Centre Africain d'études Supérieures en Gestion

CESAG

CESAG EXECUTIVE EDUCATION (CEE)

MBA Audit et Contrôle de Gestion

Promotion 27

(2015 – 2016)

Mémoire de fin d'études

THEME

AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION :

CAS DE L'HOPTILAL GENERAL DE GRAND YOFF (HOGGY)

Présenté par :

YAO Koffi Innocent

Dirigé par :

M. N'TSOUGAN Koffi

Professeur associé au CESAG

Octobre 2016

DEDICACE

Nous dédions ce mémoire à

- ✓ l'Eternel tout puissant pour son amour et sa grâce toujours renouvelée ;
- ✓ ma mère DJEZOU N'dri Catherine et ma tante Mme DIBY Odile pour leur soutien affectif, spirituel et financier inestimable ;
- ✓ mes sœurs KOUAME Félicite, YAO Brigitte, YAO Angeline, YAO Eudoxie, YAO Natacha et YAO Daniel pour leurs prières et toute la confiance placée en moi.

REMERCIEMENTS

Nos remerciements les plus sincères vont à l'endroit de :

- ✓ Docteur CHABI, chef de département CESAG EXECUTIVE, pour sa disponibilité, son encadrement et ses conseils avisés ;
- ✓ M. N'TSOUGAN Koffi Medouwodji, notre Directeur de mémoire, pour ses remarques et observations pertinentes et surtout pour sa disponibilité ;
- ✓ M. Jacob DIOP, contrôleur de Gestion à l'HOGGY pour sa disponibilité et ses conseils.
- ✓ M. Alioune DIOUF, informaticien à l'HOGGY pour sa disponibilité et sa collaboration.
- ✓ M. Narcisse NZI, notre cousin et tuteur à Dakar pour son accueil, ses conseils et son soutien tout au long de mon séjour ;
- ✓ Messieurs EMMANUEL SIALOU et MAXIM SIALLOU pour leur confiance sans cesse renouvelée ;
- ✓ ROSTAND N'GUESSAN, MICHAEL YORAGON, nos voisins de chambre pour la cohabitation pacifique ;
- ✓ la famille source de vie du CESAG, pour le soutien spirituel ;
- ✓ toute la promotion MBA ACG 2015-2016 avec à sa tête ARMAND COULIBALY pour tous les bons moments passés ensemble et pour le partage d'expérience ;
- ✓ L'association des Ivoiriens du CESAG.

LISTE DES SIGLES ET ABREVIATIONS

A : Ampère

ACP : Agence Comptable Particulière ;

AI : Acquérir et Implémenter ;

ANSSI Agence Nationale de la Sécurité des Systèmes d'information ;

CHAI : Comité d'Harmonisation de d'Audit Interne

CIGREF : Club Informatique des Grandes Entreprises de France.

CME : Commission Médicale d'Etablissement

CMMI : Capacity Maturity Model Integration

CNTS : Centre National de Transfusion Sanguine

COBIT: Control Objectives for Information and related Technology;

COSO: Committee Of Sponsoring Organizations of the Treadway Commission.

CTE : Comité Technique d'Etablissement

CTO : Centre de Traumatologie et d'orthopédie

DS : Délivrer et Supporter ;

DSSI : Direction de la Sécurité du Système d'Information

EDI : Electronic Data Interchange

EPS : Etablissement Publique de Santé

ERP : Enterprise Ressources Planning

FRAP : Feuille de Révélation et d'Analyse de Problèmes

HOGGY : Hôpital Général de Grand Yoff

IB : Initiative de Bamako

IFACI : Institut Français des Auditeurs et Contrôleurs Internes

IIA: Institute of Internal Auditors

ISACA: Information Systems Audit and Control Association

ISO: International Standardization Organization

ITIL: Information Technology Infrastructure Library

KVA: KiloVoltAmpère

KW: KiloWatt

NSA: National Security Agency

ORL : Oto-Rhino Laryngologie

PO : Planifier et Organiser ;

QCI : Questionnaire de Contrôle Interne ;

RSSI Responsable de la sécurité du système d'information

SAP: Systems, Applications and Products for data processing;

SE : Surveiller et Evaluer ;

SENELEC : SENegal ELECtricité (Société nationale d'électricité du Sénégal)

SI : Système d'Information

SIH : Système d'Information Hospitalière

SSI : Sécurité du Système d'Information

UCAD : Université Cheikh Anta Diop

LISTE DES TABLEAUX ET FIGURES

- **LISTE DES TABLEAUX**

- **LISTE DES FIGURES**

LISTE DES ANNEXES

SOMMAIRE

INTRODUCTION GENERALE

Les fuites survenues au mois d'avril 2016 de plus de 11,5 millions de documents confidentiels issus du cabinet d'avocats panaméen Mossack Fonseca, détaillant des informations sur plus de 214 000 sociétés offshores ainsi que les noms des actionnaires de ces sociétés et les différents scandales qui y ont suivis (démission du premier ministre islandais, démission du ministre espagnol de l'industrie et son retrait définitif de la vie politique) ont montré comment l'information est sensible et, comment sa divulgation pourrait entrainer des problèmes de tous ordres (image écornée, perte de réputation, pertes financières…)

Sa sauvegarde et sa protection s'avèrent plus que nécessaire pour les organisations. De nos jours, du fait de multiples interconnexions, l'information est de plus en plus exposée et vulnérable.

L'information se présente sur des supports variés. Elle peut être disponible sur papier, stockée électroniquement, transmise par voie postale ou électronique, diffusée sur des supports audiovisuels ou verbalement. Quel que soit le support ou le moyen utilisé pour la partager ou la stocker, il convient de toujours protéger l'information de manière adaptée.

