte automatique à la caserne des pompiers la plus proche, (CLEUET & al, 2008a) et (SMI, 2010).

Tous ces dispositifs doivent être entretenus et testés régulièrement par un personnel compétent et ces opérations doivent être consignées dans un registre.

1.3.4.2. Les dispositifs de sécurité logique

Nous ferons une présentation de quelques dispositifs ou solutions suivant la présentation faites des risques logiques (dans le paragraphe 1.2.3.).

- Les malwares : face à ces menaces, la solution de sécurité est l'usage d'un logiciel antivirus sur les postes clients ainsi que sur les serveurs, couplé à un dispositif pare-feu ou *firewall,* (CLEUET & al, 2008a).
- Les Spam : tout comme les malwares, ces menaces peuvent être repoussées grâce à l'usage d'un logiciel antivirus qui intègre un module de filtre de courriers indésirables.
- Les facteurs humains : les erreurs humaines peuvent être détectées lorsque la séparation des tâches et des environnements est effective et que le personnel informatique est supervisé. Le *social engineering* et le *phising* se préviennent par la sensibilisation et une grande vigilance du personnel d'entreprise, la charte informatique trouve ici toute son utilité (ACISSI, 2009).
- Les atteintes à la disponibilité ou déni de service : l'usage d'un *proxy,* d'un firewall, de sonde réseaux et la mise en place de réseau privé virtuel permettent de faire face à ce type d'attaque. Les contrôles d'admission réseau, le compartimentage du système

informatique et l'usage d'un *honey pot* sont d'autres parades limitant les attaques au cœur du dispositif informatique (CALE & TOUITOU, 2007).

- La compromission de l'information et l'usurpation d'identité : une séparation des environnements études et exploitation de tel sorte que les personnes qui développent les applications et celle qui gèrent le fonctionnement des postes clients ne puissent pas accéder aux même fichiers. Un deuxième dispositif consiste à la limitation des accès aux utilitaires et fichiers systèmes en instaurant des droits d'accès en fonction des tâches auxquelles le personnel utilisateur est affecté. Le troisième dispositif est l'usage de mot de passe « fort » qui doit comporter au moins huit caractères différents et qui doit être changé régulièrement et rester confidentiel. Au-delà de ces mesures préventives, la majorité des systèmes peut conserver la trace des principaux évènements passés, il s'agit de mouchard ou fichier log system qui constitue une piste d'audit pour trouver l'origine des problèmes systèmes ou des fraudes. L'usage de dispositif biométrique (empreintes digitales et rétiniennes, carte d'accès, etc.) sur les postes utilisateurs se répand dans les zones sensibles, de même que le recours à la cryptographie pour les documents confidentiels, (ACISSI, 2009) et (ROYER, 2004).
- Les nouvelles menaces : le wifi doit être fermé afin de ne pas diffuser des informations de nature à permettre une authentification par des pirates, un système de détection des intrusions propre au wifi doit être installé, il doit permettre de signaler des interférences qui sont des indices de tentative de mise en œuvre d'un point d'accès pirate. L'usage des périphériques amovibles doit être limité, pour ceux dont l'usage est fréquent et indispensable, il faudrait privilégier lors de l'achat de ces périphériques, ceux disposants d'une autorisation d'accès par mot de passe, (CALE & TOUITOU, 2007).

Ces dispositifs techniques comme nous le voyons font partie d'une gestion organisationnelle de la sécurité et dont ils ne sont qu'une composante.

1.3.5. Le plan de sauvegarde et le plan de secours informatique

Ces processus sont des éléments du plan de continuité d'activité. Leurs mises en place résultent de la dépendance de plus en plus grande des entreprises envers l'informatique. Ces processus ont pour rôle de permettre à l'entreprise de continuer son activité en mode dégradé en cas de sinistre important, de récupérer des données effacées ou d'utiliser des versions

antérieures des logiciels et informations du système informatique . Le contexte limité de cette étude ne permet pas d'aborder le sujet de façon exhaustive. Nous ferrons une présentation sommaire de ces deux dispositifs de la gestion organisationnelle de la sécurité.

1.3.5.1. Le plan de sauvegarde

Selon BUTEL (2008) 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. Improvisation et sauvegarde sont deux mots antinomiques. En revanche, anticipation et sauvegarde sont étroitement liées. Un bon plan de sauvegarde doit être exhaustif, fiable, évolutif, cohérent et auditable. De façon concrète il est composé de trois éléments essentiels :

- 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 détaillée des actions à entreprendre pour sauvegarder les données, les méthodes et outils employés, les fréquences de sauvegarde, le nombre de générations 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).

1.3.5.2. Le plan de secours informatique

« 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 des conditions qui permettent la survie de l'entreprise », (MENTHONNEX, 1995 : 211).

Un plan de secours est composé de dispositifs élémentaires dont l'activation dépendra de l'événement survenu et du contexte général. Ces dispositifs sont généralement classés par type d'activité :

- mobilisation des ressources nécessaires ;

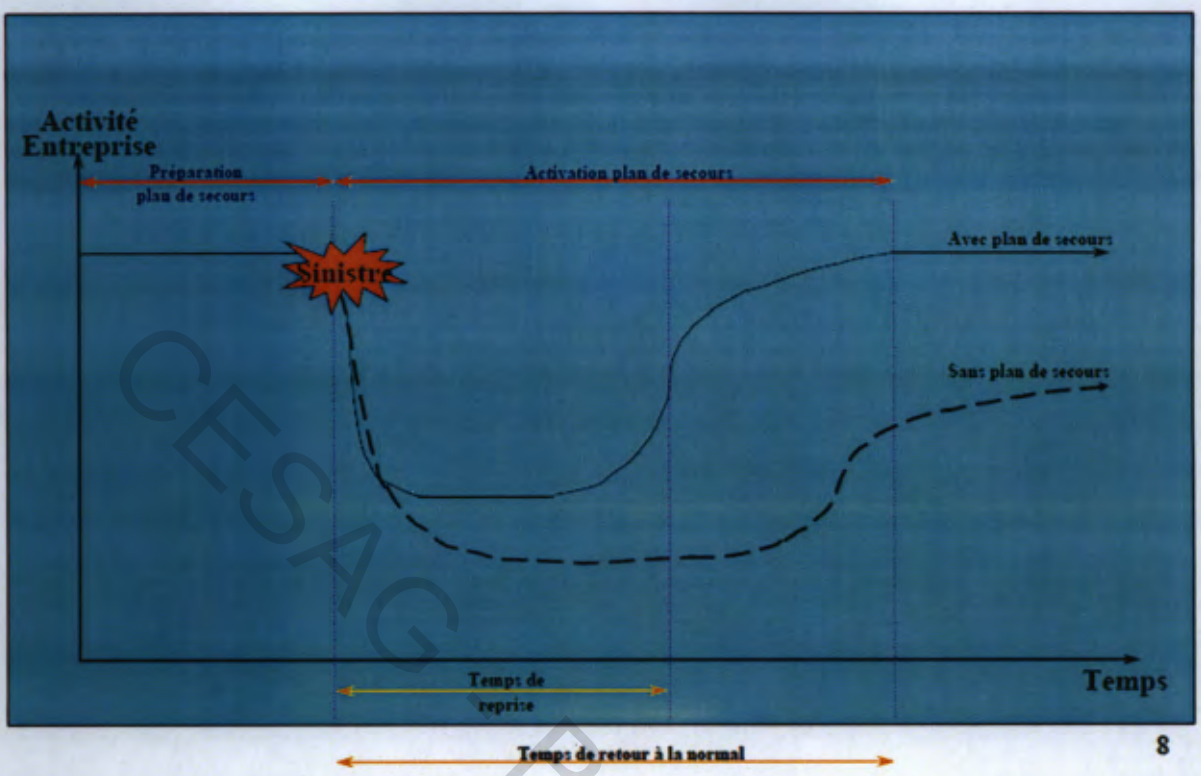
- secours des équipements informatiques, des réseaux et de la téléphonie ;
- reprise des traitements ;
- logistique ;
- relogement ;
- reprise des activités des services utilisateurs ;
- communication de crise ;
- dispositifs de post-reprise.

Afin que leurs niveaux soient garantis, les dispositifs de secours doivent être accompagnés de dispositifs permanents tel qu'un plan de sauvegarde, la formation des acteurs, etc. (CLUSIF 2003).

Le plan de secours aboutit assez souvent à une duplication de l'infrastructure informatique sur un autre site. Un contrat peu être également passé avec un fournisseur et/ou un assureur pour une fourniture de matériel en cas de survenance d'un sinistre lorsqu'on ne dispose pas d'un site de secours préalablement équipé.

Selon CLEUET & al (2008 : 46), « cette démarche de remplacement des ressources matérielles du système d'information peut être complétée par des procédures, dites dégradées, permettant aux utilisateurs de travailler manuellement en l'attente d'une remise en service du système informatique ».

Figure 4: Pourquoi un plan de secours ?



Source : BUTEL in (CLUSIF, 2008 : 8).

Comme l'indique la figure ci-dessus, un plan de secours permet à une entreprise de retrouver assez rapidement son niveau d'activité tandis que sans plan de reprise, le retour au niveau d'activité d'avant sinistre est très lent et l'entreprise ne retrouve pas son niveau d'activité d'avant sinistre.

1.3.6. Les contraintes légales et réglementaires

L'acte uniforme de l'Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA) portant harmonisation des comptabilités en son article 22 relatif au traitement informatique de la comptabilité reprend dans ses alinéas 1 à 7 les principes de la sécurité informatique que nous avons présentés en début de cette section qui sont : la confidentialité, l'intégrité, la disponibilité, la non-répudiation, l'authentification et la journalisation ou preuve. Le même acte uniforme en son article 24 évoque la conservation des pièces comptables pour une période de dix ans, ce qui nous ramène à la sauvegarde et l'archivage

informatique. Les administrations fiscales de nombreux pays[7] tel que le Cameroun (dans le livre de procédures fiscales en ses articles L4, L5 et L6) ou la France (dans le livre de procédures fiscales notamment les articles L13, L47, L74 et L102b) vont d'ailleurs dans ce sens.

L'Organisation Africaine de la Propriété Intellectuelle (OAPI) ne propose pas à ce jour de classification claire pour les œuvres informatiques en effet, les informations présentées sur son site internet ainsi que les formulaires d'enregistrement des œuvres intellectuels ne comportent pas de section relative aux œuvres informatiques.

En France, la loi n° 85-660 du 3 juillet 1985 relative à la protection des logiciels et des progiciels protège la propriété intellectuelle des concepteurs de logiciels contre la copie ou l'utilisation non autorisée. La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique protège les propriétaires d'un système informatique contre une série d'actes de malveillance ou de piraterie qui sont : l'accès ou maintien frauduleux dans un système informatique avec dommages, volontaires ou non, la modification ou la suppression de données, altération du système, l'entrave volontaire au fonctionnement d'un système informatique, l'introduction, suppression, modification intentionnelles du mode de traitement, des transmissions de données, la falsification de document informatique, usage de document falsifié, (CLEUET & al, 2008a).

Conclusion

Le système informatique est stratégique pour l'entreprise car il constitue un processus transversal, support de tous les métiers. Cependant il est sous la menace de nombreux risques liés à son environnement et à sa nature. La sécurité informatique qui est un dispositif de contrôle interne, technique et organisationnel, doit donc prémunir le système informatique de la survenance d'un risque qui pourrait mettre en péril la disponibilité de ce système et donc, la continuité de l'exploitation de l'entreprise.

[7] Il s'agit des Etats membres de l'OHADA : Bénin, Burkina Faso, Cameroun, Centrafrique, Comores, Congo-Brazzaville, Cote d'Ivoire, Gabon, Guinée-Conakry, Guinée Bissau, Guinée Equatoriale, Mali, Niger, Sénégal, Tchad, Togo et Congo-Kinshasa (adhésion en cours).

Chapitre 2. L'audit de la sécurité informatique

Le système informatique est d'une importance stratégique pour l'entreprise. Selon le CLUSIF (2010a), dans son rapport 2010 intitulé *Menaces Informatiques et Pratiques de Sécurité en France*, 73% des entreprises ayant participées à l'enquête jugent lourdes de conséquences une indisponibilité de leurs outils informatiques sur une durée de 24h, ce pourcentage est de 83% pour les entreprises commerciales.

La valeur de ces composants ou actifs, tangibles et intangibles conduits l'entreprise à mettre en place un système de contrôle interne efficace, en adéquation avec les objectifs de l'entreprise. Ce dispositif de contrôle interne doit être évalué afin de s'assurer de son adéquation, de son effectivité et de son efficacité. Pour CLEUET & al (2008a), le contrôle interne se déplace sur le système d'information car l'entreprise ne fonctionne plus qu'à travers celui-ci ; l'enjeu autour de l'information et de la disponibilité du système d'information impose une sécurisation des infrastructures (serveurs) et des réseaux. La notion de plan de continuité se généralise et s'impose dans certains contextes contractuels (aérien, spatial,…) voire réglementaires (applicable aux établissements financiers).

Selon l'IIA in (IFACI, 2009 : 26), la norme 2110.A2, « l'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient et supporte la stratégie et les objectifs de l'organisation ». L'IFACI commente cette norme en précisant que « les systèmes d'information doivent supporter les objectifs actuels et futurs de l'organisation et contribuer à la qualité du contrôle interne (gestion du portefeuille des investissements SI, maîtrise de la fiabilité et de la disponibilité des informations...) ».
L'audit informatique a pour objectif de s'assurer que les activités informatiques d'une entreprise ou d'une organisation se déroulent conformément aux règles et aux usages professionnels, appelés de manière traditionnelle les bonnes pratiques. On va pour cela s'intéresser aux différents processus informatiques comme la fonction informatique, les études informatiques, les projets informatiques, l'exploitation, la sécurité informatique, etc. L'audit de sécurité informatique peut aussi consister à évaluer le niveau de maturité d'un ou de plusieurs processus de l'informatique de l'entreprise.

Pour mener à bien sa mission, l'auditeur doit faire le choix d'une norme et d'un standard correspondant au domaine audité, puis il définit ses objectifs d'audit et enfin il décide d'une approche méthodologique, (CLEUET & al, 2008b).

2.1. Les normes, les standards, les référentiels et les méthodes d'audit informatique

Afin de mener sa mission de manière professionnelle et efficace, l'auditeur va s'appuyer sur des normes, des standards, des référentiels de bonne pratique ou des méthodes spécifiques à l'audit informatique. Nous allons faire une présentation de quelques uns de ces outils.

2.1.1. Les normes ISO 27001 et ISO 27002

Les normes ISO 27001 et ISO 27002, de part leurs universalités, ont été reprises en partie ou totalement dans la plupart des référentiels, standards ou méthodes « technologies de l'information ».

2.1.1.1. L'ISO 27001

Cette norme a pour titre : Technologies de l'information - Technique de sécurité-Système de gestion de l'information - Exigences. Elle a été publiée en octobre 2005 par l'ISO (*International Organization for Standardization* - Organisation Internationale de Normalisation).

D'après l'AFAI (2007) et GUIDEINFORMATIQUE (2010), La norme ISO 27001 définit la Politique du Management de la Sécurité des SI au sein d'une entreprise. Elle spécifie les contrôles de sécurité dont la mise en œuvre est exigée.

La norme ISO 27001 comprend 6 domaines de processus qui sont : définir une politique de la sécurité des informations, 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*).

Selon l'AFAI (2007), l'ISO 27001 porte moins sur l'efficacité de l'organisation mise en place, que sur leur existence, et la mise en place d'une boucle d'amélioration (Planifier-Développer-Contrôler-Ajuster) ou roue de Deming.

2.1.1.2. L'ISO 27002

Publiée en 2OO5 par l'ISO, son titre est: « Codes de Bonnes Pratiques pour la Gestion de la Sécurité de l'Information ».

Selon l'AFAI (2007) et GUIDEINFORMATQUE (2010), La norme ISO 27002 répond à un niveau de détail plus fin que la 27001 et définit une politique de la Sécurité des systèmes d'information. C'est une liste détaillée et annotée de mesures de sécurité. Cette norme est un guide de Bonnes Pratiques pour maîtriser la sécurité d'un système d'information.

Schématiquement, la démarche de sécurisation du système d'information doit passer par 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) et GUIDEINFORMATQUE (2010), la norme ISO 27002 comporte 39 catégories de contrôle et 133 points de vérification répartis en 11domaines :

- politique de sécurité ;
- organisation de la sécurité : organisation humaine, implication hiérarchique, notion de propriétaire d'une information et mode de classification, évaluation des nouvelles informations, mode d'accès aux informations par une tierce partie, cas de l'externalisation des informations ;
- classification et contrôle des biens ;
- sécurité du personnel ;
- sécurité physique : organisation des locaux et des accès, protection contre les risques physiques (incendies, inondations...), systèmes de surveillance et d'alerte, sécurité des locaux ouverts et des documents circulant ;
- 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, dispositions ou politique internes).

Selon l'AFAI (2007), cette norme est essentiellement pragmatique et n'impose pas d'autre formalisme que la mise en place d'une organisation qui garantit un bon niveau de sécurité au fil du temps. Elle est orientée processus et déborde de ce fait des simples aspects de technique informatique. Elle s'intéresse à l'organisation du personnel ainsi qu'aux problèmes de sécurité physique (accès, locaux...).

2.1.2. MEHARI

Selon le CLUSIF (2010c), MEHARI (Méthode Harmonisée d'Analyse des Risques) est une méthode complète d'évaluation et de management des risques liés à l'information, ses traitements et les ressources mises en œuvre. Réduire les risques impose de connaître 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 d'utiliser les pratiques et solutions à la hauteur des enjeux et des types de menaces pesant sur l'information, sous toutes ses formes, et les processus comme les éléments qui la gèrent et la traitent.

Selon l'AFAI (2007), MEHARI est destinée à permettre l'évaluation des risques mais également le contrôle et la gestion de la sécurité de l'Entreprise sur court, moyen et long terme, quelle que soit la répartition géographique du système d'information.

La méthode MEHARI s'articule sur 3 types de plans :

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

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

- analyser les enjeux majeurs ;
- étudier les vulnérabilités ;
- réduire la gravité des risques ;
- piloter la sécurité de l'information.

" 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 ces dysfonctionnements. Il s'agit d'une analyse totalement focalisée sur les objectifs et attentes des " métiers " de l'entreprise, et, de ce fait pérenne. Elle met à contribution les décideurs et le management stratégique de l'entreprise ou de l'entité dans laquelle elle est menée.

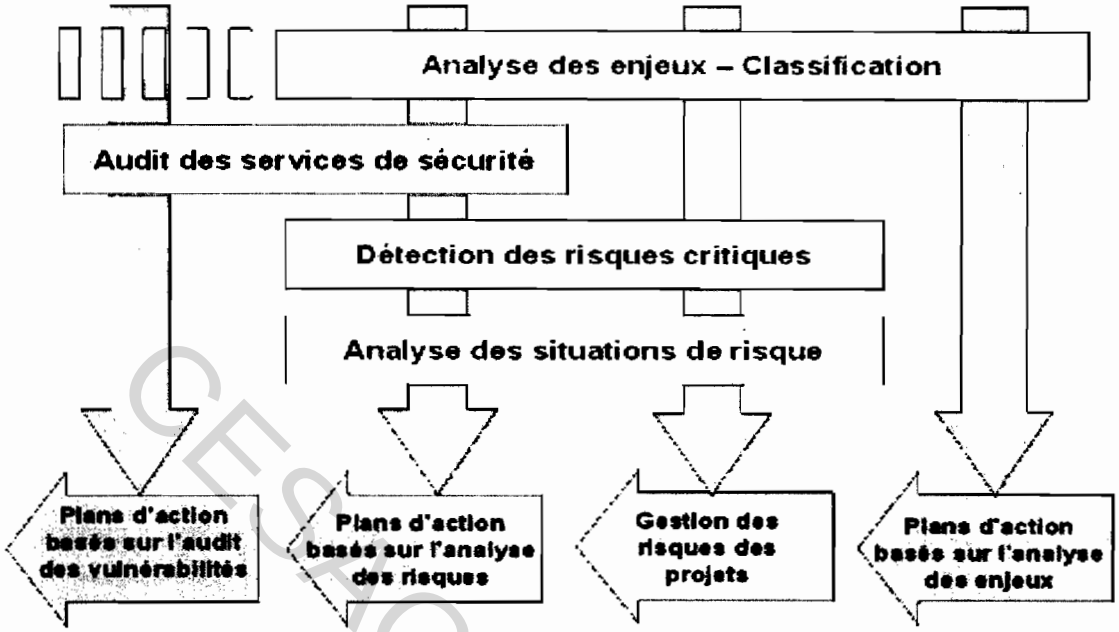
L'analyse des vulnérabilités revient à identifier les faiblesses et les défauts des mesures de sécurité. En pratique, il s'agit d'une évaluation quantitative de la qualité des mesures de sécurité qui couvre l'efficacité des services de sécurité, la robustesse et la mise sous contrôle. Cette analyse des vulnérabilités vise le plus souvent, à vérifier l'absence de points faibles inacceptables, à évaluer l'efficacité des mesures 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, 2010c).