La sécurité de l'information vise à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des transactions, à réduire le plus possible le risque et à optimiser le retour sur investissement ainsi que les opportunités en terme d'activité pour l'organisme.

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Ces mesures doivent être spécifiées, mises en œuvre, suivies, réexaminées et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'un organisme. Pour ce faire, il convient d'agir de manière concertée avec les autres processus de gestion.

La sécurité du système d'information se définit quant à elle comme la structure de contrôle mise en place dans le but de protéger l'intégrité, la confidentialité et la disponibilité des ressources et des données. Avec le développement des nouvelles technologies de ces dernières décennies qui ont permis une plus grande rapidité dans le traitement de l'information et une plus grande capacité de stockage, la majorité des organismes en

dépend. Ce développement de la technologie s'accompagne toutefois de nouvelles menaces pour l'organisation. : Perte de service, vol ou fuite d'informations, panne d'origine interne…

Pour faire face à ces menaces, les organisations en commençant par les Etat**s,** se sont dotées d'instruments dont la mission est d'assurer la sécurité de l'information. Il s'agit entre autres de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour la France et de la National Security Agency (NSA) pour les Etats-Unis.

Les autres organisations, notamment celles du secteur privé ne sont pas en reste**.** En effet, la norme ISO 27001:2013 concernant la Sécurité du Système d'information (SSI) oblige l'évaluation des conséquences telles que : la perte de confidentialité, de disponibilité ou d'intégrité.

Tous ces risques et leur gestion sont présents à l'HOGGY (Hôpital General de Grand Yoff). Ces risques s'expliquent par le nombre élevé d'informations provenant de ses différents services, ses fournisseurs que l'HOGGY doit traiter quotidiennement et dont elle doit maintenir l'intégrité, la confidentialité et la disponibilité. Par conséquent la nécessité de disposer d'un système d'information fiable et sécurisé reste une préoccupation majeure pour l'HOGGY et l'une des difficultés généralement rencontrées est la maitrise des risques liés à ce système d'information.

Malgré les conséquences auxquelles est exposé l'HOGGY, nous avons constaté lors de notre stage dans ladite structure qu'aucun audit de la sécurité du système d'information n'y avait jamais été fait afin d'identifier et évaluer les risques liés au système d'information. L'analyse de ce problème nous a conduit à déterminer les causes suivantes :

- ✓ l'absence de politique formalisée en matière de sécurité du système d'information ;
- ✓ le département d'audit interne n'est pas suffisamment outillé pour identifier et évaluer les risques liés au Système d'information ;
- ✓ la méconnaissance du rôle et de la responsabilité des auditeurs internes dans la maitrise des risques liés au système d'information ;
- ✓ le coût relativement élevé de l'audit de la sécurité du système d'information.

Les conséquences de ce problème sont entre autres :

- ✓ la non maitrise des risques liés au système d'information ; ce qui peut impacter de façon négative les activités de l'hôpital ;
- ✓ l'élaboration incomplète d'une cartographie des risques sur laquelle se basent les auditeurs internes pour la programmation de leur mission d'audit ;
- ✓ l'accès non autorisé d'agents étrangers aux informations violant la confidentialité de celles-ci ;
- ✓ la violation du principe de séparation des tâches incompatibles ;
- ✓ la perte de crédibilité de l'information financière et comptable.

Après analyse du problème, nous pensons que les mesures correctives suivantes peuvent être prises :

- ✓ tenir compte de la politique de sécurité du système d'information dans la politique globale de l'hôpital ;
- ✓ développer ou acquérir des capacités en audit des Systèmes d'Information, les intégrer au service d'audit interne de l'hôpital ;
- ✓ intégrer la dimension culture du risque lié au système d'information dans l'élaboration de la cartographie ;
- ✓ auditer la sécurité du système d'information de l'hôpital général de grand Yoff.

Une seule solution retiendra notre attention pour cette étude à savoir : auditer la sécurité du système d'information, car de par le niveau d'exposition aux risques liés aux SI que l'audit nous présentera, nous pourrons formuler des recommandations afin de garantir la disponibilité, l'intégrité et la confidentialité des données.

Notre audit nous permettra donc de répondre à la question fondamentale qui est : quel est le niveau de vulnérabilité aux risques du système d'information de l'hôpital général de grand Yoff ?

De cette question fondamentale découlent d'autres plus spécifiques :

- ✓ Qu'est-ce que le système d'information ?
- ✓ Quelles en sont ses composantes ?
- ✓ Quelles sont les risques liés au système d'information ?
- ✓ Qu'est-ce que la sécurité du système d'information ?

- ✓ Comment l'hôpital général de grand Yoff assure-t-il la sécurité de son système d'information ?
- ✓ Quel est niveau de vulnérabilité du système d'information de l'HOGGY ?
- ✓ Quels axes d'amélioration pourrions-nous proposer pour aider l'hôpital à renforcer son dispositif de sécurité ?

Nous essayerons de répondre à toutes ces questions à travers l'étude du thème suivant : A**udit de la sécurité du système d'information : cas de l'hôpital général de grand Yoff.**

Notre objectif principal par cette étude est d'appréhender le niveau de vulnérabilité de l'hôpital. Cet objectif principal est accompagné par d'autres plus spécifiques que sont :

- ✓ d'appréhender les notions de système d'information et de sécurité du système d'information ;
- ✓ présenter les risques liés au système d'information ;
- ✓ dérouler les différentes étapes d'un audit des systèmes d'information ;
- ✓ identifier les contrôles et les dispositifs mis en place par l'HOGGY et vérifier leur conformité par rapport aux lois, règlements et bonnes pratiques en la matière ;
- ✓ analyser ce dispositif pour en dégager ses forces et ses faiblesses
- ✓ formuler des recommandations au regard des faiblesses relevées.

Compte tenu du champ très vaste de l'audit de la sécurité des systèmes d'information, nous nous limiterons aux aspects fonctionnels et organisationnels.

Cette étude revêt un double intérêt.

Premièrement pour l'entreprise, elle permettra de montrer aux dirigeants de l'entité le niveau de vulnérabilité aux risques et de formuler des recommandations pour leur permettre de prendre des mesures idoines pour y remédier.

Deuxièmement pour nous même, ce travail nous permettra d'approfondir nos connaissances jusque-là théoriques en matière d'audit de la sécurité des systèmes d'information.

Pour atteindre les objectifs que nous nous sommes fixés, notre étude se fera en deux grandes parties.

- ✓ la première partie consacrée à la littérature consistera à présenter les notions de système d'information, de risques (chapitre 1), la méthodologie de recherche et la présentation de l'hôpital général de grand Yoff (chapitre 2).
- ✓ la seconde partie porte sur la description du système d'information actuel de l'HOGGY (chapitre 3) et enfin nous présenterons et analyserons les résultats de notre audit (chapitre 4).

PARTIE I : CADRE THEORIQUE

Introduction de la première partie

De nos jours, avec la concurrence rude que se mènent les entreprises, une information mal maitrisée, diffusée en temps inopportun, un arrêt inattendu des outils de traitement de ces données peut avoir des conséquences désastreuses. De plus en plus, le traitement de ces données se fait automatiquement et s'accompagne de nouveaux risques qui sont souvent méconnus. La question donc de système d'information et de sa sécurité se pose avec acuité dans toute structure.

De ce fait, sa gestion doit être la plus optimale pour l'atteinte des objectifs. Mais force est de constater que ce sujet demeure mal maitrisé par bon nombre d'acteurs de l'entreprise.

Il nous parait dès lors nécessaire dans cette première partie de consacrer le premier chapitre au concept de système d'information et, le second chapitre quant à lui exposera la méthodologie de recherche et la présentation de l'hôpital général de grand Yoff.

Chapitre 1 : Sécurité du système d'information

Le système d'information est au cœur du fonctionnement des activités de l'entreprise, son fonctionnement, les risques auxquels il est exposé et leur gestion feront l'objet de notre étude au cours de ce chapitre.

1.1 Système d'information et gestion des risques

Selon Graeve et Poitier (2001 : 3) « le système d'information peut être considéré comme la moelle épinière de l'entreprise, de même que le pilotage en est le cerveau et que le système opérant en est les membres **».**

Une telle notion mérite donc une attention particulière c'est pourquoi nous lui consacrerons cette section.

1.1.1 Système d'information

Reix (2007 : 1) définit le système d'information comme « un ensemble de ressources affectées à des fonctions d'acquisition, de stockage, de traitement et de diffusion de l'information ». Quant à Alter (1996 : 2) un système d'information est un système qui utilise des technologies de l'information pour saisir, transmettre, structurer, retrouver, manipuler ou afficher l'information utilisée dans un ou plusieurs processus de gestion.

Nous pouvons alors dire que le système d'information est une combinaison de technologies de l'information **(**langages de programmation, logiciels, serveurs, bases de données, des télécommunications et réseaux, ordinateurs individuels, téléphones mobiles…) et d'activités humaines utilisant ces technologies en support des opérations, du management et de la prise de décision.

1.1.1.1 Composants du système d'information

Selon Deyrieux (2004 :10) le système d'information de l'entreprise comprend : l'ensemble des informations, formalisables ou non, structurées ou non, accessibles par les agents de l'entreprise, les process de création, de recherche, d'organisation, de conservation, de traitement, de diffusion des informations, les moyens mis en œuvre pour assurer ces process, notamment les systèmes informatiques et les systèmes de communication.

Autrement dit, nous pouvons identifier les données, les hommes qui gèrent les process et le système informatique qui comporte une partie logicielle et une partie matérielle.

1.1.1.1.1 Les données

Gillet (2011 : 60) définit une donnée comme : « un élément d'information externe au système d'information de l'organisation, pertinent pour gérer un processus métier et qui se retrouvera le plus souvent intégré dans les indicateurs décisionnels ». Pour aboutir à ce résultat, les données doivent être collectées dans le système d'information, ce qui peut se faire manuellement par saisie ou par des procédés d'acquisitions automatiques.

Obtenir une bonne qualité des données est donc essentiel. Les procédés d'acquisition automatique (lecture de codes à barres, EDI…) permettent de rendre la collecte plus productive et plus fiable.

1.1.1.1.2 Les personnes

On peut identifier deux types de personnes : les utilisateurs du système à savoir les cadres et employés de l'organisation d'une part et d'autre part, les spécialistes de sa construction (analystes, programmeurs dont le travail consiste à concevoir, à implanter les bases technologiques du système et à assurer son fonctionnement. L'homme est au début et à la fin du système d'information. C'est pourquoi Reix & al. (2011 : 4) dit : « qu'il ne peut y avoir de système d'information sans les personnes ».

1.1.1.1.3 Le matériel

Monaco (2014 : 18) le définit comme « le dispositif physique composé de photocopieurs, de scanners, d'ordinateurs, d'autres moyens de communication plus ou moins techniques qui permettent de recevoir, d'émettre et de manipuler les informations » Ce matériel est un support pour les données et les logiciels et un outil de travail pour les personnes dans le traitement des données.