L'analyse des risques couvre l'identification des situations susceptibles de remettre en cause un des résultats attendus de l'entreprise ou de l'organisme ou d'une entité en son sein. La mise en évidence des mesures susceptibles de ramener chaque risque à un niveau acceptable.

Le pilotage de la sécurité demande un cadre structurant pour définir les objectifs annuels ou les étapes de plans d'action, des indicateurs permettant de comparer les résultats obtenus aux objectifs (en termes qualitatifs, quantitatifs et de délais) et des références externes permettant un benchmarking.

Les modules de MEHARI peuvent être combinés, en fonction de choix d'orientation ou de politiques d'entreprise, pour bâtir des plans d'action ou, tout simplement, pour aider la prise de décision concernant la sécurité de l'information (CLUSIF, 2010b).

Figure 5: Les modules de la méthode MEHARI et ses objectifs



Source : CLUSIF (2010c).

2.1.3. COBIT

Le COBIT (*Control Objectives for Information and related Technology* - Objectifs de contrôle de l'information et des technologies associées) a été développé par l'ISACA dont l'AFAI est le correspondant en France. Il couvre 34 processus (voir figure cadre de référence), répartis en quatre grands domaines qui sont :

- le planning et organisation ;
- l'acquisition et mise en place ;
- la fourniture du service et support ;
- la surveillance et évaluation.

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

COBIT s'intéresse à ce qui est nécessaire pour une gouvernance, une gestion et un contrôle adéquats des systèmes d'information au niveau général. COBIT se conforme à d'autres cadres,

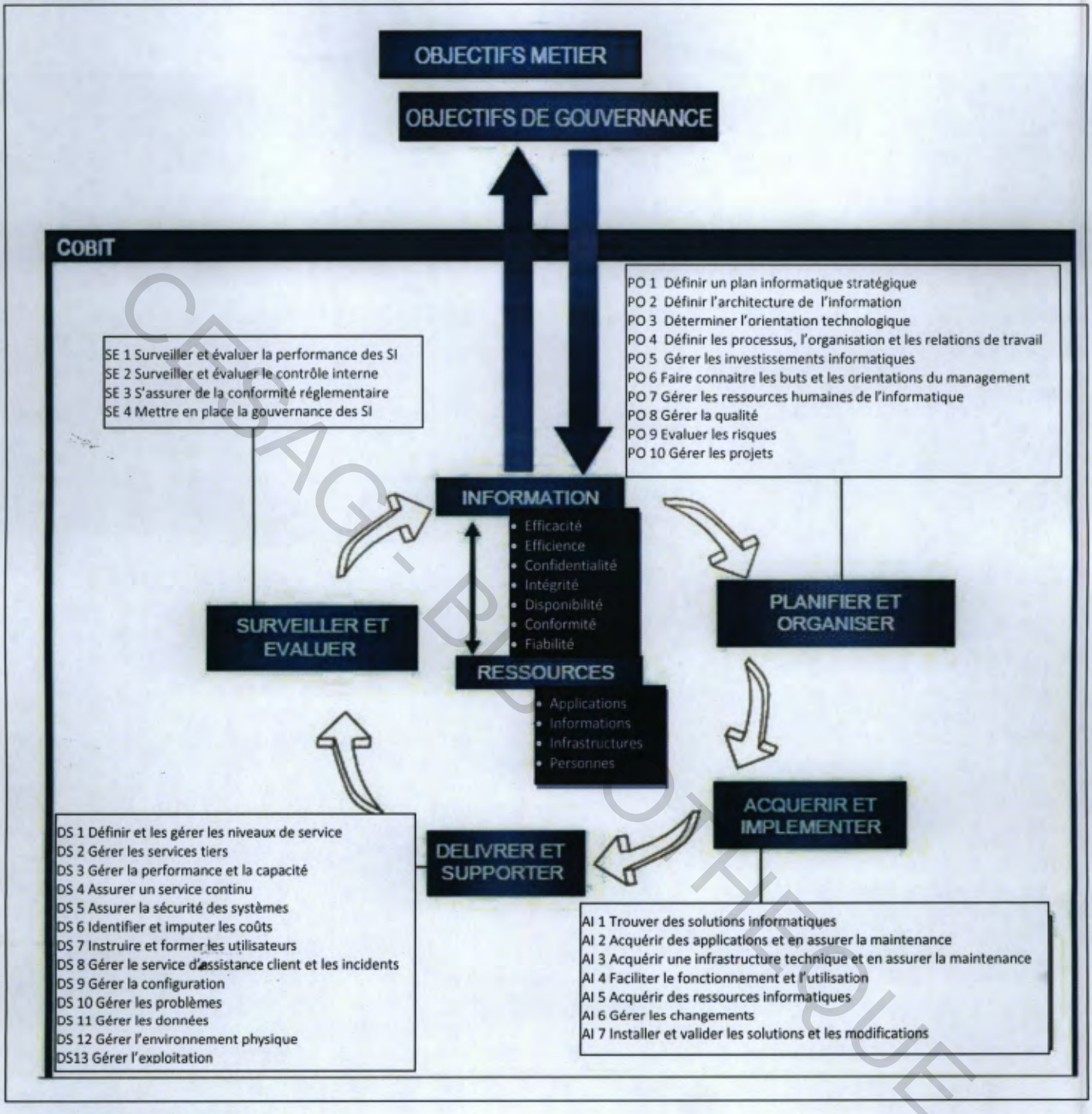
normes et meilleures pratiques informatiques plus détaillés tel que l'ISO 9000, l'ITIL ou le CMMI. COBIT agit comme intégrateur de ces différents guides en réunissant les objectifs clés dans un même cadre de référence général qui fait aussi le lien avec les exigences de gouvernance et les exigences des métiers. Dans ce contexte, le référentiel de contrôle interne COSO et d'autres référentiels semblables qui se conforment aux mêmes principes sont généralement considérés comme les référentiels de contrôle interne pour les entreprises. COBIT est généralement considéré comme le cadre de référence de la gestion et du contrôle des systèmes d'information.

Selon AFAI (2008a), l'adoption de COBIT comme cadre de gouvernance des systèmes d'information offre les avantages suivants :

- 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 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 COBIT est résumé par la figure ci-après.

Figure 6: Cadre de référence COBIT



Source : AFAI (2008b : 10).

A partir de ce cadre de référence global, COBIT donne une liste détaillée de plus de 300 objectifs de contrôle qui permettent à l'auditeur de cadrer son investigation.

Selon CLEUET & al (2008a : 78), « le référentiel d'audit et/ou de contrôle établi à partir de COBIT permet à des auditeurs non informaticiens de mener de façon professionnelle des audits informatiques car il permet de prendre en compte des points 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. Il est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information ».

Selon AFAI (2007), AFAI (2008a), CLEUET & al (2008a) & GUIDEINFORMATIQUE (2010), de nombreux autres référentiels, méthodes et standards existent pour cadrer une mission d'audit informatique. Il s'agit entre autre de ITIL (*Information Technology Infrastructure Library* – Bibliothèque de l'infrastructure des technologies de l'information), du CMMI (*Capability Maturity Model Integrated*), de l'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) ou encore les vingt points de contrôle critique pour une cyber-défense efficace (*20 Critical Security Controls for Effective Cyber Defense*), méthode éditée par le *SANS (SysAdim Audit Network Security) Institute*.

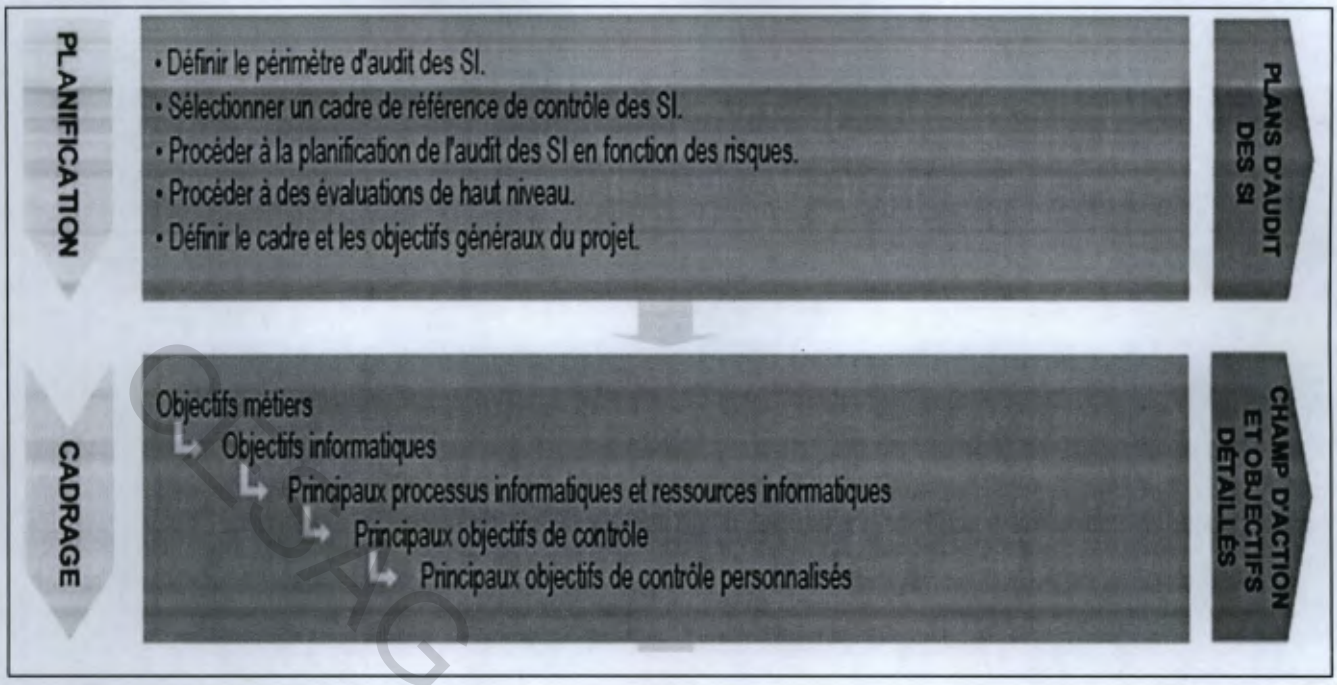
Nous faisons le choix du cadre de référence COBIT pour le cadrage de nôtre étude.

2.2. Le déroulement d'une mission d'audit de sécurité informatique

Selon l'ISACA in AFAI (2008b), pour procéder à un audit, il convient de suivre une méthodologie ou une démarche cohérente. Même si la démarche spécifique peut être propre à chaque entreprise et type de mission, une approche relativement commune est utilisée. Cette approche s'appuie sur trois phases : la planification, le cadrage et l'exécution, cette dernière phase étant divisée en étapes. Les phases et les étapes de ce plan d'action sont présentées dans par la figure 7.

La phase de cadrage définit par l'ISACA est particulière à l'audit informatique / l'audit des systèmes d'information. Cette phase correspond à la préparation de la mission en audit interne. Le choix et l'utilisation d'un cadre de référence révèle ici toute son importance. Pour CLEUET (2008a), « le choix du référentiel COBIT permet à l'auditeur non-informaticien de mener avec efficacité une mission d'audit des systèmes d'informations ».

Figure 7: Plan d'action de l'audit informatique.



Source: ISACA in AFAI (2008b: 19).

Cette figure s'analyse comme suit:

- **La planification**

La définition du périmètre d'audit des SI pour la mission d'audit sert de point de départ de chaque mission d'audit. Pour créer un plan complet, l'auditeur doit combiner la compréhension du périmètre d'audit des SI et la sélection d'un cadre de contrôle des SI approprié, tel que COBIT. La réunion de ces deux éléments permet de planifier la mission d'audit en fonction des risques. Pour définir les objectifs d'audit appropriés, il est d'abord nécessaire de procéder à une évaluation de haut niveau. Le livrable final de cette étape est le plan d'audit des SI, (AFAI : 2008b).

- **Le cadrage**

Selon l'ISACA in AFAI (2008b), le processus de cadrage peut être mis en œuvre de trois façons différentes :

La méthode de cadrage la plus détaillée débute par la définition des objectifs métiers et informatiques pour l'environnement évalué et par l'identification d'un ensemble de ressources et processus informatiques (c'est-à-dire, le périmètre d'audit) requis pour favoriser la réalisation de ces objectifs. L'étendue des objectifs concernés par la mission d'audit des SI

peut être réduite à une granularité inférieure (principaux objectifs de contrôle adaptés à l'entreprise).

Une démarche de cadrage de haut niveau peut débuter par une analyse comparative effectuée, fournissant des recommandations génériques sur les relations entre les objectifs métiers, les objectifs informatiques et les processus informatiques, comme le décrit COBIT.

Cette succession générale d'objectifs et de processus peut servir de base à un cadrage plus détaillé, si l'environnement spécifique évalué l'exige, (CLEUET & al, 2008a).

Une démarche hybride de cadrage combine la méthode de haut niveau et la méthode détaillée. Cette approche débute par la succession générale d'objectifs et de processus mais elle est adaptée et modifiée en fonction de l'environnement spécifique avant de poursuivre le cadrage à un niveau plus détaillé, (AFAI 2008b).

Les livrables finaux de cette étape sont le champ d'intervention et les objectifs des différentes missions d'audit des SI (objectifs présentés dans la section 3 de ce chapitre).

Le point de vue et de la démarche proposé par l'ISACA et celle d'autres auteurs permettra à travers une synthèse de bâtir une démarche référenciée et adaptée aux spécificités de l'entité et du domaine à auditer. Cette démarche pourra servir de guide à service d'audit interne pour la réalisation d'une mission d'assurance de l'un des processus d'un système d'information ou d'un système informatique. Ainsi nous avons choisi un échantillon de cinq auteurs : THORIN (2000), LY (2005), SCHICK (2007), AFAI (2008b), RENARD (2010) dans divers domaines (audit informatique et audit interne) et nous présenterons la synthèse sous la forme du tableau suivant.

Tableau 1: Synthèse des idées de différents auteurs

Auteurs / Phases	Etapes	THORIN (2000 : 137-159)	LY (2005 : 67-83)	SCHICK (2007 : 67-142)	AFAI (2008b : 25-38)	RENARD (2010 : 209-312)
Préparation et Cadrage	Ordre de mission	✓	✓	✓		✓
	Familiarisation	✓	✓	✓	✓	✓
	Identification et évaluation des risques			✓	✓	✓
	Définition des objectifs	✓	✓	✓	✓	✓
Réalisation	Réunion d'ouverture					✓
	Programme de vérification	✓	✓	✓	✓	✓
	Travail sur le terrain	✓	✓	✓	✓	✓
Conclusion	Projet de rapport	✓	✓	✓		✓
	Réunion de clôture	✓	✓	✓		✓
	Rapport définitif	✓	✓	✓	✓	✓
	Suivi des recommandations	✓		✓		✓

Source : Nous même.

Nous analyserons le tableau en indiquant les différentes phases et étapes.

2.2.1. La phase de préparation et de cadrage

Cette phase est encore appelée phase d'étude. Elle se décompose en quatre étapes qui sont l'ordre de mission, la familiarisation, l'identification et l'évaluation des risques et la définition des objectifs ; le cadrage englobe les trois dernières étapes de cette phase.

2.2.1.1. L'ordre de mission

Selon LY (2005), RENARD (2010) et SCHICK (2007), l'ordre de mission est un droit d'accès par lequel la Direction Générale de l'entreprise donne mandat à l'Audit Interne. Cette étape 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. L'ordre de mission rempli deux fonctions qui sont la fonction de mandat et la fonction d'information.

2.2.1.2. La familiarisation

Selon RENARD (2010) et SCHICK (2005), cette étape permet d'avoir une vision d'ensemble de l'organisation auditée et des contrôles mis en place par des lectures, rassemblement d'une documentation, interviews, discussions avec divers responsables. Elle aide à identifier les objectifs de la mission et à identifier les problèmes essentiels concernant le sujet ou 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 celles-ci, (AFAI, 2008b).

Pour THORIN (2000), la familiarisation ou prise de connaissance permet de situer le système informatique dans son contexte, de rencontrer des utilisateurs, d'apprécier le contrôle interne et de se placer dans un repère provisoire des points forts et des points faibles.

C'est lors de cette étape que débute le cadrage que nous avons décrit plus haut au point 2.2.

2.2.1.3. L'identification et l'évaluation des risques

Selon l'AFAI (2008b), SCHICK (2007) et RENARD (2010), cette étape conditionne le dosage et la nature des contrôles à effectuer ensuite. En fonction des risques inhérents identifiés, l'auditeur interne construira son référentiel et son programme de travail. L'identification et l'évaluation des risques se fait à travers le tableau des risques.

2.2.1.4. La définition des objectifs

Cette étape est encore appelée construction du référentiel, rapport d'orientation ou plan de mission. Selon l'AFAI (2008b), RENARD (2010) et SCHICK (2007), la stratégie d'audit doit être définie, le périmètre et les objectifs de la mission d'audit doivent être formalisés. Le rapport d'orientation définit les objectifs généraux, les objectifs spécifiques et le champ d'intervention. 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 de l'ISACA offre la possibilité de choisir parmi ses 34 processus celui ou ceux correspondant à la mission d'audit (voir section 3).

La phase de préparation est la plus importante et un budget temps conséquent doit lui être réservé, elle conditionne la seconde phase.

2.2.2. La phase de réalisation

Selon l'ISACA in AFAI (2008b), la troisième phase du plan d'action d'audit des Systèmes Informatiques est la phase d'exécution ou de réalisations (voir **figure 8**).

C'est la phase des travaux de terrain. Elle est encore appelée phase de vérification. Selon LY (2005 : 72), « c'est une phase primordiale de la mission qui a pour objectif 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 ».

2.2.2.1. La réunion d'ouverture

Selon RENARD (2010), il s'agit d'une réunion qui se tient juste avant le début des travaux de vérification. Cette réunion se tient sur les lieux des travaux, son objet est de présenter le référentiel de l'auditeur. Elle regroupe les auditeurs internes et les responsables audités. Il s'agit de présenter les parties prenantes, de faire des rappels sur l'audit interne, de prendre des rendez-vous et des contacts, de définir les conditions matérielles de la mission et de faire un rappel sur la procédure d'audit.

2.2.2.2. Le programme de vérification

Cette étape est encore appelée programme d'audit ou planning de vérification.
Le programme de travail est établi sur la base du 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, des points à voir, des procédures à rechercher. Les travaux sont décomposés en tâches distinctes (sous-objectifs) afin d'être attribués aux membres de l'équipe, (SCHICK, 2007).

Selon l'AFAI (2008b), le programme d'audit permet d'évaluer les contrôles, de vérifier que ceux-ci sont appliqués et d'évaluer l'efficacité opérationnelle des contrôles. Ces évaluations et tests peuvent aussi porter sur l'efficacité des contrôles. Au cours de cette étape, différents types de vérifications et de tests peuvent être appliqués.

Pour RENARD (2010), le programme de vérification conduit au questionnaire de contrôle interne.

2.2.2.3. Le travail sur le terrain

Le travail sur le terrain consiste à conduire les contrôles prévus dans le programme de vérification.

Elle débute par l'évaluation du contrôle interne. Selon l'AFAI (2008b : 37), « 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 ». Pour RENARD (2010), il permet à l'auditeur de réaliser sur

chacun des points soumis à son jugement critique, une observation complète ; c'est donc 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.

La phase de réalisation d'un audit dans le domaine informatique avec ses particularités est présentée dans la figure ci-après.

Figure 8: La phase de réalisation ou d'exécution.

Source : Nous même, adapté de ISACA in AFAI (2008b : 19).

Pour RENARD (2010), AFAI (2008b), SCHICK (2007), LY (2005) et THORIN (2000), l'auditeur devra ici s'informer et confirmer, inspecter, observer, réexécuter 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. Cette étape conduit à l'élaboration des Feuilles de Révélation et d'Analyse des Problèmes (FRAP) ou des Feuilles de Révélation des Risques (FAR).

Les éléments qui figurent sur les différentes FRAP et FAR permettent, après exploitation, de formuler l'ensemble des conclusions et recommandations, c'est-à-dire rédiger le rapport d'audit.