1.1.1.1.4 Les logiciels

Un logiciel est un ensemble de programmes agrégés permettant de répondre à un besoin de gestion d'un ensemble de processus (Gillet, 2011 : 128).

On fait souvent l'amalgame entre un logiciel et un programme. Un programme peut être un logiciel, dans le cas où le logiciel est constitué d'un seul programme, mais souvent le logiciel est constitué de plusieurs programmes. Ces logiciels vont permettre aux ordinateurs de fonctionner et commander le traitement automatisé des données.

1.1.1.2 Système d'information et système informatique

Il est important de distinguer les deux systèmes, car les rôles et les responsabilités liés à chacun d'entre eux ne sont pas les mêmes c'est ce que soutient Pesenti (2011 : 1). Pour lui : le système informatique est l'ensemble des actifs matériels et logiciels de l'entreprise ayant pour vocation à automatiser le traitement de l'information. C'est la partie visible à laquelle tout le monde pense quand on parle de projets et d'infrastructures informatiques. Ce sont entre autres les logiciels, les serveurs, les écrans, etc. alors que le système d'information est l'ensemble des actifs du système informatique (matériels et logiciels) mais comprend aussi et surtout, les actifs humains et immatériels, les procédés, procédures, et processus.

Pour Gillet (2010 : 45) c'est une relation de demande et d'offre qui existe entre le système d'information et le système informatique ; ainsi le système d'information est le maître d'ouvrage qui exprime des besoins qui sont satisfaits par l'offre du système informatique qui est le maitre d'œuvre.

En un mot le système informatique est un sous-système du système d'information qui lui sert de support technique. Cette confusion entre les deux termes s'est installée du fait de l'importance croissante de l'utilisation quasi systématique de l'informatique dans le traitement des données.

1.1.1.3 Le système d'information d'aujourd'hui : LES ERP

Il existe un grand nombre de définitions des ERP, vu sous différents angles mais celles présentées ci-dessous entrent plus dans le cadre de notre étude.

En effet d'après Tomas (2007 : 11) le progiciel de gestion intégré ou ERP (Enterprise Ressource Planning) est un ensemble de modules applicatifs généralement signés par un même éditeur et travaillant en mode natif sur une base de données unique, au sens logique

du terme (même si celle-ci est géographiquement distribuée sur un réseau). Fonctionnellement, ces modules couvrent :

- ✓ la gestion comptable et financière ;
- ✓ la gestion de la trésorerie ;
- ✓ le contrôle gestion ;
- ✓ la gestion de production ;
- ✓ la gestion des achats et des stocks ;
- ✓ l'administration des ventes ;
- ✓ la logistique ;
- ✓ la paie.

Pour Deixonne (2006 :10), l'ERP désigne « une application informatique qui permet à une entreprise de gérer et d'optimiser l'ensemble de ses ressources. La valeur ajoutée d'un ERP et sa différence, par rapport aux autres applications sont derrière le mot intégration ».

Pour Giard (2003 :24) les ERP sont « des progiciels de gestion intégrés qui visent à gérer de manière efficace l'ensemble des ressources de l'entreprise ». Ils proposent une architecture modulaire permettant de composer à la carte un système sur mesure, en s'appuyant sur une base de données relationnelles et une base de processus adaptable aux spécificités du pays (langue, règlementation) et de l'entreprise (métiers, procédures).

Les applications sont caractérisées par le fait d'être modulaires et intégrées. En fait, un progiciel ERP complet peut tenir compte d'une grande partie ou de tous les aspects des fonctions de gestion d'une entreprise. Il peut même dépasser ses aspects internes pour gérer les relations de l'entreprise avec ses fournisseurs, ses clients et ses partenaires comme le souligne Deixonne (2011 :15). Il a pour objet de relier entre elles les différentes fonctions et les différentes activités de l'entreprise, dans le but de coordonner et synchroniser leur fonctionnement, à l'aide de processus plus ou moins automatisés. Reposant sur un système d'information centralisé mais le plus accessible, il doit permettre de croître en efficacité tout en réduisant les coûts de traitement de l'information.

Ces ERP se sont imposés aux entreprises du fait de la multiplicité des applications dont elles devaient gérer et faire communiquer pour le traitement des informations. Cependant ces applications étant développées dans différents langages informatiques, elles avaient du

mal à communiquer. Ce disfonctionnement a donc conduit les développeurs d'application à mettre en place une solution plus optimale d'où la naissance des ERP (Deixonne, 2006 :11).

1.1.2 Gestion des Risques

La gestion du risque s'attache à identifier les risques, c'est-à-dire les pertes potentielles et quantifiables, inhérentes à une situation ou à une activité, associée à l'occurrence d'un événement. Cette prévention des risques aboutit à établir une grille des risques avec des veilles correspondant à chaque type de risque, et des contre-mesures adaptées.

1.1.2.1 Notion de risque

L'IFACI définit le risque comme étant « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maitrise » (Renard, 2013 : 137).

Le risque résulte donc de toute situation, évènement, comportement susceptible de provoquer un dommage à l'organisation et/ou de l'empêcher de réaliser ses objectifs ou de maximiser ses performances ou encore de saisir une opportunité. Se référant à la sécurité du système d'information, le risque serait la possibilité qu'une menace donnée exploite une ou plusieurs vulnérabilités d'un actif ou d'un groupe actifs et ainsi cause un préjudice à l'organisation (ISACA, 2013 :74).

C'est sur cette dernière définition que portera tout particulièrement notre attention pour la suite de notre étude.