2.2.3. La phase de conclusion

Cette phase se décompose en quatre étapes qui sont : la rédaction du projet de rapport, la réunion de clôture, la rédaction du rapport définitif et le suivi des recommandations, (RENARD, 2010).

2.2.3.1. Le projet de rapport

Pour RENARD (2010), SCHICK (2007), LY (2005) et THORIN (2000), il s'agit de faire la synthèse des constats et des recommandations qui pourront être discutés avec les audités, cela permet d'affiner le travail et permet une meilleure acceptation du rapport final par les audités. Cela favorise donc une excellente mise en œuvre des recommandations qui seront formulées par l'auditeur.

2.2.3.2. La réunion de clôture

La réunion de clôture se déroule dans les mêmes conditions que la réunion d'ouverture. Il s'agit de l'examen des différents points du projet de rapport.

Selon RENARD (2010), SCHICK (2007), LY (2005) et THORIN (2000), la réunion de clôture ou réunion de validation à pour objet de recueillir l'avis des audités sur les constats, raisonnements et conclusions faits par l'équipe d'audit. Une fois cette étape passée, le rapport définitif pourra être élaboré.

2.2.3.3. Le rapport définitif

Selon l'AFAI (2008b), cette étape rassemble les résultats des étapes précédentes. Le rapport doit communiquer les actions recommandées pour atténuer les faiblesses de contrôles, le comparatif de performance par rapport aux normes et aux meilleures pratiques pour une vue relative des résultats et le niveau de risque associé au processus.

Pour THORIN (2000) et LY (2005), ce rapport doit être concis et il doit être rapidement rédigé et déposé. Il contient des recommandations qui doivent être économiquement réalistes afin d'être mises en œuvre rapidement et à moindre frais pour l'entreprise. L'auditeur

proposera pour ce faire un plan d'action. Il faudra donc procéder à un suivi de ces recommandations.

2.2.3.4. 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 celles-ci afin de mesurer l'efficacité, d'alimenter les dossiers et de parfaire les audits ultérieurs, (RENARD, 2010). Pour SCHICK (2007), l'auditeur interne doit effectuer un suivi du plan d'action adopté, des questionnaires peuvent également être adressés aux prescripteurs de la mission et aux auditeurs internes dans une logique d'amélioration et de démarche qualité.

2.3. Les objectifs de la mission d'audit de sécurité informatique

Le choix comme support de notre étude du référentiel COBIT nous amène à présenter dans cette section les objectifs d'un audit de sécurité basé sur trois des processus décris dans ce référentiel.

2.3.1. Evaluer et gérer les risques informatiques

Ce processus répond à l'exigence d'analyser et de communiquer sur les risques informatiques ainsi que sur l'impact potentiel de ces risques sur les objectifs et les processus métiers. Pour ce faire, le contrôle doit se concentrer sur le développement d'un cadre de référence de gestion des risques, 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. Cet objectif est atteint en s'assurant que la gestion des risques est pleinement intégrée aux processus de management, en interne et en externe et que ceux-ci sont régulièrement appliqués, grâce à une évaluation des risques qui permet de recommander et de communiquer des plans d'action pour réduire ces risques, (AFAI, 2008a). Cet objectif correspond au processus PO 9 du cadre de référence COBIT.

2.3.2. Assurer la sécurité des systèmes

La surveillance de ce processus exige de maintenir l'intégrité de l'information et l'infrastructure technologique et réduire au maximum les conséquences de failles et d'incidents de sécurité. Pour ce faire, l'attention doit être porter sur la définition des politiques, des procédures et des plans de sécurité informatique, surveiller et détecter des vulnérabilités et des incidents de sécurité ainsi que leur résolution et leur compte-rendu. Cet objectif est atteint lorsque la gestion des identités et les autorisations des utilisateurs sont standardisées, que les exigences sont comprises, de même que les vulnérabilités et les menaces de sécurité et que des tests réguliers sont effectués, que la séparation des tâches est effective, (AFAI, 2008a). Cet objectif se réfère au processus DS 5 de COBIT

2.3.3. Evaluer la gestion de l'environnement physique

L'objectif de contrôle (qui correspond au processus DS 12 de COBIT) ici est de protéger les actifs informatiques et les données métiers et de réduire le risque d'interruption de l'activité. Pour cela il faut veiller à la fourniture et à la maintenance d'un environnement physique adapté afin de protéger l'accès aux ressources informatiques d'une détérioration ou d'un vol. Il faut donc mettre en place des mesures de sécurité, sélectionner et gérer les installations, (AFAI, 2008a).

Conclusion

L'audit de sécurité informatique permet à l'entreprise de situer sa maîtrise et sa gestion des risques pesant sur son système informatique. Ceci permettra de se situer par rapport à un référentiel de bonnes pratiques tel que le COBIT ou d'autres que nous avons évoqué dans ce chapitre, de prendre des mesures correctives et de se fixer des objectifs qualitatifs en matière de sécurité informatique. Nous avons mis en relief la démarche d'approche par les risques en audit informatique. Un modèle d'analyse basé sur cette approche peut être envisagé. Le chapitre suivant sera consacré à l'élaboration d'un modèle d'analyse pour la conduite d'une mission d'audit de sécurité informatique par un service d'audit interne.

Chapitre 3. Méthodologie de l'étude

Les chapitres précédents nous ont permis de présenter le système informatique ainsi que l'audit de la sécurité de celui-ci. Nous passerons ainsi à la présentation de notre modèle d'analyse qui nous permettra de mener à bien la partie pratique de cette étude. L'élaboration d'une démarche référentielle d'audit de la sécurité du système informatique est l'objet de ce chapitre ; pour ce faire, le travail sera réparti en deux parties. La première consistera à la présentation de notre démarche référentielle, la seconde mentionnera les outils de collecte et d'analyse des données nécessaires à la conduite d'une mission d'audit de sécurité informatique.

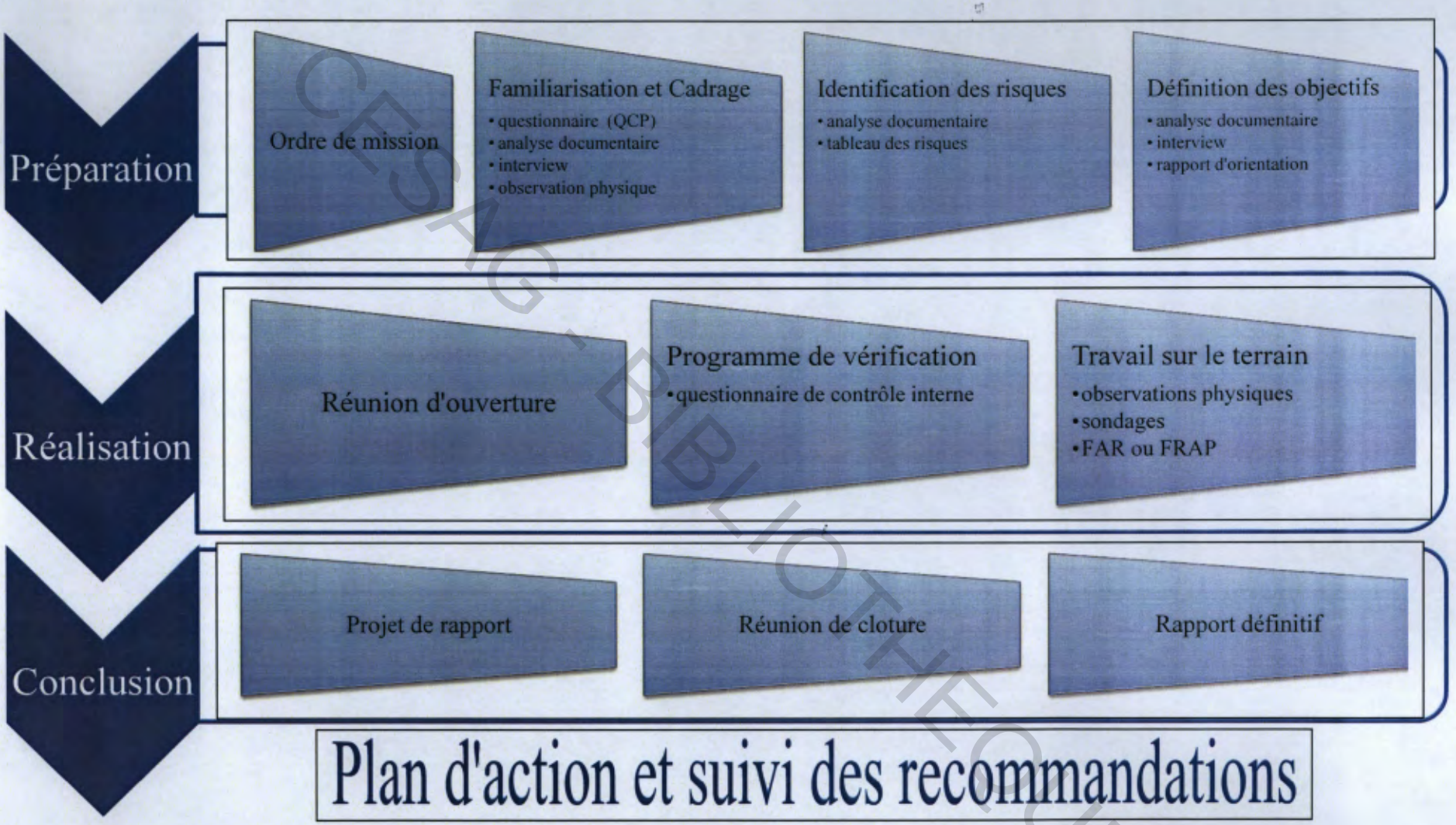
3.1. La démarche référentielle : l'approche par les risques

Le référentiel proposé met en exergue l'approche par les risques. Il se présente comme suit :

- trois phases ;
- dix étapes ;
- huit outils de collecte et d'analyse de données.

La figure 7 ci-après illustre nôtre modèle d'analyse.

Figure 9: Le modèle d'analyse



Source : Nous même.

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

L'accès au maximum d'information sur le processus de sécurité du système informatique étant notre objectif, nous nous adresserons aux responsables intervenant dans ce processus pour la collecte des données.

L'évaluation du dispositif de contrôle interne se réalise grâce à divers outils. Ces outils peuvent être soit des outils de collecte d'information, soit des outils d'analyse des données ou de diagnostic. Ils peuvent être utilisés isolement ou de simultanément.

3.2.1. Les outils de collecte

Nous distinguons ici le questionnaire de prise de connaissance, l'interview, l'observation physique et les sondages.

3.2.1.1. Le questionnaire de prise de connaissance

Comme son nom l'indique, il permet à l'auditeur d'avoir une vision d'ensemble de l'entité et du domaine audité. Il liste les documents à se faire communiquer. D'après RENARD (2010), il permet de bien définir le champ d'application de la mission, de prévoir l'organisation du travail et en mesurer l'importance et enfin il aide à l'élaboration du questionnaire de contrôle interne.

Le questionnaire de prise de connaissance sera utilisé comme une check-list de documents et d'informations à obtenir dès le début de la mission d'audit. Le dépouillement des informations obtenues permettra de faire une présentation de l'entité, de se familiariser avec les procédures en place et d'identifier les principaux protagonistes à la sécurité informatique.

3.2.1.2. L'interview

Cet outil permet de recueillir des informations auprès de l'interlocuteur qui décrira les activités qu'il mène. Il a pour but d'une part de connaitre et comprendre les activités au sein de l'entreprise, et d'autre part d'avoir une idée des procédures de fonctionnement de la sécurité et déterminer les procédures de contrôle qui régissent le domaine audité. Il peut porter sur des questions ouvertes ou sur des questions fermées et n'est possible que dans un milieu où le contact avec le personnel est aisé et possible. Dans le cas d'un besoin

d'approfondissement de certaines informations suite à l'analyse des informations précédemment recueillies, une interview complémentaire peut être demandée.
L'interview sera mise en œuvre pour obtenir des explications détaillées sur des faits et manquements relevés. L'interview permettra aussi de dérouler les points des différents questionnaires auprès des personnes choisies relativement à leurs fonctions ou rôles joués dans le processus de la sécurité du système informatique. Il s'agira principalement d'interviews semi-directifs et d'interviews sous forme de causeries pour tirer le maximum d'informations des différents interlocuteurs grâce à un guide d'entretien prévu à cet effet.

3.2.1.3. L'observation physique

Selon RENARD (2010), l'observation physique est un outil d'application universelle. On peut observer les processus, les biens, les documents ou les comportements. L'observation peut être directe (réalisé par l'auditeur) et conduire à un constat ou indirecte (c'est-à-dire réalisé par une tierce personne). C'est l'outil de validation par excellence lors d'une mission d'audit de sécurité informatique. Il permet de s'assurer de la réalité, de la permanence ou de la conformité des dispositifs de contrôle interne.

Cet outil nous permettra d'identifié et d'observer la mise en application des différents dispositifs de sécurité logique et physique, le contrôle de la sécurité et l'accès aux sites et locaux sensibles, ceci grâce à un guide d'observation et de contrôle. Ce sera le principal outil de validation des dispositifs physiques.

3.2.1.4. Le sondage

L'utilisation du sondage statistique en audit permet à partir d'un échantillon prélevé de façon aléatoire dans une population de référence d'extrapoler à l'ensemble de la population les observations faites sur l'échantillon. Il n'est pas nécessaire d'exiger des niveaux de confiance élevés vue que la taille de l'échantillon ne dépend pas de la taille de la population de base objet de l'étude (RENARD, 2010).
Le sondage statistique sert au dépistage des dysfonctionnements, à l'appréciation de l'ordre de grandeur d'un phénomène ou à l'estimation des attributs dudit phénomène.
Cet outil sera utilisé pour valider les réponses positives du questionnaire de contrôle interne et se faire une idée de l'application des mesures de sécurité. Il servira également lors de la phase

de prise de connaissance à évaluer le niveau d'application des dispositifs de sécurité tel que la distribution de l'antivirus, la présence des onduleurs pour chaque poste etc.

3.2.2. Les outils d'analyse et de diagnostic

Il s'agit de l'analyse documentaire, du tableau des risques, du questionnaire de contrôle interne, des FRAP et des FAR.

3.2.2.1. L'analyse documentaire

Elle consiste à l'exploitation des documents de l'organisation faisant l'objet de l'étude. Il s'agit de consulter les documents obtenus ainsi que les informations collectées afin d'en tirer une connaissance plus approfondie de l'entité audité. C'est donc une bonne technique de rapprochement pour la vérification des données. L'analyse documentaire se fera tout au long de la mission avec un pic d'utilisation lors de la phase de préparation.

3.2.2.2. Le tableau des risques

Il sert à l'identification des risques. Ce tableau découpe l'activité (la fonction ou le processus) objet de l'audit en tâches élémentaires. Il permet d'associer à chaque tâche, les risques susceptibles de se produire si son objectif n'est pas réalisé et les pratiques d'organisation communément admises (POCA) ou dispositif de contrôle interne. En fonction du degré d'affinement de l'analyse, il comportera de 3 à 8 colonnes. C'est à partir de ce tableau que l'auditeur interne précisera les objectifs de sa mission (RENARD, 2010).

Selon SCHICK (2007) le tableau des risques se conçoit en deux phases :

- Le tableau des risques « référentiel » qui comme son nom l'indique sera le référentiel convenu entre les parties prenantes pour évaluer la maîtrise des risques.
- Le tableau des risques « forces et faiblesses apparentes » qui permet de faire un état des lieux des forces et faiblesses réelles ou potentielles de l'entité ou du domaine audité afin d'orienter les travaux détaillés.

Le tableau des risques est le point de départ du questionnaire de contrôle interne. Le découpage en objectif ou tâches élémentaires sera inspiré de COBIT (PO 9, DS 5 et DS 12).

3.2.2.3. Le questionnaire de contrôle interne (QCI)

D'après RENARD (2010), le QCI est issue du même découpage en tache élémentaire que le tableau des risques.

Cet outil est un questionnaire préétabli pour chaque fonction et chacun des objectifs de l'entreprise ; il liste également les principaux points de contrôle interne qu'il est généralement nécessaire de prévoir. Le questionnaire permet de relever les mesures du contrôle interne existant, de constater les lacunes et les points forts du processus de sécurité informatique mis en place. Les questions sont de types « fermées » et le questionnaire est conçu de sorte qu'un « non » équivaut à une lacune ou une faiblesse. Un « oui » sera par contre considéré comme une force et devra ensuite être validé soit par sondage, soit par observation physique. Il sera construit à partir des processus de COBIT que nous avons décrit dans la dernière section du chapitre 3.

3.2.2.4. La FRAP et la FAR

Ce sont les outils d'analyse des problèmes rencontrés (FRAP) ou des risques identifiés (FAR) lors du déroulement de l'audit. Les éléments de la FRAP sont étagés en cinq lignes (problèmes ; faits ; causes ; conséquences ; solutions), ceux de la FAR sont également présentés de la même manière (types de risques identifiés ; faits constatés ; causes explicatives ; conséquences réelles ou potentielles ; recommandations). Elles servent pour l'ossature du rapport qui est élaboré à partir des "problèmes" figurant sur les FRAP ou des risques figurant sur les FAR; l'ossature du rapport est en quelque sorte un rassemblement des FRAP/FAR d'une manière cohérente et selon une logique de hiérarchisation des problèmes rencontrés/risques recensés, assorti d'un commentaire descriptif.

Conclusion

Ce chapitre nous a permis de présenter la démarche référentielle que nous utiliserons lors de la phase pratique. Il a également permis de présenter les différents outils qui nous serons nécessaires pour la réalisation de l'audit de la sécurité du système informatique à l'ASECNA Cameroun. Il marque l'achèvement de la revue de littérature et le passage à la partie pratique de notre étude.

Conclusion de la première partie

La revue de la littérature a permis de présenter le système informatique ainsi que l'audit de la sécurité du système informatique, et notre démarche référentielle.

L'inhérence des risques informatiques nécessite de leurs accorder une attention particulière. Les entreprises qui évoluent dans le secteur aéronautique sont concernées par cette assertion ; le système informatique de la Représentation ASECNA du Cameroun est particulièrement concerné par ces risques.

La mission de l'ASECNA, les mutations technologiques en cours et la gouvernance du système informatique posent des exigences de performance. Cela passe par la connaissance du niveau de sécurité actuelle notamment celle du système informatique. Le support le plus adéquat à cette mesure est de procéder à l'audit de la sécurité du système informatique car, il attirera l'attention des dirigeants et des protagonistes du processus sur le niveau de sécurité et les menaces qui pèsent sur la performance de l'Agence et permettra de définir des axes d'amélioration de ce processus hautement stratégique.

DEUXIEME PARTIE : CADRE PRATIQUE

Introduction :

La mondialisation oblige les entreprises africaines à être plus performante que par le passé. Pour ce faire, elles procèdent de plus en plus à l'informatisation de leurs processus. Cela a pour conséquent de les exposer à de nouveaux risques pour leurs activités. Un état des lieux doit par conséquence être effectué afin de situer la maîtrise des risques de cet outil et évaluer les mesures de sécurité prises pour veiller sur ces actifs.

La sécurité informatique nécessite une véritable prise de conscience et la mise en place de mesures techniques et organisationnelles adéquates.

L'activité à laquelle s'adonne l'ASECNA est l'objet d'importants risques. Son système informatique n'y échappe pas. Il convient donc d'effectuer un audit de la sécurité du système informatique. Elle constituera donc l'objet de cette seconde partie.

Nous présenterons dans cette partie la Représentation de l'ASECNA au Cameroun et les services impliqués dans le processus de sécurité du système informatique, nous ferons ensuite une présentation de l'état des lieux dudit processus et de nos travaux d'audit et nous achèverons cette partie par la présentation des résultats de nôtre étude.

Chapitre 4. La Représentation de l'ASECNA au Cameroun

L'Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar (ASECNA) est l'un des plus beaux exemples de coopération Nord-Sud et Sud-Sud ainsi que l'organe de l'unité Africaine par excellence en matière d'aviation civile. Il paraît opportun de présenter la Représentation du Cameroun structure qui nous a accueilli pour nôtre stage ainsi que le système informatique, objet de notre étude.

4.1. Brève présentation de l'ASECNA

Cette section nous permettra de faire l'historique d'ASECNA, de présenter ses missions, son organisation (voir annexe 1) ainsi que ses activités afin de mieux comprendre le rôle de la Représentation de l'ASECNA au Cameroun.

4.1.1. L'historique

L'ASECNA a été créée à Saint-Louis du Sénégal le 12 décembre 1959. Établissement public à caractère multinational, elle rassemble 18 Etats membres dont 15 Etats d'Afrique de l'Ouest et du Centre[8] (dont la Guinée Bissau depuis janvier 2006), Madagascar, les Comores (depuis 2004) et la France.

4.1.2. La mission et les activités

L'agence à comme mission essentielle : la sécurité de la navigation aérienne.

Conformément à la Convention de Dakar de 1974, l'ASECNA exerce à titre principal les activités communautaires prévues en son Article 2 et, à titre subsidiaire, gère les activités dites nationales au bénéfice des Etats membres pris individuellement (Articles 10 et 12) ainsi que des Etats et organismes tiers (Articles 11 et 12).

[8] Bénin - Burkina Faso - Cameroun - Centrafrique - Comores - Congo - Côte d'Ivoire - France - Gabon – Guinée Bissau - Guinée Equatoriale – Madagascar - Mali - Mauritanie - Niger - Sénégal - Tchad - Togo.

4.2. La Représentation ASECNA du Cameroun

Dans chaque État membre (hormis la France), la mission et les activités de l'Agence sont assurées par une Représentation ayant à sa tête un Représentant nommé par le Directeur Général en accord avec le Ministre de tutelle concerné; cet agent est responsable des activités de l'Agence dans son Etat d'affectation.

La Représentation du Cameroun à son siège à l'aéroport international de Douala. Les bâtiments qui l'abritent sont une concession de l'Etat camerounais par l'entremise de l'entreprise « Aéroports Du Cameroun » (ADC SA) et ceci pour les deux autres aéroports internationaux du Cameroun (Yaoundé-Nsimalen et Garoua) et la station météorologique de Ngaoundéré.
L'effectif de la Représentation au 19 octobre 2010 est de 410 agents[9].

4.2.1. L'organisation administrative

La Représentation est organisée comme suit (voir annexe 2):

- le cabinet du Représentant ;
- le service exploitation de la navigation aérienne ;
- le service exploitation de la météorologie ;
- le service infrastructures radioélectriques ;
- le service infrastructures génie civil ;
- le service administratif et financier ;
- la paierie.

L'organigramme détaillé de la Représentation est présenté en annexe 3.

[9] Source : Bureau Solde.

4.2.2. Les activités de l'ASECNA-Cameroun

La Représentation ASECNA du Cameroun a la charge d'un espace aérien étendu sur 475 442 km² (superficie du Cameroun) couverte par le centre d'information en vol de N'Djamena.

Elle supervise à ce titre:

- 03 tours de contrôle ;
- 03 aéroports internationaux (Douala, Yaoundé-Nsimalen et Garoua) ;
- la station radio de Manfé ;
- la station météorologique de Ngaoundéré.

Elle y assure :

- le contrôle de la circulation aérienne ;
- le guidage des avions ;
- la transmission des messages techniques et de trafic ;
- l'information de vol ;
- le recueil des données ;
- la prévision et la transmission des informations météorologiques.

Ces prestations couvrent aussi bien la circulation en route que l'approche et l'atterrissage.
La Représentation assure les aides terminales sur les O3 aéroports internationaux, c'est-à-dire :

- le contrôle d'aérodrome ;
- le contrôle d'approche ;
- le guidage du roulement des aéronefs au sol ;
- l'aide radio et visuelle à l'approche et à l'atterrissage ;
- les transmissions radio ;
- les prévisions météorologiques ;
- le bureau de piste et d'information aéronautique et ;
- les services de sécurité et lutte contre l'incendie.

A ce titre l'ASECNA-Cameroun assure la maintenance de l'ensemble des installations nécessaires à la mise en œuvre de ces différentes prestations (mais non des pistes).

Outre ses activités qui sont d'assurer les missions de l'Agence au Cameroun et de contribuer à l'élaboration et la mise en œuvre des décisions prises par la Direction Générale, la Représentation à également pour rôle de percevoir les redevances de route (6 milliards de franc CFA en 2009) pour les services fournis aux usagers (compagnies aériennes).

Au Cameroun, l'ASECNA n'intervient pas dans la gestion des activités nationales. La Représentation assure l'application de l'article 2 de la convention de Dakar.

4.2.3. Le Cabinet du Représentant

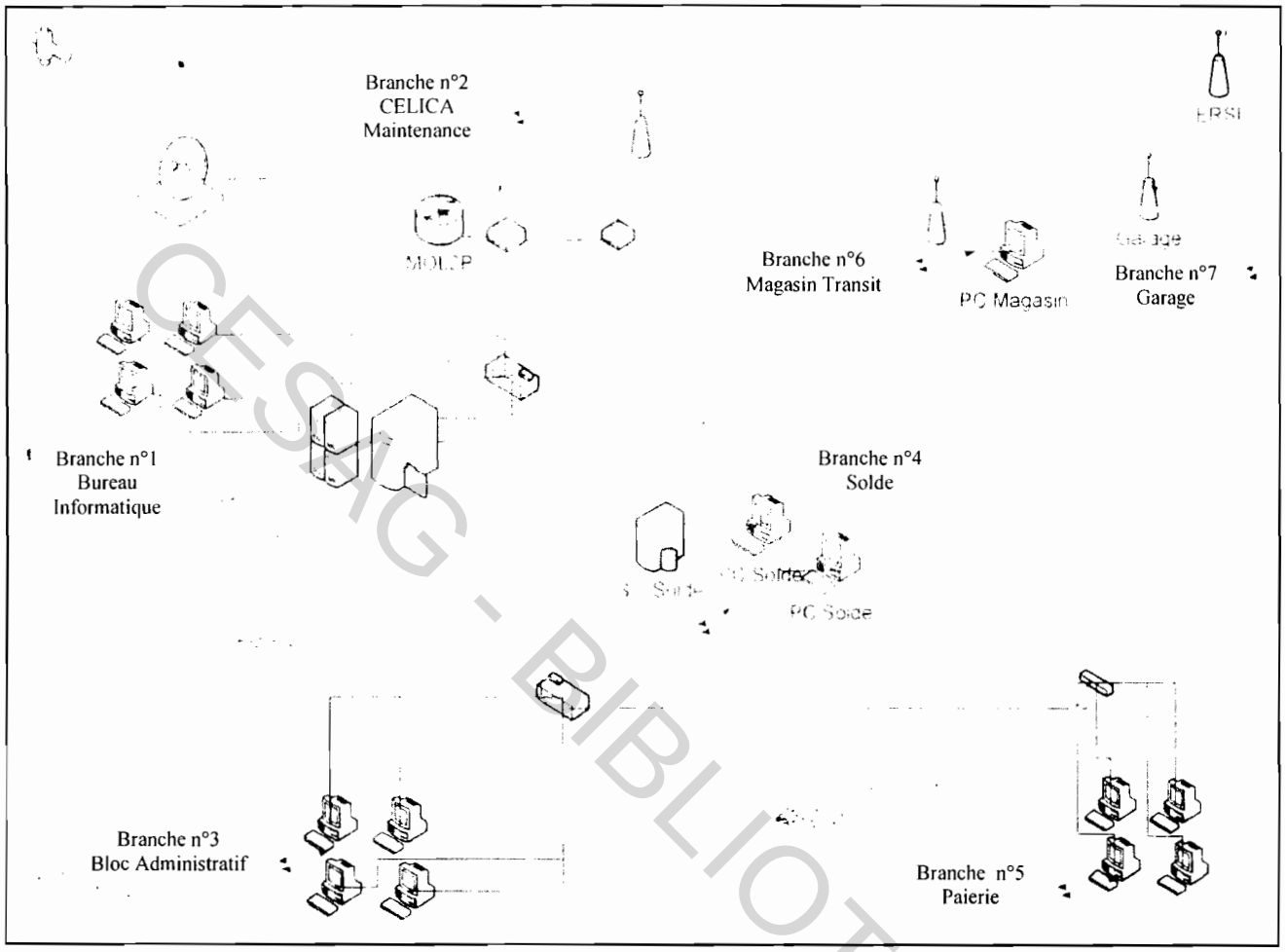
Il est composé du :

- Secrétariat ;
- Délégué du Représentant à Garoua ;
- Délégué du Représentant à Yaoundé ;
- Bureau Contrôle de gestion ;
- Bureau Informatique.

Nous avons été affecté au cabinet du Représentant durant notre séjour à la Représentation ASECNA Cameroun.

4.3. Le système informatique de la Représentation

Figure 10: Répartition en branche du système informatique



Source : ASECNA-Cameroun, obtenu du Bureau Informatique le 17 septembre 2010.

Le système informatique de la Représentation est reparti en sept branches qui sont :

- branche n°1 : le bureau informatique qui est également la salle des serveurs ;
- branche n°2 : CELICA / Maintenance ;
- branche n°3 : bloc administratif ;
- branche n°4 : solde ;
- branche n°5 : paierie ;
- branche n°6 : magasin / transit ;
- branche n°7 : garage.

Tableau 2: La répartition du matériel bureautique par service

Unité utilisatrice	Ecran+unité centrale	Imprimante
Cabinet du Représentant à Douala	10	5
Exploitation de la navigation aérienne	21	15
Exploitation de la météo	18	11
Infrastructures radio électriques	12	8
Paierie	8	4
SAF	10	9
Infrastructures de génie civil	2	1
Délégation de Yaoundé	30	14
Ecole Régionale de Sécurité Incendie (ERSI)	41	21
Total	**152**	**88**

Source : Nous même, à partir de l'état d'inventaire au 31 décembre 2009.

Ce système se compose de deux réseaux distincts :

- le réseau local constitué par toutes les branches excepté la branche n°2,
- le réseau opérationnel ou réseau des télécommunications (spécifique à la navigation aérienne).

4.3.1. Le réseau local

Ce réseau est géré par le bureau informatique. Les serveurs de ce réseau sont entreposés dans la salle informatique, située au premier étage du bloc technique. Cette salle sert également de bureau au Chef du bureau informatique. Elle héberge également la baie qui abrite l'essentiel des routeurs et des commutateurs du réseau.

Des applications centralisées sont distribuées à partir de ces serveurs. Il s'agit de COGEST qui traite les opérations de comptabilité, DELTA-Paie qui gère la solde, TRAFIC qui est le logiciel de facturation des redevances de route. Les applications ISAKAS, FREDA et PAIE ne sont pas encore en exploitation car la Baie HP STOKAGE 6 Server abritant les serveurs sur lesquels ces applications sont installées n'est pas encore opérationnelles à ce jour.

Tableau 3: Les serveurs de la salle informatique

Modèle	Utilisation / Application
UNISYS	COGEST, TRAFIC
HP ML 370 Windows Advanced server	DELTA-Paie
HP DC 5700 Windows server 2003	PROXY
HP DC 5700 Windows server 2003	DHCP DNS
Baie HP STOKAGE 6 server	ISAKAS, FREDA, PAIE

Source : Nous même.

4.3.2. Le réseau opérationnel

Ce réseau est sous la responsabilité du bureau réseau et système informatique. Il est exploité depuis le CAT (Centre Automatique de Transmission) situé au premier étage du bloc technique (aile opposée au bureau informatique).

Il est le support des applications MESSIR-AFTN[10] qui gère les appareils de radionavigation et génère les messages aéronautiques et MESSIR-COMM[11] qui gère les appareils de prévision météo ainsi que les messages météorologiques. Ces deux applications sont installées chacune sur deux serveurs distincts, un pilote et un secours. Ces applications sont développées par la société COROBOR Systèmes qui en assure la maintenance.

Ces quatre serveurs ainsi que les modules de commandes des autres appareils de télécommunication et de radio guidage sont hébergés dans la salle technique située au sixième étage du bâtiment technique.

Les différents appareils de la salle technique et leurs utilisations sont détaillés ci-après :

- une baie HP contenant les 4 serveurs (deux pour le logiciel MESSIR-AFTN et deux pour le logiciel MESSIR-COMM), un Swift (distributeur local) et un onduleur ;
- un tableau général basse-tension (TGBT) ;
- un répartiteur pour les communications VHF, le téléphone et les messages voix ;
- un autocommutateur pour le téléphone de sécurité reliant les pompiers(SSLI), la tour de contrôle, la prévision météo, le bureau de piste et le centre de contrôle en route ;

[10] Aeronautical Fixed Telecommunications Network
[11] Organisation Météorologique Mondiale

- un autocommutateur réseau dédié à la sécurité et au commandement à priorité voix et données qui relie KANO, BANGUI, BRAZZAVILLE et LIBREVILLE ;
- quatre multiplexeurs à priorité voix ;
- douze modems ;
- une baie VHF (émetteurs/récepteurs) ;
- télécommande des équipements de radionavigation (approche et atterrissage) :
    - DME[12] : donne la distance entre l'avion et la piste.
    - Localizer : donne l'axe de la piste.
    - ILS[13] : système d'aide à l'atterrissage aux instruments.
    - Glide-path : donne la pente de descente.
    - VOR DME[14] de route qui donne le radian et la distance en vol.
- une horloge centrale donnant l'heure à tous les postes en temps universel ;
- cinq émetteurs/récepteurs en HF (haute fréquence) ;
- une interface d'arrivée pour la fibre optique ;
- deux PC enregistreurs dont un principal et un secours (DVD et disques durs) qui enregistrent toutes les conversations entre les différents acteurs de la navigation aérienne ;
- un compresseur à air pour souffler la poussière sur les appareils cités plus haut.

Conclusion

Nous avons effectué une présentation sommaire de l'ASECNA, de la Représentation de l'ASECNA du Cameroun et des principaux éléments constitutifs du système informatique.
Cette présentation achevée, nous ferons une description du processus de sécurité et des services concourant à ce processus et nous présenterons le déroulement de nos travaux d'audit.

[12] DME : Distance Measuring Equipement
[13] ILS : Instrument Landing System
[14] VOR : Very High Frequency Omnidirectionnal Range

Chapitre 5. Description des dispositifs de la sécurité informatique

Nous allons procéder à une présentation des unités concernées par la sécurité informatique, puis une présentation sera faite suivant l'ordre des objectifs définis au début de notre étude. Le même découpage en sous-processus sera retenu pour l'identification et l'évaluation des risques et le déroulement de nos travaux conformément à nôtre modèle d'analyse.

5.1. Les différents acteurs de la sécurité du système informatique

Il s'agit des services, bureaux ou personnes impliqués dans le processus objet de notre étude.

5.1.1. Le bureau informatique

Ce bureau est animé par le chef de bureau informatique et par l'agent informatique.

5.1.1.1. Le chef du bureau informatique

Les attributions principales du chef du bureau informatique sont de :

- veiller au bon fonctionnement du système informatique de la Représentation ;
- veiller à la maintenance de l'ensemble du parc informatique ;
- veiller à la sécurité des données.

Le titulaire de poste doit posséder un diplôme d'ingénieur en informatique (Bac+5) ou équivalent, avec cinq ans années d'expérience.

Ce poste est occupé par l'ancien agent informatique dont le profil n'est pas en adéquation avec les exigences de la fiche de poste du Chef du Bureau Informatique.

5.1.1.2. L'agent informatique

Il a pour rôle :

- d'assurer le bon fonctionnement des serveurs, bases de données, des systèmes et du réseau ;
- d'assister les utilisateurs dans la maîtrise de l'outil informatique.

C'est cet agent qui est en charge de la gestion de la sécurité (antivirus et systèmes d'application) et de la surveillance de l'environnement informatique.
Le titulaire de ce poste doit être titulaire d'un Diplôme Universitaire de Technologies (DUT) ou d'un Brevet de Technicien Supérieur en Informatique (BTS) ou équivalent.

Ce poste est vacant à la Représentation. Toutefois, ces tâches sont assumées en partie par un ex-stagiaire du bureau informatique ne disposant pas de contrat de travail

.

5.1.2. Le chef du bureau exploitation des télécommunications

Il veille au bon fonctionnement des services de télécommunication (service fixe aéronautique, service mobile aéronautique, service de radionavigation aéronautique, service de surveillance et de tous les services faisant appel aux télécommunications. Ses tâches sont de :

- configurer et administrer les systèmes sous sa responsabilité (réseau opérationnel) ;
- s'assurer de la gestion et la protection du spectre de fréquence aéronautiques contre les brouillages et l'utilisation par des entités non aéronautiques.

5.1.3. Le chef bureau radio

Son rôle est de :

- veiller à la sécurité de la salle technique ;
- procéder à la sauvegarde et à l'archivage des données et de toutes les communications sur la plate forme ;
- assurer la disponibilité heure 24 des équipements sous sa responsabilité.

5.1.4. Le service infrastructures de génie civil

Le chef de service a pour tâche de suivre l'exécution des contrats locaux de services et de maintenance, d'assurer la gestion du patrimoine conformément à la réglementation en vigueur (immatriculation, inventaire, reforme…).

Le chef du bureau bâtiments, pistes et voiries a pour tâche le suivi des biens meubles et immeubles et l'inventaire physique. Il identifie les biens meubles et matériels à soumettre à la reforme.

5.1.5. La section sauvetage et lutte contre l'incendie

La section a pour mission de :

- s'assurer du maintien en bon état de fonctionnement des moyens de sauvetage et de lutte contre l'incendie ;
- surveiller et préserver le patrimoine destiné au sauvetage et à la lutte contre l'incendie sur l'ensemble de la plate-forme ;
- organiser la maintenance préventive, l'entretien et la réparation du matériel de lutte contre l'incendie et en suivre la disponibilité ainsi que celle des points d'eau.

5.1.6. La centrale électrique

Elle a pour rôle de :

- s'assurer de la disponibilité de l'énergie électrique en heure 24 pour les installations techniques de la plate-forme ;
- veiller à l'entretien et à l'installation du matériel électrique ;
- s'assurer du bon fonctionnement des unités de secours électrique.

5.1.7. Le bureau contrôle de gestion

Il a pour rôle de :

- élaborer et piloter les outils de contrôle interne ;
- veiller à la mise en œuvre et au respect de l'organigramme de la Représentation ;
- veiller au respect des normes et standards en vigueur à l'Agence.

Ce poste est vacant à la Représentation.

Nous avons effectué une présentation des unités concourant au processus de sécurité informatique à la Représentation. Nous allons à présent décrire ce processus tel que nous l'avons identifié.

5.2. Les dispositifs de sécurité informatique à ASECNA Cameroun

Comme présenté dans la section précédente, ce processus implique plusieurs services. Il n'existe pas de manuel de procédure décrivant expressément les mesures à prendre pour sécuriser le système que nous avons étudié dans son ensemble. Toutefois en nous basant sur l'exploitation des fiches de postes, les interviews et nos observations sur le terrain, nous avons pu identifier les mesures de sécurité qui seront décrites dans cette section. Le réseau opérationnel est sécurisé suivant des directives de l'OACI dont la plupart sont confidentielles.

5.2.1. La gestion et l'évaluation des risques

Nous n'avons pas identifié de processus de gestion et d'évaluation des risques informatiques à la Représentation. Ce processus est en place au siège à Dakar d'après le chef bureau informatique et le chef section de la navigation aérienne.

5.2.2. La sécurité du système

Il s'agit ici des mesures prises pour assurer la sécurité logique et la protection des données.

5.2.2.1. Gestion des identités et des comptes d'utilisateurs

Les clients du réseau local utilisent des sessions administrateurs, sans mot de passe. Un login et un mot de passe sont exigés avant le lancement des applications DELTA-Paie, COGEST et TRAFFIC.

Les clients du réseau opérationnel se connecte à leurs applications via deux profils : administrateur (qui permet la modification et l'envoi des messages) et menu (qui ne permet que la consultation) ; l'accès au profil administrateur est verrouillé par un mot de passe.

5.2.2.2. Prévention, détection, neutralisation des logiciels malveillants

La Représentation dispose d'une licence commerciale pour le logiciel anti-virus KASPERSKY Internet Security (version 6.0.837) avec mises à jour, valable jusqu'au 10 novembre 2012 pour 746 postes.

Les postes du réseau opérationnel ont leurs lecteurs de CD/DVD et de clef USB désactivés. Du fait du non accès à la connexion internet pour d'éventuelles mises à jour, les antivirus ne sont pas installés. Néanmoins des antivirus sont installés sur les quatre serveurs.

5.2.2.3. Sécurité des réseaux, échange des données sensibles

Pour le réseau local, un serveur PROXY est en place. C'est ce serveur qui reçoit la connexion internet. L'antivirus dispose d'un pare-feu intégré.

Les postes clients du réseau opérationnel ne sont pas connectés à internet. Des antivirus sont néanmoins installés sur les serveurs mais les mises à jour ne sont pas faites (pas de connection à internet). Ce réseau est propre à l'OACI. Un spectre de fréquence propre à l'aviation civile est attribué par l'Agence de Régulation des Télécommunications du Cameroun.