1.1.2.2 Identification des risques

Ce paragraphe fera l'objet de la présentation des différentes techniques d'identification des risques au sein d'une organisation. Le choix sera fait selon l'objectif poursuivi par l'organisation.

Les techniques d'identifications des risques sont les suivantes :

- ✓ l'identification par processus : l'objectif de cette approche est la description des processus mis en œuvre dans l'entreprise et par celles des activités liées entre elles par des échanges de produits ou d'informations, et contribuant à la fourniture d'une même prestation à un client interne ou externe de l'entreprise (Nguena, 2008 :66) ;
- ✓ l'identification par tableau de risque : elle consiste à un découpage de l'activité (ou du processus) en tâches élémentaires, ce qui permet un recensement des risques en fonction des objectifs (Renard, 2010 :236) ;
- ✓ l'identification basée sur les actifs créateurs de valeurs : elle met au premier plan les actifs créateurs de valeurs comme le client dans une entreprise commerciale, et de procéder à l'identification affectant les autres actifs (Maders & al, 2006 :51) ;
- ✓ l'identification par l'analyse historique : elle est caractérisée par l'utilisation des bases de données des risques rencontrées par l'entreprise antérieurement (Jiménez & al, 2008 : 164) ;
- ✓ l'identification par l'analyse de l'environnement : elle se fait en fonction des variations que peut subir l'environnement dans lequel est implantée l'entreprise (COSO II, 2009 :67) ;
- ✓ l'approche Botton-up : également appelée ascendante, cette méthode consiste à identifier les risques par les opérateurs qui sont impliqués dans le processus. Elle part de l'évaluation des détails des risques par causes, objectifs de risques, conséquences, par processus dans chaque activité, pour décrire la situation des risques de l'entreprise (Verel & al, 2005 ; 136) ;
- ✓ l'approche top-down : ou encore approche descendante ; elle consiste à la mise en place par le risk manager et son équipe qui sont chargés de détecter les risques et de les soumettre ensuite aux opérationnels pour qu'ils émettent leur avis (Jimenez & al, 2008,63) ;

1.1.2.3 Les risques liés au système d'information

Darsa (2014 : 178-203), met en évidence les différents risques auxquels les entreprises sont régulièrement exposées**.** Il y consacre une partie importante aux risques liés au système d'information parmi lesquels nous avons retenu cette liste non exhaustive. Ces risques sont les suivants :

- ✓ l'arrêt de maintenance des logiciels, par la disparition du fournisseur concepteur de la solution qui peut être défini comme l'arrêt temporaire ou permanente d'évolutivité ou de tierce maintenance applicative des solutions déployées par défaillance du fournisseur ou du prestataire en charge. Ce risque a pour cause l'indisponibilité ou le déficit de compétences ou de connaissance du mainteneur, la défaillance financière du prestataire, la technologie, un langage hybride ou atypique non maintenu, spécificités techniques ou logicielles non repliables ou non évolutives, une gestion de la connaissance ou de la documentation applicable (technique et fonctionnelle) inappropriée. Il a pour conséquence : l'impossibilité d'évolution, de développement ou de maintenance corrective des applications et solutions logicielles de l'entreprise, stagnation ou régression des outils utilisés, risques opérationnels, économiques et financiers, risques d'image ;
- ✓ le blocage du centre informatique ou des locaux métiers défini comme l'incapacité des sites centraux par inaccessibilité des locaux opérationnels. Il a pour causes des risques environnementaux (les séismes, les inondations, la pollution), les risques sociaux (mouvement social), les risques d'infrastructures (rupture d'énergie, réseaux télécom…). Les conséquences sont l'indisponibilité temporaire ou permanente des outils, infrastructures, solutions ou données informatiques nécessaires à l'exploitation de l'entreprise, risques économique et financier ;
- ✓ l'accident naturel : altération de l'intégrité physique des matériels informatiques (serveurs, switch, réseaux PC, portable) par désastre naturel de toute nature ; les causes sont l'absence de sécurisation des sites de dépôt, de stockage ou d'exploitation des matériels informatiques, la non prise en compte des risques naturels en présence**,** les principales conséquences sont la dégradation, la destruction ou l'endommagement des actifs informatiques de l'entreprise, l'indisponibilité d'outils de traitement des données, la perte d'informations, des risques économiques et financiers ;
- ✓ le vandalisme (sans intrusion) **:** altération de l'intégrité physique des matériels informatiques par vandalisme sans intrusion dans les locaux (virus). Les différentes causes sont l'inefficacité des solutions de protection des applications, des données et des infrastructures informatiques de l'entreprise, attaque virale, actualisation insuffisante des solutions sécuritaires informatiques en présence ;
- ✓ le vandalisme (avec intrusion) **:** altération de l'intégrité physique des matériels informatiques par vandalisme avec intrusion dans les locaux (vol, destruction,

dégradation) qui a pour causes l'inefficacité des solutions de protection et des sites, des infrastructures**,** des équipements et des données informatiques de l'entreprise. Pour conséquences l'indisponibilité des outils, applications, données informatiques de l'entreprises, risques économiques et financiers, risques d'image et de dégradation de la satisfaction client ;

- ✓ le vol d'équipement qui a pour conséquences des pertes économiques et financières, des pertes de données ;
- ✓ le vol d'informations et de données qui a pour causes la sécurisation insuffisante ou inappropriée des réseaux et/ou des données informatiques de l'entreprise et des erreurs humaines. Pour conséquences nous avons des pertes de données sensibles, des pertes d'avantages concurrentiels, des risques commerciaux, économiques, financiers ;
- ✓ la destruction volontaire d'informations ou de données **:** le**s** causes sont la malveillance, des erreurs humaines, des outils ou applications inadaptées. Pour conséquences on a des pertes de données sensibles, opérationnelles, comptables, économiques ou financières, risque d'image, insatisfaction client ;
- ✓ modification volontaire d'information ou de données qui a pour cause des malveillances, des erreurs humaines.