5.2.2.4. La sauvegarde et l'archivage des données

Pour le réseau non-opérationnel, les fichiers sont sauvegardés tous les jours à 21h sur deux jeux de DVD et un disque dur externe ; ces fichiers sont ensuite archivés et un jeu est conservé au sein du bureau du Représentant et le second jeu est transmis au siège à Dakar.

Pour le réseau opérationnel, les deux enregistreurs situés dans la salle technique enregistrent toutes les transmissions simultanément sur deux DVD et deux disques durs. Ces enregistrements sont conservés pendant trois mois avant une réutilisation des supports d'enregistrement conformément à la réglementation de l'OACI. Ces supports sont stockés entre les écrans des enregistreurs, il n'y pas d'armoire ou de coffre prévu à cet effet.

5.2.3. La gestion de l'environnement physique

Nous allons décrire dans cette sous-section les mesures de sécurité physique que nous avons identifiées durant la phase de prise de connaissance.

5.2.3.1. Sélection du site et agencement

La salle informatique et la salle de maintenance sont situées dans le bloc technique. C'est le bâtiment de la tour de contrôle de l'aéroport de Douala. Il est composé de sept étages plus la vigie à son sommet. Ces deux salles occupent l'aile gauche de cet étage. Des barreaux en métal protègent la fenêtre extérieure de la salle des serveurs. Les murs intérieurs sont des cloisons en contre-plaqué. Une large baie vitrée donne une vue complète de la salle des serveurs depuis le couloir. Une porte fermée à clé limite l'accès à cette salle.

La salle informatique abrite tous les serveurs du réseau local, excepté le serveur de la solde qui est disposé dans un bureau situé au premier étage du bloc administratif ; les deux blocs de bâtiments sont distants de 300 mètres environ et ils sont séparés par une clôture en grillage barbelé.

La salle technique est située au sixième étage du même bâtiment. Une porte en bois avec une vitre de 1,70m X 0,50m avec vue sur les équipements l'isole de la cage d'escaliers. Les murs à l'intérieur de ce bloc sont des cloisons en contre-plaqué.

5.2.3.2. Mesures de sécurité physique / Accès physique

Une société privée de gardiennage sous contrat assure la protection des locaux. Deux agents sont postés à l'entrée du bloc administratif et un troisième veille sur l'entrée du bloc technique. Ces gents disposent de registres où ils doivent noter les noms des personnes qui accèdent dans le bâtiment, le service de destination, l'heure d'arrivée et de départ.

Les agents de toutes les organisations travaillant sur la plate forme doivent porter des badges pour faciliter leur identification.

Les composants du système informatique disposent chacun d'un numéro d'identification et des inventaires réguliers sont effectués pour le gros matériel. Nous avons été témoin d'un inventaire à la salle technique le 21/09/2010.

Les câbles réseaux se trouvant dans les bureaux sont abrités dans des goulottes de câblage et des gaines en PVC[15]. Les câbles électriques et les câbles réseaux reliant les différents bâtiments sont enterrés.

[15] Matière plastique constituée de polychlorure de vinyle

Dans le bâtiment technique les câbles passent par des conduits aménagés dans la structure des murs (colonnes montantes), des portes d'armoires qui ferment à clé permettent d'y accéder. Les planchers sont creux et amovibles afin de permettre le passage et l'installation des réseaux de câblage.

5.2.3.3. Protection contre les risques liés à l'environnement

Un prestataire de service assure le nettoyage des locaux de la Représentation.

Le bureau informatique assure la maintenance préventive de l'ensemble des PC ainsi que des serveurs du réseau local.

Les appareils et les serveurs situés dans la salle technique sont régulièrement soufflés grâce au compresseur disposés dans cette salle. De plus cette salle dispose de trois climatiseurs Split muraux de forte puissance qui refroidissent en permanence les équipements. La température dans cette salle ne doit pas être supérieure à 30° Celsius ; toutefois il n'existe pas d'instrument de mesure de la température et de l'hygrométrie.

La salle informatique est également réfrigérée à l'aide d'un climatiseur de forte puissance.

5.2.3.4. Gestion des installations matérielles

Des bouches d'incendies sont disponibles à chaque étage du bâtiment, ainsi que des extincteurs (révisés le 29/09/2010) dans les couloirs et certaines salles. Un téléphone de secours relie la salle technique à la caserne des pompiers de l'aéroport.

La plateforme dispose d'une centrale électrique alimentée par deux lignes d'électricité de moyenne tension. L'arrivée d'électricité passe par des onduleurs et des batteries. La centrale dispose également de quatre générateurs électriques de 250 KVA[16] chacun. Ces générateurs fonctionnent en tandem (un principal et un secours). En cas de rupture de courant électrique, le premier tandem assure la fourniture d'électricité au bloc technique et le second le fait pour les autres installations de l'aéroport. De plus ces générateurs sont équipés de batteries et d'onduleurs avec une autonomie de huit heures, le relais en cas de coupure d'électricité se fait automatiquement.

[16] Kilo volt Ampère

Le bloc administratif est également équipé d'un groupe électrogène de 220 KVA sans reprise automatique. Des groupes électrogènes mobiles disponibles peuvent également être déployés sur les installations radio et météo périphériques.

La salle technique et la salle informatique disposent chacune de deux arrivées de courant séparées qui passent par des tableaux électriques avant alimentation des équipements. Les serveurs de ces salles sont équipés d'onduleurs : un onduleur pour les serveurs de la salle technique et deux onduleurs pour tous les serveurs de la salle informatique.

Conclusion

Ce chapitre a permis de se faire une idée de la sécurité informatique à la Représentation ASECNA du Cameroun à travers la présentation des principaux intervenants du processus et la description des mesures de sécurité existantes, permettant ainsi d'avoir une bonne idée de l'état des lieux. Cette description achevée, nous allons présenter le déroulement de nos travaux d'audit ainsi que les résultats obtenus. C'est l'objet du prochain et dernier chapitre de notre étude.

Chapitre 6. Présentation des travaux et des résultats de l'étude

L'ultime chapitre de cette étude est l'occasion de faire une présentation du déroulement de nos travaux d'audit et d'effectuer une synthèse des forces et des faiblesses constatées. Chaque faiblesse et/ou chaque force donne lieu à des recommandations qui devraient permettre de corriger les faiblesses et de renforcer les dispositifs existants. La mise en œuvre desdites recommandations nécessite pour cela qu'un plan d'action soit mis en œuvre pour assurer une prise en compte efficace et méthodique des solutions retenues.

6.1. Le déroulement de la mission d'audit

Cette narration reprendra les points les plus significatifs de notre méthodologie ainsi que les outils retenus. Il est donc question ici de la mise en œuvre de notre modèle d'analyse.

6.1.1. La préparation et le cadrage de la mission

Cette phase a débuté avec la présentation d'une proposition d'ordre de mission qui définit les objectifs généraux de la mission (voir annexe 4).
Le questionnaire de prise de connaissance de l'entité (voir figure ci-après) a permis de nous familiariser avec l'environnement interne et externe de la Représentation ; en l'absence d'une unité d'audit interne, cette phase a été particulièrement longue. Elle a permis d'effectuer la présentation de l'entité (chapitre 3), et d'identifier les services impliqués dans le processus que nous avons audité (section 1 et section 2 du chapitre 5).

Tableau 4: Questionnaire de prise de connaissance.

QUESTIONNAIRE DE PRISE DE CONNAISSANCE		
Objectif : Avoir une vision d'ensemble de l'entité, du système informatique et de la sécurité informatique.	**Réf.**	**OBSERVATIONS**
Se faire présenter l'entité	**A**	
Missions, activités, produits, organisation, statuts.	AA	Ok
Historique	AB	Ok
Appartenance à un groupe	AC	Ok
Obtenir l'organigramme général	AD	Ok
Prendre connaissance du système informatique	**B**	
L'organisation générale	BA	Ok
Les missions, l'effectif.	BC	Ok
Les méthodes de travail	BD	Voir fiches de postes et entretiens
Examiner le manuel de procédures	BE	Pas de manuel
Visite des principaux locaux	BF	Salle informatique, salle technique
Documents à obtenir	**C**	
Manuels de procédures	CA	Non, voir Réf. BE
Statuts	CB	Voir site internet
Rapport annuel / Rapport d'activité	CC	Rapport d'activité 2008
Etat récapitulatif du matériel informatique	CD	OK
Organigramme détaillé	CE	partiel, à dessiner et à compléter
Fiches de postes des différents protagonistes	CF	Incomplètes, manque Service ESIR
Schéma descriptif du système	CG	OK

Source : Source non spécifiée, adapté par Nous même.

L'étape de familiarisation a également été l'occasion de faire connaissance avec le personnel et les principaux responsables, grâce à des interviews visant à comprendre le fonctionnement des différents services de la Représentation (voir annexe 5) et une visite des locaux dont l'objectif était de localiser la salle technique et la salle informatique.

Un entretien avec le Chef de bureau informatique a été sollicité afin de se faire une première idée sur les dispositifs de sécurité mis en place, les réponses sont présentées ci-après.

Tableau 5: Identification et évaluation des dispositifs de sécurité informatique.

Section	Oui / Force	Non / Faiblesse
Sécurité physique		
Infrastructures physique		
Qualité des murs et des fenêtres		✓
Détection d'intrusion (alarmes, gardiennage)		✓
Protection incendie		
Dispositif détection/extinction		✓
Protection électrique		
Un onduleur avec batterie est en place sur chaque serveur	✓	
Climatisation	✓	
Contrôle des accès		
Contrôle des accès (jour/nuit)		✓
Conditions de fonctionnement		
Hygiène – propreté	✓	
Rangement des locaux informatiques		✓
Proximité d'autres risques		✓
Maintenance du matériel	✓	
Des contrats existent pour les serveurs	✓	
Plan de secours informatiques		
Existence et documentation	✓	
Tests de sécurité		✓
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 réguliers 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		✓
Procédure de sauvegarde		
Stockage externe	✓	
Contrôle de relecture	✓	
Sauvegarde des postes individuels (PC)		✓

Source : Nous même, adapté de CLEUET & al (2008a :58-59)

Tableau 6: Evaluation des dispositifs de sauvegarde.

Questions	Réponses
En fonction du contexte et de la configuration informatique, combien de jours sont nécessaires pour remplacer celle-ci suite à un vol ou à un incendie ?	1 semaine au plus
Combien de jours d'arrêt informatique peut-on tolérer ?	1 semaine au plus
Sait-on travailler en mode « manuel » en se référant à des procédures dégradées ?	Non

Niveau de risque en cas de sinistre				
Application	**Conséquences d'un arrêt (jours)**			**Mesures dégradées**
	Faible	**importante**	**vitale**	
COGEST (comptabilité)			✓	Non
DELTA-Paie (solde)			✓	Non
Achat		✓		Non
TRAFIC (facturation)			✓	Non
MESSIR-ATN			✓	Non
MESSIR-COMM			✓	Non

Délai de reconstruction du système informatique	**Jours**
Récupération d'un serveur	30
Configuration OS, outils et réseau	15
Restauration, applications, données	15
Récupération hub et câbles de secours	07
Installations et câblage volant	N/A
Temps total d'indisponibilité en jours	**67**

Cycle	**Contenu**	**jeux**	**Stockage** (lieu, accès, conditions, températures…)
Quotidienne	Données et applications	02	Disque dur externe, DVD.
Hebdomadaire			
Mensuelle			
Annuelle			

Source : Nous même, adapté de CLEUET & al (2008a : 57-59).

Cette étape conduit à l'élaboration du tableau des risques. Le tableau des risques (référentiel et TFfA) dans sa version finale est présenté dans les pages suivantes.

Tableau 7: Tableau des risques

Tâches / Opérations	Objectifs	Risques	Evaluation	Dispositif de contrôle interne / POCA	Constat
Gestion et évaluation des risques	▪ Protéger l'atteinte des objectifs informatique ; ▪ Protéger tous les actifs et en être comptable ; ▪ Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et ressources informatiques.	▪ Réponse aux risques non efficace ; ▪ Confiance excessive dans les contrôles insuffisants existants ; ▪ Perte d'actif informatique ▪ Non détection de l'impact d'un risque informatique sur l'entreprise.	Elevé Elevé Elevé Elevé	▪ Plan d'action de gestion des risques. ▪ Cartographie des risques. ▪ Fonction de gestion de risques (RSSI, risk manager). ▪ Mise en place d'une action de sensibilisation à la valeur des actifs informatiques. ▪ Approche élargie de la gestion des risques informatiques.	Non Non Non Non Non
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 de l'information et de l'infrastructure de traitement.	▪ Données et actifs informatiques non protégés ▪ Disparités entre les mesures de sécurité prévues et appliquées ; ▪ Mesures de sécurité mises en échec par les parties prenantes et les utilisateurs.	Moyen Elevé Moyen	▪ Protection des actifs informatiques critiques ▪ Plan de sécurité informatique ▪ Charte de sécurité informatique	Oui Non Non
Gestion des identités / gestion des comptes d'utilisateurs	▪ s'assurer que les données critiques et confidentielles ne sont pas accessibles à ceux qui ne doivent pas y accéder.	▪ Dénie de service ; ▪ Modification non autorisée des données ; ▪ Perte de confidentialité ; ▪ Reconfiguration non autorisée des systèmes ; ▪ Compromission de la sécurité logique.	Moyen Moyen Elevé Moyen Moyen	▪ Mot de passe, outil de gestion d'accès ▪ Verrouillage des configurations ▪ Limitation de l'accès au panneau de configuration ▪ Existence de procédure d'attribution, de suppression et de mise à jour des mots de passe	Oui Non Non Non

Prévention, détection, neutralisation des logiciels malveillants	▪ S'assurer de la protection des accès logiques aux systèmes d'information	▪ Divulgation d'information ; ▪ Systèmes et données ; exposés aux attaques de virus ; ▪ Contre mesures inefficaces ; ▪ Faille de sécurité.	Elevé Elevé Moyen Moyen	▪ Pare-feux ▪ Logiciels anti-virus ▪ Limitation des téléchargements ▪ Application des correctifs et patchs de sécurité ▪ Compartimentage du système informatique ▪ Sonde réseaux, honey pot	Oui Oui Non Non Oui Non
Sécurité des réseaux/ Echange des données sensibles	▪ S'assurer que les transactions métiers automatisées et les échanges d'information sont fiables.	▪ Divulgation d'informations confidentielles ; ▪ Systèmes et données exposés aux attaques de virus ; ▪ Contre mesures inefficaces ; ▪ Faille de sécurité ; ▪ Mise en péril de l'architecture de sécurité globale ; ▪ Attaques des cybers pirates.	Elevé Elevé Moyen Moyen Moyen Elevé	▪ Pare-feux, logiciels anti virus ▪ Serveurs proxy ▪ Limitation des téléchargements ▪ Application des correctifs et patchs de sécurité ▪ Compartimentage du système informatique ▪ Sonde réseaux, honey pot ▪ Cryptographie	Oui Oui Non Non Oui Non Non
Sauvegarde et archivage des données	▪ S'assurer que les services et l'infrastructure informatique 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 ; ▪ Risque juridique ; ▪ Arrêt de l'activité ; ▪ Reprise d'activité compromisse.	Elevé Elevé Moyen Elevé Elevé	▪ Procédures de sauvegarde des données définies ▪ Procédures d'archivage des données ▪ Armoire sécurisée de protection des supports de sauvegarde ▪ Contrôle de relecture des archives ▪ Conservation des données conforme aux délais légaux d'archivage ▪ Plan de secours et de reprise	Oui Oui Non Oui Oui Non

Sélection du site et agencement	▪ s'assurer que les services et l'infrastructure informatique peuvent résister convenablement à une panne due à une erreur, à une attaque délibérée ou à un sinistre, et se rétablir ; ▪ s'assurer que l'information critique et confidentielle n'est pas accessible à eux qui ne doivent pas y accéder ; ▪ S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'ait qu'un impact minimum sur l'activité ; ▪ Protéger tous les actifs informatiques et en être comptable.	▪ Non-identification des menaces envers la sécurité physique ▪ Vulnérabilité accrue vis-à-vis des risques de sécurité, résultant de l'emplacement et/ou de l'agencement du site	Elevé Moyen	▪ Bâtiment de construction solide ▪ Murs intérieurs pleins ▪ Portes extérieures blindées ▪ Dispositif de détection d'ouverture relié à une alarme ▪ Fenêtre en double vitrage blindée ▪ Barreaux sur les fenêtres extérieures	Oui Non Non Non Non Oui
Mesures de sécurité physiques / Accès physique		▪ Vol du matériel informatique ▪ Accès non autorisé aux sites sensibles ▪ Système reconfiguré sans autorisation ▪ Attaques terroristes	Faible Elevé Elevé Elevé	▪ Inventaire physique ▪ Service de gardiennage ▪ Système de détection d'intrusion ▪ Protection des câbles réseaux ▪ Contrôle d'accès aux bâtiments ▪ Gardiens armés et sensibilisés	Oui Oui Non Oui Oui Non
Protection contre les risques liés à l'environnement		▪ Poussière ▪ Chaleur / Humidité ▪ Inondation	Faible Faible Faible	▪ Service de nettoyage ▪ vitrage hermétique ▪ Climatisation/réfrigération redondante ▪ Salles sensibles situées en hauteur	Oui Non Oui Oui
Gestion des installations matérielles		▪ Destruction des bâtiments ▪ Destruction du système ▪ Coupures d'électricité ▪ Risques électriques ▪ Incendie / feu	Elevé Elevé Faible Moyen Elevé	▪ Contrat d'assurance du matériel ▪ Plan de reprise ▪ Groupes électrogènes ▪ Onduleurs avec batteries-relais ▪ Capteurs de fumée ▪ Extincteurs à poudre ▪ Extincteurs automatique d'incendie	Oui Non Oui Oui Non Oui Non

Source : Nous même, à partir de RENARD (2010 : 239), AFAI (2008a), AFAI (2008b), CLEUET & al (2008a) et CLEUET & al 2008b).

L'analyse du tableau des risques qui est au cœur de nôtre approche par les risques répertorie les risques opérationnels dans sa troisième colonne, identifie les meilleures pratiques dans sa cinquième colonne ; la quatrième colonne nous a permis de faire une évaluation des risques opérationnels en fonction de la présence ou non d'un dispositif de contrôle interne ou POCA (Pratique d'Organisation Communément Admise) de la sixième colonne ; cette évaluation des risques est présenté dans le tableau ci-après.

Du fait de l'absence d'une unité d'Audit Interne, de la vacance de poste au Bureau Informatique et du Profil du Chef du Bureau Informatique jugé inadéquat, la majorité des risques opérationnels identifiés ont une évaluation « élevé ».

Tableau 8: Matrice d'évaluation des risques.

Cotation du risque	Evaluation de l'impact	Nature des travaux
1	Faible	Contrôle par intermittence
2	Moyen ou important	Sondages et inspections
3	Elevé ou vital	Contrôle exhaustif

Source : Nous même, d'après l'approche de RENARD (2010) et SCHICK (2007).

Ce tableau est également le guide de mise en œuvre des tests que nous concevrons pour la recherche d'éléments probant.

Les objectifs généraux définis dès le début de la mission et les objectifs spécifiques figurant dans le tableau des risques conduisent à déterminer le champ d'action suivant.

Tableau 9: Champ d'action des travaux d'audit.

Lieu, local ou emplacement	Population cible
▪ Salle informatique ▪ Salle technique ▪ Bâtiment technique ▪ Bloc administratif	▪ Tous les serveurs ▪ Ordinateur du réseau local (42) ▪ Responsables des salles sensibles ▪ Paierie, Service Administratif.

Source : Nous même.

La phase de préparation s'achève avec la définition du champ d'action. Nous passons à la phase d'exécution de la mission.

6.1.2. La réalisation de la mission d'audit : les travaux sur le terrain

Cette phase a consisté à la finalisation du questionnaire de contrôle interne, à son administration auprès des principaux acteurs impliqués. Nous avons ensuite procéder à l'élaboration d'un programme de travail et à la conduite des travaux de vérifications sur le terrain.

Le contexte de l'étude n'a pas permis d'effectuer une réunion d'ouverture classique. Toutefois, avant de procéder à une quelconque opération, une sensibilisation a été effectuée auprès de chaque personne rencontrée. Notamment en ce qui concerne les objectifs de l'étude et la méthodologie

Le planning d'audit est présenté dans le tableau ci-après.

Tableau 10: Programme d'audit

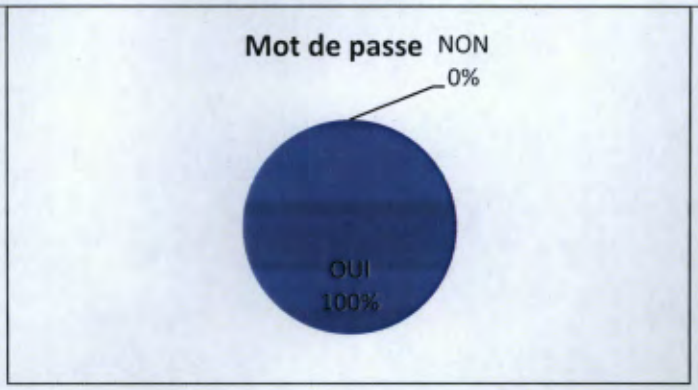
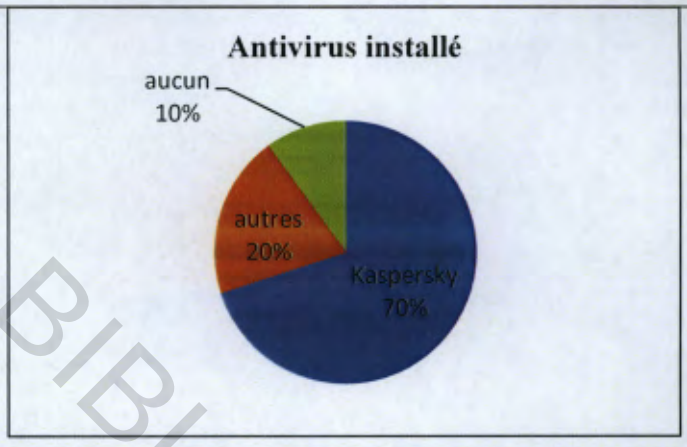
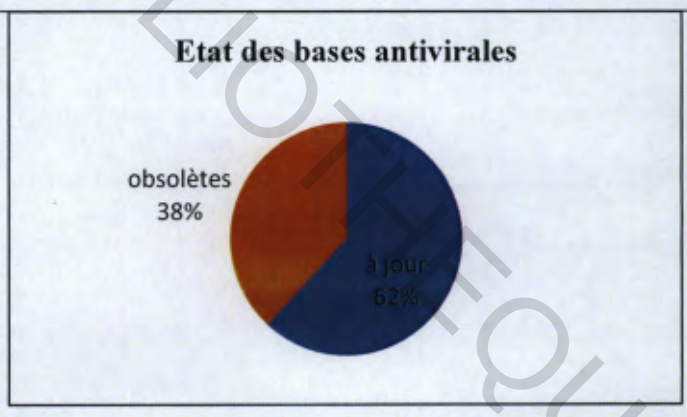
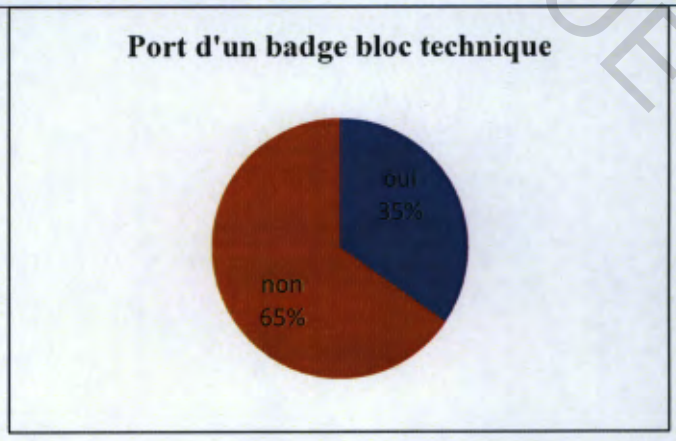
Objet	Service / lieu	Nature des travaux
Questionnaire de contrôle interne	▪ Bureau informatique ▪ Service IGC ▪ Service ESIR ▪ Section SSLI ▪ Bureau radio	▪ S'informer et confirmer ▪ Observer
Sécurité logique	▪ PC utilisateurs ▪ Serveurs	▪ Inspecter ▪ Observer
Sécurité physique	▪ Salle informatique ▪ Salle technique	▪ Inspecter ▪ Observer

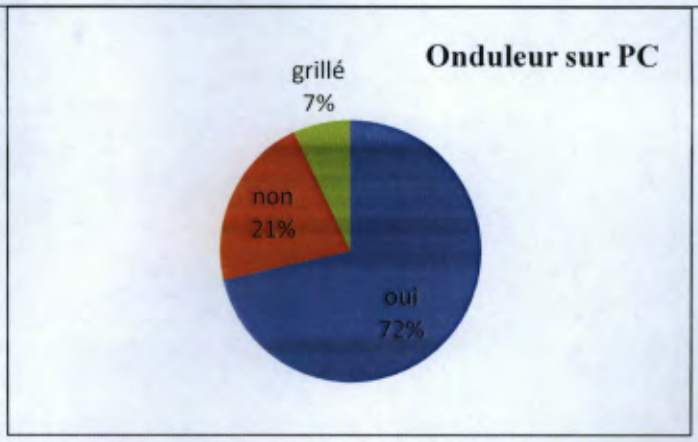
Source : Nous même.

Le questionnaire de contrôle interne (annexe 6) a été conçu de telle sorte qu'une réponse négative équivaut à une faiblesse (c'est-à-dire l'absence de tout dispositif de contrôle interne ou de bonnes pratiques) et une réponse positive équivaut à une force qui devra être confirmée par tests de conformité. Cette étape marque également le début de la fabrication des FRAP et des FAR.

Le programme de travail a été élaboré à partir des réponses positives du questionnaire de contrôle interne. Les résultats sont présentés dans le tableau avec figures imbriquées ci-après :

Tableau 11: Tests de confirmation du questionnaire de contrôle interne

Tests	Résultat des tests
B-2-2 : sélectionner un échantillon d'utilisateur (COGEST, DELTA-Paie, TRAFIC). vérifier qu'un mot de passe est exigé pour procéder aux traitements des données. ▪ Population cible : 15 ▪ Echantillon : 10	
B-3-2-a : sélectionner un échantillon ; vérifier que l'antivirus KASPERSKY est installé. ▪ Population étudiée : 42 ▪ Echantillon : 30 ▪ KASPERSKY : 21 ▪ Autres antivirus : 6 ▪ Aucun : 3	
B-3-2-b : vérifier que les bases de l'antivirus sont à jour pour l'antivirus KASPERSKY ▪ Population : 21 (issue de l'échantillon du test B-3-2a)	
C-3-4 : pendant trois jours, à raison d'un quart d'heure par jour, observer les entrées des personnes au bloc technique, vérifier que ces personnes portent des badges d'identification ▪ Nombre de visiteurs observés : 26 ▪ Port du badge : 9 ▪ Pas de badge : 17	

C-5-2 : sélectionner un échantillon d'ordinateur au bloc administratif, vérifier que ceux-ci sont protégés chacun par un onduleur et que celui-ci est en état de marche ▪ Echantillon : 14 ▪ Onduleur : 10 ▪ Grillé : 1	

Source : Nous même, à partir des réponses positives du questionnaire de contrôle interne.

Le test (C-5-2) a permis de constater que le serveur abritant l'application Delta-paie situé dans un bureau du bloc administratif n'est pas protégé par un onduleur.

Au terme de la réalisation de ces tests, une confirmation de l'existence d'autres dispositifs de prévention des risques les plus élevés doit être effectuée. Il s'agit pour cela de procéder à l'inspection de la salle abritant les serveurs du réseau local et de la salle abritant les serveurs, les appareils de communications et de radionavigation du réseau opérationnel.
Le tableau suivant est le guide qui a permis de faire une revue de la sécurité des deux salles (informatique et technique) et du bâtiment les abritant :

Tableau 12: Guide d'observation et d'inspection des locaux et des dispositifs de sécurité.

Points à observer	Constats
Qualité des murs	Murs solide à l'extérieur ; cloisons en bois dans le bâtiment technique
Qualité des portes	Porte en bois, porte en bois avec ouverture vitrée
Qualité des fenêtres et du vitrage	Simple vitrage (lamelles de vitre non hermétiques). Barreaux à la fenêtre extérieure de la salle informatique
Traces d'humidité sur plafond et mur	Trace d'humidité au plafond de la salle technique, le plancher de l'étage supérieur n'est pas étanche

Système de détection incendie	Aucun, téléphone de secours dans la salle technique relié à la caserne des pompiers, une personne en poste 24h/24
Alarme automatique ou manuel	Aucune alarme, vigilance de la personne de garde
Extincteurs	Aucun extincteur dans la salle informatique ; un seul extincteur à poudre dans la salle technique, disposé derrière les baies, donc pas facile d'accès quand on ne connait pas la salle ou son emplacement ; un second extincteur dans le sas d'entrée
Extincteurs entretenus	Dernière date de révision le 29/09/2010
Bouches d'incendies	Les tuyaux au premier étage sont absents dans la colonne montante
Protection des câblages	Câbles dans les goulottes dans les salles. Portes d'accès des colonnes montantes ne se ferment plus à cause de serrure arrachées
Arrivée multiple du courant électrique	Oui, double tableau électrique dans les deux salles
Onduleurs et batteries-relais redondant	Trois serveurs de la salle informatique branchés sur le même onduleur
Climatisation redondant	Oui, trois climatiseurs dans la salle technique, N/A pour la salle informatique
Réfrigération	Température non constante en raison des vitrages non hermétique dans la salle technique. Les joints d'étanchéité sont abimés.
Trace d'humidité	Le plafond au dessus des commutateurs présente des auréoles d'humidité, le plancher de l'étage du dessus est vétuste.

Présence de poussière	Non, présence d'un compresseur dans la salle technique. Présence de poussière dans les bureaux des utilisateurs sur les PC
Rangement des locaux	Bon rangement salle technique ; salle informatique présence de nombreux cartons
Protection des supports de sauvegarde	Aucun dispositif particulier
Lieu de stockage des sauvegardes	Stockées à coté des ordinateurs, dans la salle technique et la salle informatique

Source : Nous même.

Les lacunes constatées dès la phase de préparation et lors de l'administration du questionnaire de contrôle interne de même que les dysfonctionnements observés lors de l'inspection des salles conduisent à des analyses au travers des FAR ou des FRAP.

6.2. Synthèse de la mission d'audit de la sécurité informatique

Cette section va présenter les forces et les faiblesses du processus que nous avons audité. La présentation se fera selon le découpage déjà retenu lors de la délimitation par processus et taches retenus dans le tableau des risques (voir Tableau 7) et le questionnaire de contrôle interne (annexe 6) et ceci, suivant la codification faite dans le tableau 8.

6.2.1. Les points forts de la sécurité informatique

- **Gestion des identités / Gestion des comptes d'utilisateurs**
  - L'accès aux applications professionnelles est protégé par un processus d'authentification avec nom d'utilisateur et mot de passe.

- **Prévention, détection, neutralisation des logiciels malveillants**
  - La Représentation dispose d'un antivirus avec licence commerciale et mise à jour sur internet pour 746 postes valide jusqu'au 10 novembre 2012.

- **Sécurité des réseaux / Echange des données sensibles**
  - Le système informatique de la Représentation est compartimenté.
  - Un serveur Proxy est installé en amont de la connexion internet.
  - L'antivirus KASPERSKY dispose d'un pare-feu intégré.

- **Sauvegarde et archivage des données**
  - Les données sur tous les serveurs sont sauvegardées tous les jours en deux copies ; CD et disque dur externe.
  - Les sauvegardes sont archivées pour une durée de trois mois pour le réseau opérationnel.
  - Les sauvegardes du réseau local sont archivées au bureau du Représentant et au Siège.

- **Sélection du site et agencement**
  - Les deux salles sensibles sont bien aménagées et rangées.

- **Mesures de sécurité physiques / Accès physique**
  - L'accès aux informations sur les sites est limité par des armoires fermées à clés.
  - La salle technique et la salle informatique ne sont pas facilement identifiables de l'extérieure.
  - Les câbles de la salle technique, la salle informatique et des bureaux sont protégés par des goulottes.

- **Protection contre les risques liés à l'environnement**
  - Les salles sont situées en hauteur dans le bâtiment technique.
  - La salle technique dispose de trois climatiseurs et la salle informatique d'un climatiseur.
  - La salle technique dispose d'un compresseur pour éliminer la poussière sur les équipements.

- **Gestion des installations matérielles**
  - L'électricité est fournie en continue par la centrale électrique qui dispose d'une arrivée de deux lignes de moyenne tension, de quatre groupes électrogènes et de batteries d'appoint.
  - Les câbles hors bâtiments sont enterrés.
  - Les serveurs de la salle technique sont entretenus directement par le fournisseur.

6.2.2. Les risques et les points faibles de la sécurité informatique

Nous allons présenter dans ce paragraphe les faiblesses que nous avons relevées tout au long de nos travaux d'audit ainsi que le niveau de risque correspondant tel que déjà présenté dans le tableau des risques (voir tableau 7) et la matrice d'évaluation des risques (voir tableau 8). Les risques recensés dans le tableau des risques (troisième colonne) sont repris avec leurs cotation entre parenthèses, suivis des faiblesses dont ils émanent.

- **Gestion et évaluation des risques**
  - Les risques identifiés sont : réponse aux risques non efficace (3), confiance excessive dans les contrôles insuffisants existants (3), perte d'actif informatique (3), non détection de l'impact d'un risque informatique sur l'entreprise (3).
    - Il n'existe pas de processus d'évaluation et de gestion des risques informatiques à la Représentation ASECNA du Cameroun.
    - Le contexte de risque informatique ne semble pas compris dans sa globalité.

- **Gestion de la sécurité informatique**
  - Les risques sont : disparités entre les mesures de sécurité prévues et appliquées (3), données et actifs informatiques non protégés (2), mesures de sécurité mises en échec par les parties prenantes et les utilisateurs (2).
    - Le poste d'Agent Informatique, chargé de la gestion de la sécurité et de la surveillance de l'environnement informatique, est vacant.
    - Il n'existe pas de standards et de procédures détaillés de sécurité informatique.
    - Les utilisateurs ne sont pas conscients des risques informatiques.
    - La Représentation ne dispose pas de charte informatique.
    - Aucune politique de sécurité informatique n'est définie.

- Il n'existe pas de structure organisationnelle et hiérarchique de la sécurité informatique.

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

❖ Les risques sont : perte de confidentialité (3), dénie de service (2), modification non autorisées des données (2), reconfiguration non autorisée des systèmes (2), compromission de la sécurité logique (2).

- Il n'existe pas de procédures pour évaluer régulièrement et ré-authentifier les droits d'accès aux systèmes et aux applications.
- Les droits d'accès (profils) aux applications ne sont pas gérés par le management responsable du processus.
- Les PC des utilisateurs du réseau local ne sont pas protégés par un mot de passe au démarrage ou en sortie de veille.
- Les mots de passe des utilisateurs ne sont pas personnels.
- Les mots de passe ne sont pas régulièrement renouvelés.

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

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

- L'antivirus KASPERSKY n'est pas installé sur tous les postes.
- Lorsque l'antivirus est installé, les bases ne sont pas toujours actualisées.
- Des antivirus avec licence gratuite sont utilisés sur certains PC.
- Les téléchargements ne sont pas régulés ou filtrés.
- Les utilisateurs installent eux-mêmes des logiciels sur leurs PC.
- Les utilisateurs méconnaissent les risques informatiques.

➢ **Sécurité des réseaux / Echanges des données sensibles.**

❖ Les risques sont : attaques des cybers pirates (3), divulgation d'information (3), systèmes et données exposés aux attaques de virus (3), contre mesures inefficaces (2), faille de sécurité (2), mise en péril de l'architecture de sécurité globale (2).

- Les informations confidentielles envoyées par mail ne sont pas chiffrées (cryptées).

➢ **Sauvegarde et archivage des données**

❖ Les risques sont : perte d'image (3), risque financier (3), arrêt de l'activité (3), reprise de l'activité compromise (3), risque juridique (2).

- Les supports de sauvegarde ne sont pas sécurisés contre le feu et contre une éventuelle destruction volontaire ou accidentelle.
- Les supports archivés ne sont pas protégés dans des armoires ou des coffres.

➢ **Sélection du site et agencement**

❖ Les risques sont : non-identification des menaces envers la sécurité physique (3), vulnérabilité accrue vis-à-vis des risques de sécurité résultant de l'emplacement et/ou de l'agencement du site (2).

- Le bâtiment technique présente des signes de délabrement.
- Le plancher du local au dessus de la salle technique laisse passer des infiltrations d'eau susceptibles de provoquer des courts-circuits dans les appareils de radionavigation et les serveurs.
- Les cloisons en contre-plaqué augmentent l'impact de destruction en cas d'incendie.

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

❖ Les risques sont : attaques terroristes (3), accès non autorisé aux sites sensibles (3), systèmes reconfigurés sans autorisation (3), vol du matériel informatique (2).

- Aucune procédure écrite n'est mise en œuvre pour définir et faire appliquer les mesures de sécurité physique et de contrôle d'accès.
- Il n'existe pas de système d'alarme ou de détection d'intrusion.
- Les sites sensibles ne sont pas fréquemment contrôlés par les vigiles.
- Les personnes entrant dans le bâtiment technique ne sont pas identifiés de façon systématique.
- Les personnes ne portant pas de signe d'identification ne sont pas interpellées.
- Les vigiles ne sont pas toujours présents à leur poste.
- Le registre des vigiles n'est pas régulièrement renseigné.

- **Protection contre les risques liés à l'environnement**
  - Les risques sont : poussière (1), chaleur (1), humidité (1), inondation (1).
    - Les vitrages de la salle technique ne sont pas hermétiques, la température n'est pas constante dans cette salle.
    - Les auréoles d'humidité au plafond montrent que les appareils peuvent être grillés à tout instant.

- **Gestion des installations matérielles**
  - Les risques sont : destruction des bâtiments (3), destruction du système (3), incendie/feu (3), risques électriques (2), coupures d'électricité (1).
    - Le serveur de la solde situé dans un bureau du bloc administratif n'est pas équipé d'un onduleur.
    - Trois serveurs de la salle informatique sont branchés à un seul et unique onduleur.
    - Tous les ordinateurs ne sont pas équipés d'onduleurs fonctionnels.
    - La salle informatique n'est pas équipée d'un extincteur.
    - L'extincteur de la salle technique est disposé à même le sol et derrière une rangée d'équipements.
    - Aucun dispositif de détection de chaleur, de fumée ou de feu n'est installée dans aucune salle.
    - Les bouches d'incendie ne sont pas équipées de tuyaux ou lance incendie.
    - L'usage éventuel d'eau par les sapeurs-pompiers pour l'extinction d'un feu pourrait causer des courts-circuits et la destruction du matériel informatique.

La présentation des forces et des faiblesses du processus de sécurité informatique achevées, il convient de formuler des recommandations aux différents responsables concernés.

6.3. Les recommandations

Ces recommandations devraient être mises en œuvre aussi bien au niveau organisationnel et managérial qu'au niveau technique.

6.3.1. Recommandations à Monsieur le Représentant

La représentation gagnerait à :

- créer un comité de sécurité pour le pilotage des risques et le suivi des mesures de sécurité pour les sites et les équipements sensibles ; ce comité jouera le rôle de Risk Manager ou de RSI ;
- initier un plan de continuité ou plan de secours dont les scénarii de reprise seront conçus par le comité de sécurité ;
- commander un audit organisationnel et fonctionnel du bureau informatique
- faire élaborer une cartographie des risques pour évaluer les différents risques ;
- lancer un avis de vacance de poste pour le recrutement d'un agent informatique ;
- mettre en œuvre un plan de réhabilitation des locaux abritant la salle technique ;
- élaborer une politique de sécurité informatique conforme aux standards ISO 27000, ISO 27001, ISO 27002 ;
- formaliser le processus de sécurité informatique en procédant à l'élaboration d'un manuel de procédure qui spécifie les tâches et les responsabilités des parties prenantes à ce processus ;
- faire un suivi des recommandations ci-dessous.

6.3.2. Recommandations à Monsieur le Chef de Service Infrastructures de Génie Civil

Il serait souhaitable de :

- remplacer les portes en bois par des portes blindées pour la protection des couloirs d'accès aux salles sensibles ;
- proposer des avenants au contrat de la société de gardiennage précisant ses responsabilités, le rôle et les tâches des agents affectés à la garde des points d'accès ;

- remplacer les serrures des portes des colonnes montantes pour protéger les câbles qui y sont dissimulés dans la structure du bâtiment technique;
- changer les vitrages de la salle technique afin de limiter les variations de température importantes dans cette salle ;
- acquérir et installer un dispositif de détection de fumée pour les salles sensibles;
- acquérir des coffres ou des armoires ignifuges pour stocker les supports de sauvegarde dans le bureau du Représentant, dans la salle technique et dans la salle informatique.