L'entreprise est également soumise à d'autres risques liés au système d'information.

Au niveau de la sécurité nous avons : les intrusions dans les systèmes, le détournement d'un site, le détournement d'un service vendu, la divulgation de données confidentielles, les virus informatiques, l'abus de pouvoir par une maintenance externe, la perturbation des services rendus, l'écoute d'information sur le réseau.

Au niveau de l'exploitation les risques suivants sont régulièrement rencontrés : l'altération accidentelle des données par l'exploitation, le dysfonctionnement du matériel, le dysfonctionnement d'un logiciel, le dysfonctionnement d'un service externe, des erreurs de saisie.

1.1.2.4 Gestion des risques liés au système d'information

Cigref & al. (2009 : 43-50) préconisent un certain nombre de bonnes pratiques pour le management des risques informatiques. Elles se regroupent en huit points sous la responsabilité de la Direction de la Sécurité du Système d'Information :

- ✓ elle pilote la gestion des risques informatiques en prenant en compte le cadre global de la gestion des risques de l'entreprise ;
- ✓ elle procède à une identification des risques informatiques partagée avec les « métiers » en prenant en compte les enjeux majeurs des métiers ;
- ✓ elle procède à une évaluation des risques partagée avec les « métiers » en prenant en compte les applications et les données « métiers » clés ;
- ✓ elle met en œuvre les contrôles sur les processus informatiques afin de réduire le risque à un niveau acceptable en liaison avec les contraintes des « métiers » ;
- ✓ elle prend en compte les contrôles embarqués dans les applications en relation avec le métier ;
- ✓ elle réalise une évaluation régulière de l'efficacité des contrôles SI ;
- ✓ elle doit être capable de réagir efficacement et dans les délais à des incidents majeurs avec un impact significatif pour le « métier » ;
- ✓ dans le cadre du pilotage des risques au niveau de l'entreprise, la DSSI communique au management un reporting régulier des risques pour lui donner une véritable connaissance des risques SI auxquels est exposée l'entreprise, et pour lui permettre de prendre des décisions appropriées dans les délais.

1.2. Sécurité du Système d'Information et normes de système d'information

Cette section sera consacrée à la notion de sécurité du système d'information et aux normes et standards qui gouvernent les systèmes d'information.

1.2.1 Sécurité du système d'information

La sécurité du système d'information est définie comme « la structure de contrôle mise en place dans une organisation dans le but de protéger l'intégrité, la confidentialité et la disponibilité des ressources et des données de ce système » (IFACI, 1993 : 8).

Pour Reix (2002 : 416) la sécurité du système d'information est sa non vulnérabilité à des accidents ou attaques volontaires, c'est-à-dire l'impossibilité que ces agressions produisent des conséquences graves sur l'état du système ou son fonctionnement.

Les risques pouvant compromettre l'intégrité, la confidentialité et la disponibilité des données sont légions et variés. Pour faire face à ce problème la Top management des entreprises doit mettre en place une politique pour la sécurité du système d'information en vue de réduire la probabilité et la gravité desdits risques.

1.2.1.1 Objectif de la sécurité du Système d'information

Thorin (2000 :45) disait qu'un audit n'a de sens que si sa finalité est définie quel que soit le type d'audit notamment l'audit de la sécurité du SI. Cette finalité est de porter un jugement sur le management du SI et de l'existence des objectifs.

La sécurité des SI a pour objet de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Elle va se traduire par la diminution de la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et délais acceptables en cas de sinistre. La sécurité ne permet pas de gagner de l'argent mais évite d'en perdre.

Selon ISO 27002 :2013, la sécurité du système d'information doit assurer les propriétés suivantes :

- ✓ la confidentialité (aucun accès illicite) : maintien du secret de l'information et accès aux seules entités autorisées ;
- ✓ l'intégrité (aucune falsification) : maintien intégral et sans altération de l'information ;
- ✓ l'exactitude (aucune erreur) ;
- ✓ la disponibilité (aucun retard) : maintien de l'accessoiriste en continu sans interruption ni dégradation ;
- ✓ la non répudiation (aucune contestation).

1.2.1.2 Politique de sécurité du SI

La norme de bonne pratique de sécurité du système d'information ISO 27002 : 2013 définit la politique du système d'information comme l'engagement de la direction à définir une approche de l'organisme pour gérer la sécurité de l'information contenu dans un document qui contient :

- ✓ une définition de la sécurité de l'information, les objectifs généraux recherchés et le domaine d'application retenu, ainsi que l'importance de la sécurité en tant que mécanisme nécessaire au partage de l'information ;
- ✓ une déclaration des intentions de la direction soutenant les objectifs et principes de la sécurité de l'information, en conformité avec la stratégie et les objectifs de l'organisme ;
- ✓ une démarche de définition des objectifs de sécurité et des mesures, intégrant l'appréciation et le management du risque ;
- ✓ une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour l'organisme, à savoir les éléments suivants :

    - la conformité avec les exigences légales, réglementaires et contractuelles ;
    - les exigences en termes de formation et de sensibilisation en matière de sécurité;
    - la gestion de la continuité de l'activité ;
    - les conséquences des violations de la sécurité de l'information ;
    - une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'incidents de sécurité ;

- ✓ des références à la documentation susceptible d'appuyer la politique et devant être respectée, par exemple des politiques et des procédures de sécurité plus détaillées ou des règles de sécurité devant être respectées par les usagers. Il convient de communiquer cette politique de sécurité de l'information à l'ensemble des utilisateurs sous une forme adéquate, accessible et compréhensible pour les destinataires.