6.3.3. Recommandations à Monsieur le Chef de Bureau Informatique

Afin d'assurer une meilleure sécurité logique, il serait opportun de :

- Proposer un plan de secours informatique au Représentant pour parer à un scénario de destruction du système informatique de la Représentation ;
- installer uniquement l'antivirus KASPERKY sur l'ensemble des PC du réseau local ;
- revoir la configuration de l'antivirus pour augmenter la fréquence des mises à jour ;
- acquérir un onduleur conforme et l'installer sur le serveur de la Solde ;
- brancher un serveur par onduleur à la salle informatique ;
- installer ou remplacer les onduleurs défectueux des utilisateurs ;
- migrer l'ensemble des utilisateurs de PC du profil administrateur au profil utilisateur ;
- restreindre les téléchargements des logiciels sur les PC, bloquer le téléchargement pour certaines extensions de fichiers (.exe par exemple) ;
- redéfinir les règles de création de mot de passe des utilisateurs pour tenir compte de la longueur, du nombre de caractère, 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 et les familiariser à la cryptographie pour l'échange de fichiers professionnels par mail ;
- choisir un référentiel de gestion des risques et un référentiel de gouvernance des systèmes informatiques et le proposer à Monsieur le Représentant comme canevas pour l'élaboration d'un manuel de procédure qui formalisera les tâches et les objectifs de sécurité informatique.

6.3.4. Recommandations à M. le Chef section sauvetage et lutte contre l'incendie

Il serait judicieux de :

- procéder à l'installation d'un extincteur dans la salle informatique ;
- installer un second extincteur dans la salle technique sur un support mural et à portée de vue de toute personne présente dans cette salle et dans toutes les autres salles ;
- remplacer les lances d'incendie absentes dans les colonnes sèches du bâtiment technique ;
- proposer un dispositif de détection de fumée et des spécifications techniques à Monsieur le Chef de service infrastructure et génie civil pour acquisition et installation ; assister Monsieur le Chef de service infrastructure et génie civil pour l'acquisition des coffres et des armoires ignifuges.

6.4. Mise en œuvre des recommandations

Mettre en œuvre des recommandations implique de tenir compte de certaines priorités, de la programmation budgétaire, des délais et de la disponibilité des différents protagonistes.
Le tableau de mise en œuvre suivant est un essai de proposition, il est une synthèse des recommandations aux différents responsables de l'ASECNA Cameroun, il ne saurait avoir un caractère impératif et absolu.

Tableau 13: Proposition de mise en œuvre des recommandations

Responsable concerné	Actions	Délai de mise en œuvre
Représentant	Suivi des recommandations	Immédiat
	Avis de vacances de postes	02 jours
	Comité de sécurité / politique de sécurité / plan de secours	02 semaines
	Audit organisationnel et fonctionnel du Bureau Informatique	Janvier 2011
	Réhabilitation des locaux / manuel de procédure / cartographie des risques	Budget 2011
Chef Service Infrastructures et Génie Civil	Achat de coffres et d'armoires ignifuges	01 semaine
	Avenants aux différents contrats	01 semaine
	Remplacements des serrures / remplacements des vitrages	02 semaines
	Achat et installations des dispositifs de détection de fumée	01 mois
	Achat et installations des portes blindées	Budget 2011
Chef du Bureau Informatique	Installations et remplacements des onduleurs	Immédiat
	Reconfiguration des PC et de l'antivirus	Immédiat
	Elaboration de la charte informatique	02 semaines
	Choix d'un référentiel / ébauche de scénario de reprise d'activité	02 semaines
	Ateliers de formation aux risques informatiques et à la cryptographie	01 mois
Chef Section Sauvetage et Lutte contre l'Incendie	Proposition des spécifications techniques du matériel de détection de fumée	01 jour
	Installation des extincteurs / Remplacement des lances d'incendie	02 jours

Source : Nous même.

Conclusion de la deuxième partie

Cette deuxième partie a été l'occasion de présenter l'ASECNA et la Représentation du Cameroun, le système informatique et les mesures de sécurité appliquées et les dispositifs mis en place. Les informations reçues et collectées ont permis la mise en œuvre de notre démarche référentielle et la conduite de l'audit de la sécurité du système informatique.

L'audit de la sécurité informatique permettra à la Représentation ASECNA du Cameroun de corriger certaines défaillances constatées sur le plan organisationnel, fonctionnel et pratique.

CONCLUSION GENERALE

L'informatique est un système transversal qui s'est installé au cœur des activités humaines. Il rêvait désormais un caractère stratégique et hautement sensible. C'est à ce titre que sa sécurité doit être assurée de manière efficace et efficiente. Les risques informatiques se transfèrent à l'organisation utilisatrice de cet outil. Ces risques sont de plusieurs types : logiques, physiques, environnementaux etc. La matérialisation d'un ou de plusieurs de ces risques peut entrainer des dommages de nature à mettre en péril la continuité de l'exploitation. Des mesures de sécurité doivent donc être prises afin de pallier à cette éventualité. Pour cela un dispositif de pilotage et de contrôle doit être mis en œuvre et des outils doivent être déployés.

La pratique organisationnelle de la sécurité informatique est encadrée par des normes et des standards appliqués à l'échelle planétaire. Ce formalisme permet ainsi à l'auditeur qui fait le choix d'un cadre de référence de confronter la pratique courante aux meilleurs dispositifs et pratiques existants. L'auditeur ne doit pas être obnubilé par son cadre de référence car chaque entité vit des réalités différentes. Pour faire un apport constructif, comprendre les réalités de l'organisation ou du système audité demande qu'un travail d'information préalable soit entrepris.

Le choix d'un cadre de référence et d'une démarche référentielle revêt ici toute son importance car prendre connaissance de l'entité, des risques et des dispositifs mis en place impose de suivre une méthode cohérente et efficace. L'auditeur suit un chemin balisé mais doit faire un tri parmi les nombreux outils d'audit à sa disposition. En effet certains de ses outils sont de toutes les missions tandis que d'autres ne seront mis en œuvre que dans des cas de figures particuliers. Ce choix a été fait pour la réalisation de l'audit de la sécurité effectué et présenté dans ce mémoire.

Outil de diagnostic par excellence, l'audit permet de procéder à une évaluation du contrôle interne qui dans le cas de cette étude est représenté par la sécurité informatique. Ce système n'est pas toujours facile à comprendre, tant la frontière est mouvante pour cerner ses limites. En effet l'informatique s'appuie sur l'électronique mais tout ce qui est électronique n'est pas forcement informatique. Le choix d'un périmètre d'audit s'avère donc indispensable.

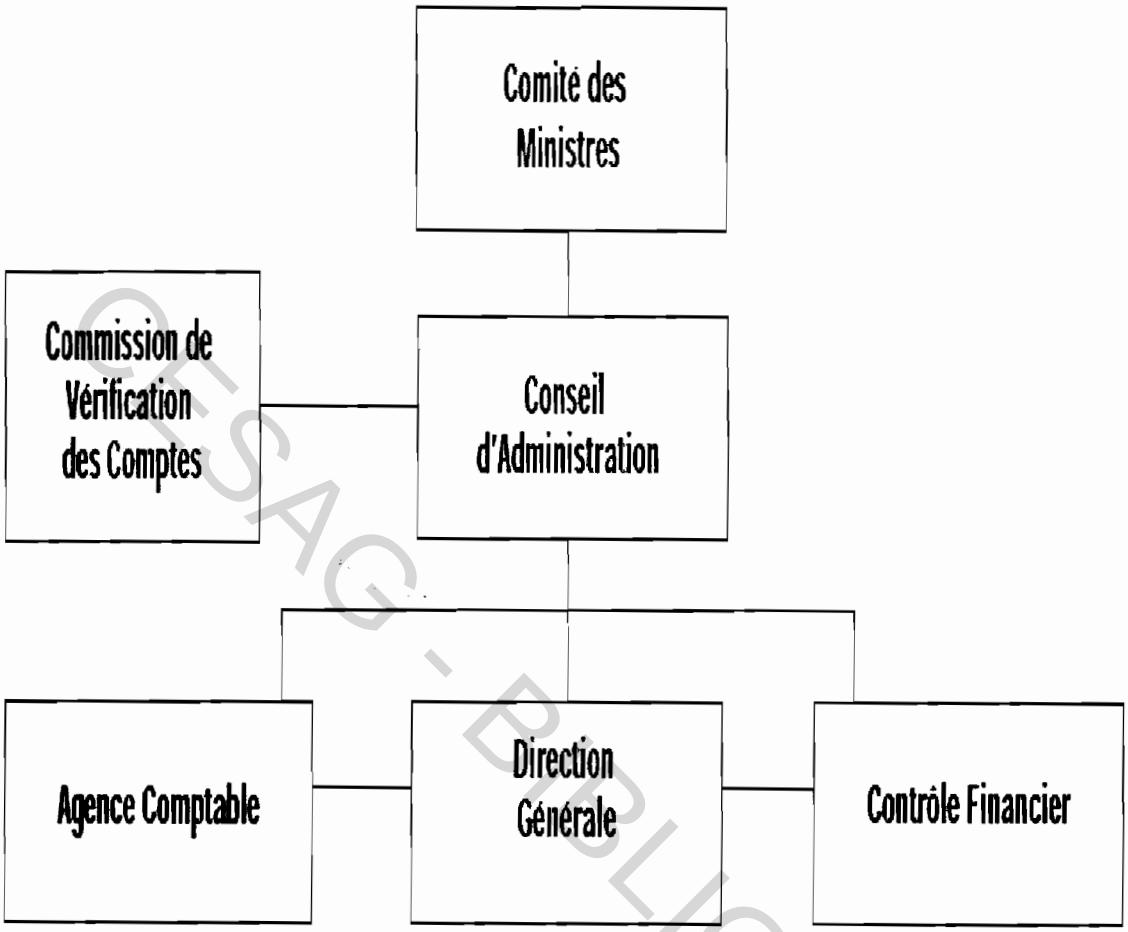
Au terme des travaux effectués, nous avons acquis une certaine connaissance du processus audité. Les interviews et les entretiens effectués, les analyses, les observations ont permis d'orienter les investigations. Des travaux de vérification poussés ont été entrepris afin de

valider des faits ou de confirmer les réalités observés. Des faiblesses et des forces ont été constatées, elles ont donné lieu à des analyses permettant de faire des recommandations qui devraient améliorer le processus audité grâce à un plan d'action.

Au terme de cette étude l'état des lieux qui peut être dressé est que l'évaluation et la gestion des risques informatiques qui est nôtre premier objectifs ne sont pas effectuées, la sécurité des systèmes et la gestion de l'environnement physique sont moyennement satisfaisantes car ces deux derniers objectifs présentent de nombreux risques à l'impact potentiels élevés. Aussi un audit global de la fonction informatique ou une réorganisation organisationnelle et fonctionnelle devrait être effectué dans les plus brefs délais.

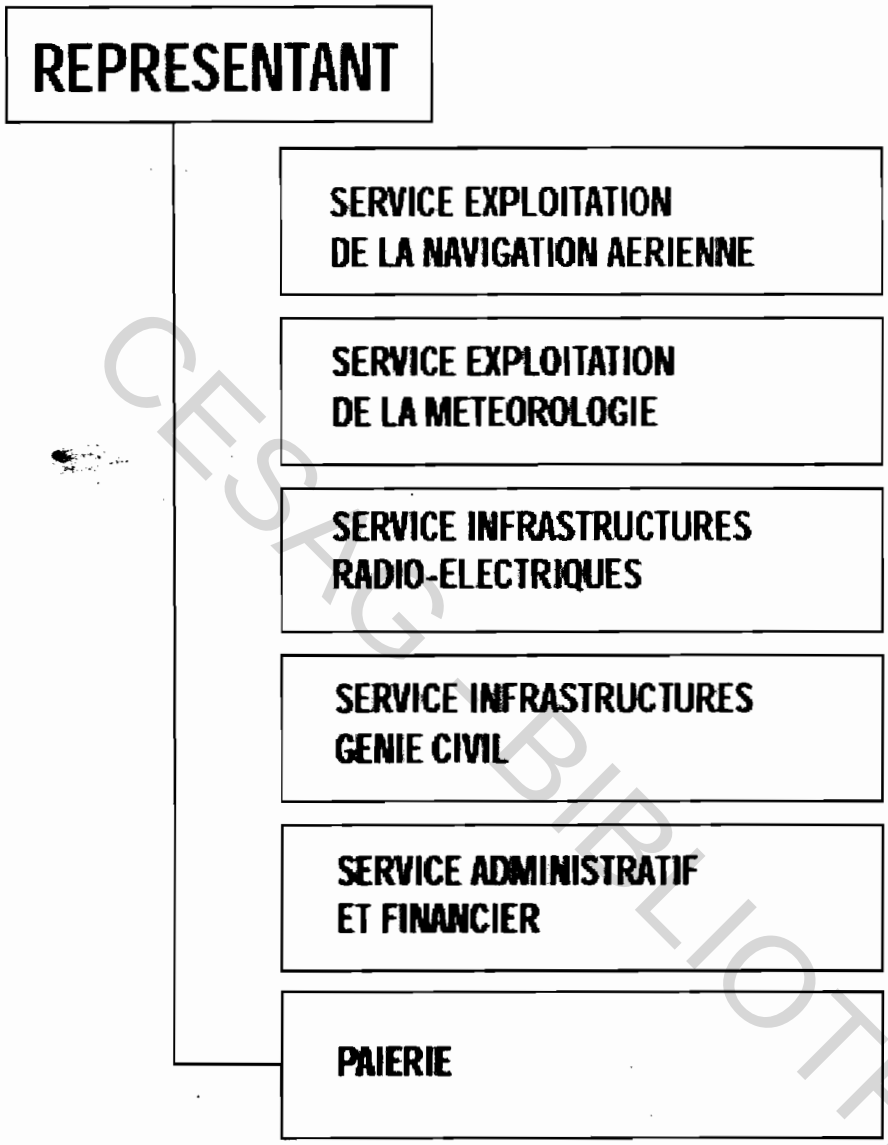
ANNEXES

Annexe 1: Les structures statutaires de l'ASECNA



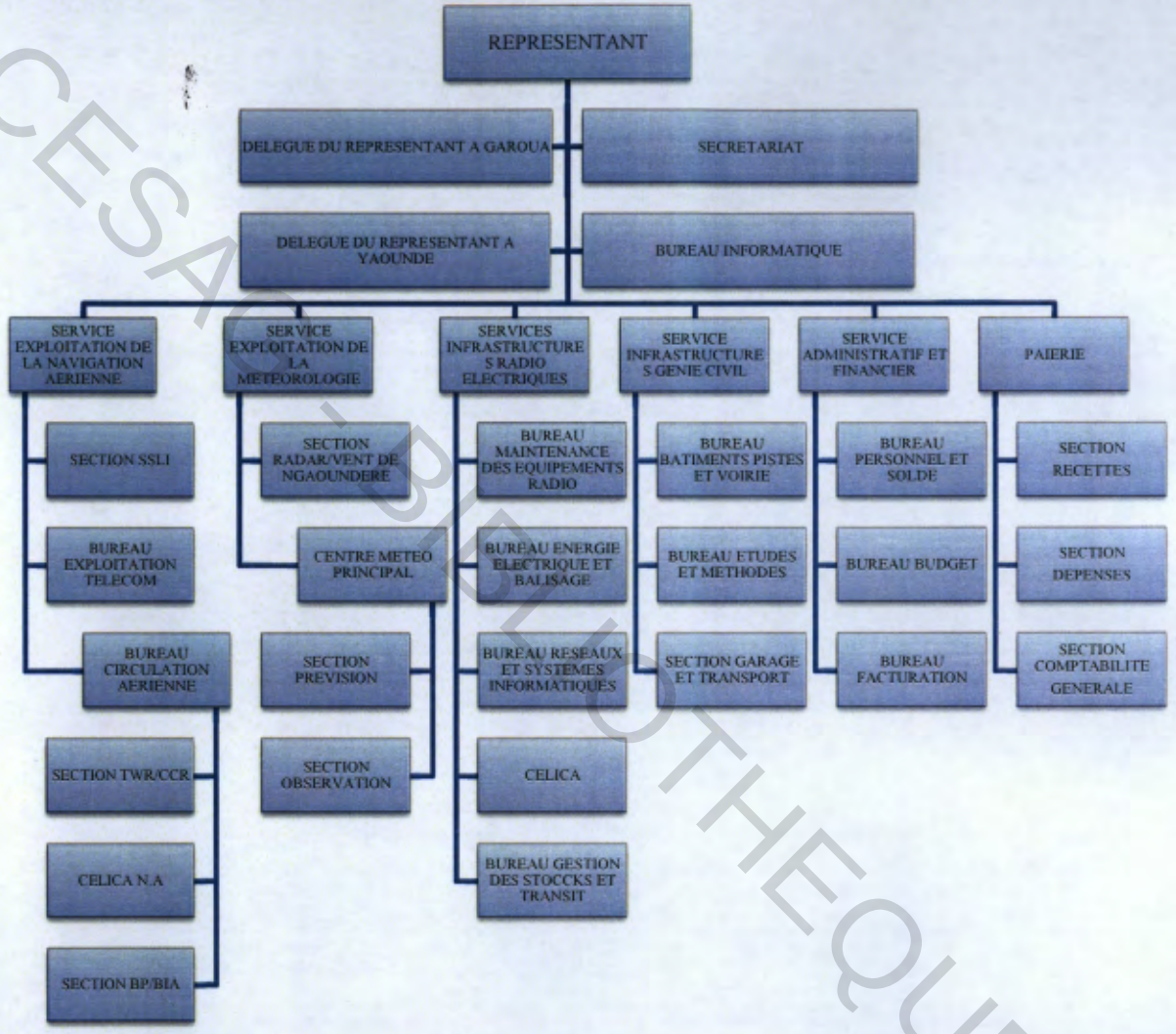
Source : ASECNA (2008 : 12).

Annexe 2: Organigramme d'une Représentation



Source : ASECNA (2008 : 13).

Annexe 3: Organigramme détaillé de la Représentation du Cameroun



Source : Nous même, adapté du Manuel des emplois de l'ASECNA (2008).

Annexe 4: Proposition d'ordre de mission

Ordonnateur : Représentation Service : Cabinet du Représentant	Date : 14 septembre 2010 Réf :

Objet : **Audit de la sécurité du système informatique**

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 du Sénégal (CESAG), Monsieur NGA ATANGANA se propose de réaliser un audit de la sécurité du système informatique du point de vue de l'auditeur interne.

La question de recherche principale de cette étude est : « Comment s'assurer que les mesures de sécurité existantes protègent efficacement le système informatique ? »
La mission se débutera dès approbation du thème de la mission et s'achèvera le 29 octobre 2010.

Cette étude à pour but d'analyser la sécurité informatique de la Représentation ASECNA du Cameroun, identifier les forces et les faiblesses afin d'émettre des recommandations en vue de son amélioration. Les objectifs spécifiques de la mission sont :

- S'assurer de l'évaluation et de la gestion des risques en analysant et communiquant sur les risques informatiques ainsi que leur impact potentiel sur les objectifs et les processus métiers;
- S'assurer de la sécurité des systèmes en évaluant les dispositifs mis en place pour maintenir l'intégrité de l'information et de l'infrastructure technologique et réduire au maximum les conséquences, des failles et des incidents de sécurité;
- S'assurer de la gestion de l'environnement physique en évaluant les mesures de protections des actifs informatiques et les données métiers et réduire le risque d'interruption de l'activité.

Cette mission se déroulera auprès des utilisateurs de l'outil informatique et du Bureau informatique/contrôle de gestion à ASECNA Cameroun

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

Le Représentant ASECNA

Destinataires : Service administratif, Bureau informatique, utilisateurs de l'outil informatique.

Source : Nous même, à partir de SCHLIK (2007).

Annexe 5: Guide d'entretien des protagonistes à la sécurité informatique.

Service Infrastructure et Génie Civil

- Quelles sont les missions dévolues à votre service ?
- Quelles sont les bureaux et sections sous votre responsabilité ?
- Quel usage faites-vous de l'outil informatique ?
- De combien d'ordinateur votre service dispose-t-il ?
- Connaissez-vous les risques informatiques ?
- Comment sont gérés les contrats des prestataires ?
- Quel appui votre service apporte au bureau informatique ?

Service Exploitation de la Navigation Aérienne

- Quelles sont les missions dévolues à votre service ?
- Quels sont les bureaux et sections sous votre responsabilité ?
- Quel usage faites-vous de l'outil informatique ?
- Votre service dispose-t-il de logiciel spécifique ?
- De combien d'ordinateur disposez-vous ? Connaissez-vous les risques informatiques ?
- Quel appui votre service apporte au bureau informatique ?
- Quelles prestations le bureau informatique vous fournit-il ?
- Par qui et comment est géré le système utilisé par votre service ?