En somme le système d'information étant d'une importance capitale pour l'entreprise, sa sécurité doit être une préoccupation pour la haute direction. Elle doit alors définir une politique formalisée pour la sécurité du système d'information et la diffusée à tous les utilisateurs.

1.2.1.3 La responsabilité de la Direction dans la gestion de la sécurité de l'information

ISO 27002 : 2013 préconise que la Direction générale soutienne activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information. Elle doit garantir que les objectifs concernant la sécurité de l'information sont identifiés, répondent aux besoins de l'organisme et sont intégrés dans des processus adaptés ; elle doit formuler, revoir et approuver la politique de sécurité de l'information ; doit s'assurer du contrôle l'efficacité de la mise en œuvre de la politique de sécurité de l'information, fournir les ressources nécessaires à la sécurité de l'information ; garantir la coordination des mesures en matière de sécurité de l'information mises en œuvre.

1.2.1.4 La charte informatique

Pour le Journal du Net (2016 :1)[1] une charte informatique est un document élaboré par une organisation (une entreprise, une association, un établissement...) et dont le but est de délimiter les droits et obligations en matière d'utilisation du système d'information et de communication des employés, membres ou adhérents de l'organisation en question. La charte informatique est élaborée par l'organisation qui souhaite réglementer l'usage des systèmes d'information de ses employés, membres ou adhérents. Il s'agit généralement d'un document se présentant sous la forme d'un règlement intérieur imposé unilatéralement par l'organisation. Le choix dont disposent les employés, membres ou adhérents est d'accepter les conditions proposées ou d'interrompre tous liens avec l'organisation.

Pour Cale et al (2007 : 214), l'objectif de la charte informatique est de fixer les droits et obligations des utilisateurs des ressources informatiques en définissant les règles d'usage et de fonctionnement, d'informer les utilisateurs des moyens de contrôle mis en place pour

[1] *Journal en ligne traitant des thèmes liés à l'entreprise.*

surveiller et de permettre une meilleure gestion des coûts et des risques liées à l'utilisation notamment en termes de sécurité, de responsabilité, d'image et de réputation.

1.2.2 Les normes et standards en matière de système d'information

Les normes ou standards de management du système d'information sont destinés à fixer le cadre d'une démarche qualité pour atteindre des objectifs. Ils servent également de démarche qualité pour les conduites de projets. Les normes ou les standards fixent les caractéristiques de qualité que doivent satisfaire le système d'information ou l'un de ses composants (matériel, logiciel, etc.). Nous verrons dans cette section les normes et standards qui sont le plus souvent rencontrés dans le monde des systèmes d'information.

1.2.2.1 COBIT

Le COBIT (**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology) est un référentiel pour la gouvernance des technologies de l'information avec un objectif de contrôle et d'audit vis à vis de l'impact de l'utilisation de ces technologies dans l'entreprise et des risques qui y sont liés. Il a été développé depuis 1996 par l'ISACA (Information System Audit and Control Association). Il constitue le référentiel le plus reconnu en matière de gouvernance de système d'information. Il fournit un cadre global de contrôle sur un modèle de processus informatique qui convient généralement à tout le monde.

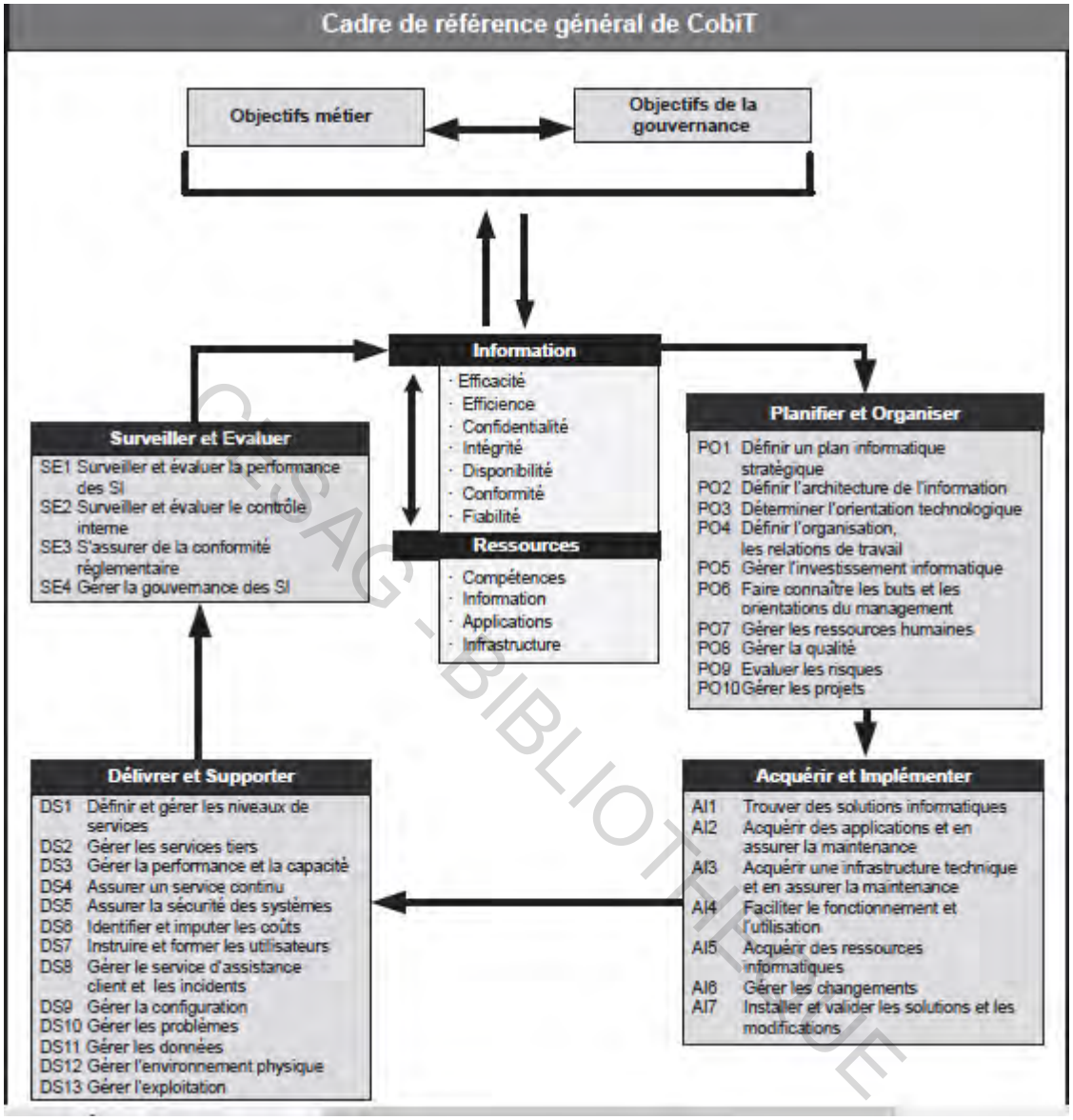
Selon Gillet (2011 :41), COBIT est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information.