Service Exploitation Infrastructures Radioélectriques

- Quelles sont les missions de votre service ?
- Quels sont les bureaux et sections qui dépendent de vôtre service ?
- La centrale électrique dépend-t-elle de l'ASECNA ?
- Comment fonctionne la centrale électrique ?
- Quel usage est fait de l'outil informatique dans votre service ?

Paierie

- Disposez-vous d'une application spécifique ? Comment-est-elle utilisée ?
- Comment est- elle sécurisée ?
- Qui a la charge de votre système d'information ?
- Comment vos données sont-elles sauvegardées ?
- Connaissez-vous les risques informatiques auxquels vous êtes exposés ?

Section Sauvetage et Lutte Contre l'incendie

- Comment fonctionne votre section ?
- Comment assurez-vous la prévention contre le feu dans les bâtiments ?
- Qui entretient les extincteurs ?
- Etes vous reliez aux bâtiments par un dispositif quelconque ? Si oui, lequel ?

Bureau Personnel et Solde

- En quoi consiste votre travail ?
- Disposez-vous d'une application spécifique ?
- Comment est –elle sécurisée ?
- Qui la gère et qui sauvegarde vos données ?
- Quel est l'effectif de la Représentation ?

Bureau Radio

- En quoi consiste votre travail ?
- Comment protégez-vous les disques et les enregistrements ?
- Pouvons-nous visiter la salle technique ?
- Quelles sont les mesures de sécurité des équipements de la salle technique ?

Bureau Exploitation des télécommunications

- Parlez-nous de vos missions ?
- Comment gérez-vous la sécurité du système sous votre responsabilité ?
- Qui entretient votre matériel ?
- Quelles sont les applications spécifiques que vous administrez ?
- De quel matériel de sécurité disposez-vous ?
- Des mesures de sécurité particulières sont-elles définies pour vôtre réseau ?
- Pourquoi n'utilisez vous pas systématiquement des antivirus ?
- Installez-vous des antivirus sur vos serveurs ?
- Pouvez-vous nous décrire le matériel utilisé pour remplir votre mission ?

Vigile du bloc technique

- En quoi consiste votre travail ?
- Vous enregistrez toutes les entrées dans le registre ?
- Contrôlez-vous les badges à l'entrée ?
- Examinez-vous le matériel qui sort du bloc technique ?

Annexe 6: Questionnaire de Contrôle Interne

QUESTIONNAIRE DE CONTROLE INTERNE	Système informatique	Folio 1/11

AUDIT DE LA SECURITE DU SYSTEME INFORMATIQUE

OBJECTIFS DE CONTROLE :

A- S'assurer que les risques informatiques sont évalués et gérés.

B- S'assurer de la gestion de la sécurité du système informatique

C- S'assurer de la gestion de l'environnement physique

Source : Nous même, d'après les Approches de CLEUET & al, AFAI, ISACA et COBIT.

QUESTIONNAIRE DE CONTRÔLE INTERNE	Bureau informatique	Folio 2/11

OBJECTIF DE CONTRÔLE :
A- S'assurer que les risques informatiques sont évalués et gérés.

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Un référentiel de gestion des risques existe-il dans l'entreprise ?	✓			ne concerne pas les risques informatiques	
2. Existe-t-il un référentiel de gestion des risques informatiques ?		✓		au Siège	
3. Le contexte de risque informatique est-il : a) compris ? b) communiqué ?	✓	✓			
4. Les principaux évènements ou menaces sont –ils identifiés ?		✓			
5. Existe-il un processus d'identification qui tient compte : a) de la probabilité ? b) des conséquences ?		✓ ✓			
6. Existe-il un processus de réponse aux risques informatiques ?		✓		au Siège	
7. Un plan d'action de gestion des risques est – il en place ?		✓			

QUESTIONNAIRE DE CONTRÔLE INTERNE	Bureau informatique	Folio 3/11

OBJECTIF DE CONTRÔLE :
B- S'assurer de la gestion de la sécurité du système informatique

B-1 : Gestion de la sécurité informatique

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Existe-t-il un comité de pilotage de la sécurité informatique ?		✓		Oui, au siège.	
2. Les membres de ce comité sont-ils issues des principaux services fonctionnels de l'entreprise ?			✓		
3. Est-ce que l'entreprise dispose d'une charte informatique ?		✓		En cours d'élaboration.	
4. La politique de sécurité couvre t-elle : a) la responsabilité du conseil d'administration ? b) la direction générale ? c) les cadres intermédiaires ?	 ✓ 	 ✓	 ✓ 	 Pas à la Représentation. 	
5. Existe-t-il des standards et procédures de sécurité détaillés ? a) Politique de sécurité des ordinateurs de bureau et ordinateurs portables? b) politique d'utilisation d'internet ? c) politique de sécurité du courrier électronique ? d) contrat de conformité aux règles de sécurité informatique ?		✓ ✓ ✓ ✓ ✓			
6. L'entreprise dispose-t-elle d'une structure organisationnelle et hiérarchique de la sécurité informatique ?		✓		En cours au siège.	

QUESTIONNAIRE DE CONTRÔLE INTERNE	Bureau informatique	Folio 4/11

OBJECTIF DE CONTRÔLE :
B- S'assurer de la gestion de la sécurité du système informatique

B-2 : Gestion des identités/ gestion des comptes d'utilisateurs

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Les actions des utilisateurs (internes, externes, temporaires) sont-elles identifiables sans ambigüité?		✓			
2. Les systèmes sont-ils configurés pour imposer l'authentification avant d'autoriser l'accès ?	✓			Uniquement pour les applications professionnelles (COGEST, DELTA-Paie, TRAFIC)	
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 CONTRÔLE INTERNE	Bureau informatique	Folio 5/11

OBJECTIF DE CONTRÔLE :
B- S'assurer de la gestion de la sécurité du système informatique

B-3 : Prévention, détection, neutralisation des logiciels malveillants / Sécurité des réseaux / Echange des données sensibles

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Une politique de prévention contre les logiciels malveillants a-t-elle été mise en place, est-elle documentée et communiquée dans l'ensemble de l'entreprise?	✓				
2. Un logiciel de protection est-il : a) distribué ? b) de façon centralisée (version et correctifs) ? c) à l'aide d'un processus centralisé de configuration et de gestion des modifications?	✓	✓ ✓		Antivirus KASPERSKY avec licence commerciale pour l'ensemble de la Représentation	
3. L'usage des mots de passe est-il généralisé sur tous les postes et pour 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?	✓ ✓			Oui, pare-feux et serveurs Proxy.	
6. Les données sont-elles chiffrées avant leur transmission hors de l'entreprise ?		✓			

QUESTIONNAIRE DE CONTRÔLE INTERNE	Bureau Informatique	Folio 6/11

OBJECTIF DE CONTRÔLE :
B- S'assurer de la gestion de la sécurité du système informatique

B-4 : Sauvegarde et archivage des données

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	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 ?		✓			
6. Un périmètre de sauvegarde est-il défini ? -concerne t-il les données ? -les applications et logiciels ? -la fréquence de sauvegarde ?	✓ ✓ ✓ ✓				
7. La sauvegarde concerne-t-elle : - les serveurs ? - les postes individuels ?	✓	✓			

QUESTIONNAIRE DE CONTRÔLE INTERNE	Service Infrastructures de Génie Civil	Folio 7 /11

OBJECTIF DE CONTRÔLE :
C- S'assurer de la gestion de l'environnement physique

C-1 sélection du site et agencement

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Est-ce que les sites physiques où se trouve l'équipement informatique ont été choisis en fonction d'une stratégie technologique conforme aux exigences du métier ?			✓		
2. Est-ce que qu'une politique de sécurité, tenant compte notamment de la situation géographique, du voisinage, de l'infrastructure et des risques (ex : vol, température, incendie, fumée, eau, vibrations, terrorisme, vandalisme, produits chimiques, explosifs) est définie ?		✓			
3. Est-ce qu'une procédure a été définie et mise en place pour identifier les risques et menaces potentiels vis-à-vis des sites informatiques de l'entreprise et pour évaluer régulièrement l'impact métiers, en tenant compte des risques liés aux sinistres d'origine naturelle ou humaine ?		✓			
4. Est-ce que le choix et l'agencement du site tient compte des lois et réglementations applicables (normes de construction, réglementations en matière d'environnement, d'incendie, de génie électrique, de santé, hygiène et sécurité, etc.). ?	✓			Excepté l'incendie	

QUESTIONNAIRE DE CONTRÔLE INTERNE	Service Infrastructures de Génie Civil	Folio 8/11

OBJECTIF DE CONTRÔLE :
C- S'assurer de la gestion de l'environnement physique

C- 2 Mesures de sécurité physique

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Est-ce qu'une politique a été définie et mise 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. Est-ce que l'accès aux informations sur les sites informatiques sensibles et à leurs plans de conception est limité ?	✓				
3. Est-ce que les signes extérieurs et autres formes d'identification des sites informatiques sensibles sont discrets et n'identifient pas le site de façon évidente depuis l'extérieur ?	✓				
4. Est-ce que l'élaboration des mesures de sécurité physique tient compte des risques liés aux métiers et aux opérations ?		✓			
Le cas échéant, les mesures de sécurité physique incluent-t-ils :					
-des systèmes d'alarme ?		✓		Les câbles à l'extérieur des bâtiments sont enterrés ; à l'intérieur des bâtiments les câbles passent dans goulottes de protection et dans les colonnes montantes aménagées dans la structure du bâtiment technique.	
- la consolidation des bâtiments ?	✓				
- une protection des câbles ?	✓				

5. Est-ce que les mesures de prévention, de détection et de correction de la sécurité physique sont régulièrement testées pour vérifier leur conception, leur application et leur efficacité ?		✓			
6. Est-ce que la conception du site tient compte du câblage physique des télécommunications et des conduites d'eau, branchements électriques et conduites d'égout ?	✓				
7. Est-ce que les mesures de prévention, de détection et de correction de la sécurité physique sont régulièrement testées pour vérifier leur conception, leur application et leur efficacité ?		✓			
8. Un processus est-t-il mis en place pour s'assurer que les périphériques de stockage contenant des informations confidentielles sont physiquement détruits ou nettoyés ?		✓			
9. Est-ce que les sites particulièrement sensibles sont fréquemment contrôlés (y compris le week-end et pendant les congés) par le personnel de sécurité ?		✓			

QUESTIONNAIRE DE CONTRÔLE INTERNE	Service Infrastructures de Génie Civil	Folio 9/11

OBJECTIF DE CONTRÔLE :
C- S'assurer de la gestion de l'environnement physique

C-3 Accès physique

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Est-ce qu'un processus a été mis en place pour gérer les demandes et l'octroi d'accès aux infrastructures informatiques ?		✓			
2. Est-ce qu'un processus permet de journaliser et de surveiller tous les points d'accès aux sites informatiques ? et d'enregistrer tous les visiteurs, y compris les sous-traitants et les fournisseurs ?		✓			
3. Est-ce qu'un règlement impose aux visiteurs d'être accompagnés ?		✓			
4. Les individus qui ne portent pas de signe d'identification approprié sont-ils signalés au personnel de sécurité ?	✓				
5. Est-ce qu'un règlement impose au personnel de porter en permanence un signe d'identification visible ? Evite-t-on l'émission de cartes d'identification ou de badges sans autorisation appropriée?	✓ ✓			Observer si les badges sont réellement portés	
6. Est-ce que l'accès aux sites informatiques sensibles est limité par le biais d'une protection péri-métrique (ex : clôtures/murs et dispositifs de sécurité sur les portes intérieures et extérieures) ?		✓			

QUESTIONNAIRE DE CONTRÔLE INTERNE	Service Infrastructures de Génie Civil	Folio 10/11

OBJECTIF DE CONTRÔLE :
C- S'assurer de la gestion de l'environnement physique

C-4 Protection contre les risques liés à l'environnement

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Est-ce qu'un processus permet d'identifier les sinistres d'origine naturelle ou humaine qui pourraient se produire dans la zone où sont situées les infrastructures informatiques sensibles ?		✓			
2. Est-ce qu'une politique décrit comment l'équipement informatique, y compris l'équipement mobile et hors site, est protégé contre le vol et les menaces environnementales ?		✓			
3. Est-ce que les installations informatiques sont placées et fabriquées de façon à minimiser et limiter le risque de menaces environnementales ?	✓			Inspecter physiquement les locaux accueillant les sites informatiques pour s'assurer que l'agencement est approprié	
4. Est ce que les sites informatiques sont situés dans des bâtiments qui minimisent l'impact du risque environnemental (vol, air, feu, fumée, eau, vibrations, terrorisme, vandalisme, etc.) ?	✓			Les cloisons en bois accentuent le risque de feu	
5. Est-ce qu'une politique a été mise en place pour garantir un nettoyage régulier à proximité des activités informatiques ?	✓			Contrôler les sites informatiques et les salles de serveurs pour s'assurer qu'ils sont toujours propres, en ordre et sécurisés (ex : pas de désordre ni de déchets, papiers ou cartons, de poubelles pleines, ni de produits chimiques ou matières inflammables).	

QUESTIONNAIRE DE CONTRÔLE INTERNE	1- Service Infrastructures Radioélectriques 2- Bureau informatique 3- Section sauvetage et Lutte contre l'Incendie	Folio 11/11

OBJECTIF DE CONTRÔLE :
C- S'assurer de la gestion de l'environnement physique

C-5 Gestion des installations matérielles

QUESTIONS	OUI	NON	N/A	COMMENTAIRES	F.T.
1. Est-ce qu'il existe une procédure étudiant la nécessité de protéger les installations informatiques contre les conditions extérieures et les pannes de courant et incidents électriques ?	✓				
2. Est-ce que l'entreprise se procure des onduleurs ? - est-ce qu'ils répondent aux exigences de disponibilité et de continuité des activités ?	✓ ✓				
3. Est-ce que dans les installations accueillant des systèmes informatiques sensibles, plusieurs entrées d'alimentation électrique sont disponibles ?	✓				
4. Est ce que l'entrée physique du courant est séparée ?	✓				
5. Est-ce que les câbles extérieurs au site informatique sont enterrés ou disposent d'une protection adapté ?	✓			Aucun capable apparent à l'extérieur des bâtiments	

6. Est-ce qu'il existe des schémas et des plans ? -les câbles situés dans le site informatique sont-ils contenus dans des conduites sécurisées ? - les câbles sont-ils renforcés et protégés contre les risques environnementaux ? - le câblage et la connexion physique (données et téléphone) 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 des sites informatiques est effectuée selon les spécifications et la périodicité recommandées par les fournisseurs ?		✓		Uniquement pour les serveurs et les applications du réseau opérationnel, maintenance effectuée par le fournisseur COROBOR Système.	
8. Est-ce que la maintenance est uniquement effectuée par le personnel autorisé ?		✓			
9. Est-ce qu'un processus a été mis en place pour informer le personnel sur les exercices d'évacuation en cas d'incendie et les exercices de secours, pour que tous les employés sachent quoi faire en cas d'incendie ou d'incident similaire ?		✓			

Source : Nous même, d'après les Approches de CLEUET & al, AFAI, ISACA et COBIT.

BIBLIOGRAPHIE

Ouvrages

1. ACISSI (2009), *Sécurité informatique: ethical hacking, apprendre l'attaque pour mieux se défendre,* Editions ENI, Paris, 355 pages.
2. AFAI (2008), *Cobit 4.1.,* IT Governance Institute, Paris, 196 pages.
3. AFAI (2008), *Guide d'Audit des Systèmes d'Information: Utilisation de Cobit,* IT Governance Institute, Paris 269 pages.
4. ASECNA (2008), *Manuel des emplois de l'ASECNA, Volume I : Représentation,* Dakar.
5. ASECNA (2008), *Rapport d'activité,* Cabinet du Directeur Général de l'ASECNA, Dakar, 105 pages.
6. BUTEL, Annie (2008), *Continuité d'Activité: Plan de secours,* CLUSIF / BNP PARIBAS, Paris 33 pages.
7. CALE, Stéphane et TOUITOU, Philippe (2007), *La sécurité informatique: réponses techniques, organisationnelles et juridiques.* Lavoissier, Paris, 282 pages.
8. CARPENTIER, Jean-François (2009), *La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques,* Editions ENI, Paris 277 pages.
9. CLEUET, Fabien, et al. (2008), *Audit des systèmes d'information,* Vol.1 (2) INTEC/CNAM, Paris, 162 pages.
10. CLEUET, Fabien, et al. (2008), *Audit des systèmes d'information,* Vol.2 (2) INTEC/CNAM, Paris, 152 pages.
11. CLUSIF (2010), *Menaces Informatiques et Pratiques de Sécurité en France,* Edition 2010, CLUSIF, Paris, 102 pages.
12. CLUSIF (2010), *MEHARI 2010: Manuel de référence de la base de connaissance Méhari 2010,* CLUSIF, Paris, 16 Pages.
13. CLUSIF (2003), *Plan de Continuité d'Activité. Stratégie et solutions de secours du S.I.* Dossier Technique, CLUSIF / COMMISSION TECHNIQUE DE SECURITE LOGIQUE, Paris, 58 pages.

14. DAYAN, Armand, et al. (2008), *Manuel de gestion Vol.1,* 2e édition, ELLIPSES/AUF, Paris 1088 pages.

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

16. GRAEVE, Jean de et POTIER, Jean (2001), *Système d'information, Management et Acteurs,* Les éditions SAPIENTIA, Paris, 135 pages.

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

18. IFACI (2009), *Normes,* The Institute of Internal Auditors, Paris, 66 pages.

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

20. LY, Henri (2005), *L'audit technique informatique,* LAVOISIER / HERMES SCIENCE, Paris, 230 Pages.

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

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

23. REIX, Robert (2005), *Systèmes d'informations et management des organisation,.* 5e édition, : LIBRAIRIE VUIBERT, Paris, 486 pages.

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

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

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

27. THORIN, Marc (2000), *L'audit informatique,* HERMES SCIENCE, Paris, 184 Pages.

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

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

Articles

30. 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.

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

Sources Internet

32. ANSSI (2007), Politiques de sécurité des systèmes d'information (PSSI). *Sécurité-info,* [En ligne] 20 Décembre 2007. [Citation : 15 Aout 2010.], http://www.securite-informatique.gouv.fr/gp_article51.html.

33. CLUSIF (2010), *www.clusif.asso.fr.* [En ligne] [Citation : 29 aout 2010.], http://www.clusif.asso.fr/fr/production/mehari/.

34. EFFI Soft (2010), Glossaire, *effisoft-consulting.com.* [En ligne] [Citation : 18 Aout 2010.] http://www.effisoft-consulting.com/Pages/Glossaire/Glossaire.aspx.

35. EOX PARTNERS SAS (2009), Charte informatique et Politique de sécurité. *Eoxpartners.fr,* [En ligne] 2009. [Citation : 11 aout 2010.] http://www.eoxpartners.fr/charte_informatique_politique-securite-eox_partners.php.

36. GUARDIAN-SOFT (2010), *www.guardian-soft.be.* [En ligne] [Citation : 8 Aout 2010.] http://www.guardian-soft.be/mat%C3%A9riels_&_solutions.htm.

37. GUIDE-INFORMATIQUE (2010), Sécurité des informations, normes BS 7799, ISO 17799, ISO 27001, EBIOS, MEHARI. *www.guideinformatique.com.* [En ligne] [Citation : 2 Septembre 2010.], http://www.guideinformatique.com/fiche-securite_des_informations-441.htm.

38. LESSAUVEGARDES(2007), Construire son plan de sauvegarde, [En ligne] 15 octobre 2007. [Citation : 16 Aout 2010.], http://www.lessauvegardes.com/lscom/2007/10/15/construire-son-plan-de-sauvegarde/.

39. PILLOU, Jean-François (2010), Mise en place d'une politique de sécurité. *Linux Plus-Value.* [En ligne] [Citation : 15 aout 2010.], http://www.linuxplusvalue.be/mylpv.php?id=184.

40. SOCIETE DE MARKETING INDUSTRIEL (2010), Sécuirté: Eviter aussi les risques physiques, *ACHETEURS INFO.COM.* [En ligne] [Citation : 10 aout 2010.], http://www.acheteursinfo.com/actualites_securite.html.

41. SUPRALOGIC SARL (2010), Politique de sécurité, *Supralogic.com.* [En ligne] [Citation : 15 Aout 2010.] http://www.supralogic.com/docs/politique_securite.htm.