Le COBIT établit des objectifs pour les informations que doivent fournir le système d'information qui sont : l'efficacité, l'efficience, la confidentialité l'intégrité, la disponibilité, la conformité, la fiabilité.

Pour atteindre ces objectifs, le système d'information doit disposer des ressources suivantes : les compétences, les applications, les technologies et les données.

Pour gérer ces ressources et atteindre ces objectifs, le COBIT 4.1 a défini 34 processus principaux répartis en 4 domaines comme le montre la figure ci-après.

Figure 1: Cadre de référence du COBIT



Source : Moissand (2009 : 30).

1.2.2.2 CMMI.

Le CMMI (capacity Maturity Model Integration) est un ensemble structuré de bonnes pratiques destinées à appréhender, évaluer et améliorer les activités d'ingénierie informatique des entreprises. Cette norme est essentiellement axée sur la certification des pratiques en matière de génie logiciel (c'est à dire de développement d'applications informatiques).

L'objectif est d'évaluer la capacité à conduire les projets avec succès, donc en respectant les trois axes de tout projet : délais, coûts et conformité des résultats par rapport au cahier de charges. Les bonnes pratiques du CMMI sont regroupées en 24 processus appartenant à quatre types :

- ✓ Process management ;
- ✓ Project management ;
- ✓ Engineering ;
- ✓ Support ;

Il a cinq niveaux de maturité qui vont permettre l'évaluation et la certification :

- ✓ Niveau initial ;
- ✓ Niveau reproductible ;
- ✓ Niveau défini ;
- ✓ Niveau maitrisé ;
- ✓ Niveau optimisation (Gillet, 2011 :40).

1.2.2.3 ITIL

ITIL (Information Technology Infrastructure Library) a été développé par le gouvernement britannique au milieu des années 1980 et s'est imposé comme un cadre de bonnes pratiques dans la fourniture de gestion d'infrastructure et la prestation de services informatiques. Il fournit une série de références pratiques pour la gestion des infrastructures et des services, il est adaptable dans n'importe quelle organisation. Les 5 livres de base couvrent chacune des étapes du cycle de vie d'un service.

1.2.2.4 ISO 27002

La Norme internationale ISO 27002-2013 est un code de bonnes pratiques pour la gestion de la Sécurité de l'Information. Elle est composée de 114 bonnes pratiques utilisables pour la mise en place du management. Cette norme est issue de la norme ISO 17799 datant de 2002 qui a évolué en ISO 27002 en 2005. L'ISO 27002 a pour objectif d'aider à l'évaluation et au traitement des risques de sécurité des informations liés à la

confidentialité, l'intégrité et aux aspects de la disponibilité. La version 2013 aborde 14 domaines comme le montre le tableau ci-dessous.

Tableau 1 : Domaines de couverture d'ISO 27002 :2013

1	Politique de sécurité de l'information
2	Organisation de la sécurité de l'information
3	Sécurité des ressources humaines
4	Gestion des actifs
5	Gestion des accès
6	Cryptographie
7	sécurité physique et environnementale
8	sécurité liée à l'exploitation
9	sécurité des communications
10	Acquisition, développement et maintenance des systèmes d'information
11	Relation avec les fournisseurs
12	Gestion des incidents liés à la sécurité
13	Aspect de la sécurité de l'information dans la gestion de la continuité de l'activité
14	conformité

Source : ISO 27002

Conclusion du chapitre 1

Ce chapitre nous a permis de décrire de façon théorique le système d'information et ses composantes d'une part et les normes et standards en matière de système d'information d'autre part.

Cette description a permis de connaitre les risques auxquels les systèmes d'information sont exposés et les mesures à prendre pour leur gestion. Cette gestion qui devra être faite par les sécurités mises en place en vue de garantir la disponibilité, l'intégrité et la confidentialité des données.

Chapitre 2 : Méthodologie de la recherche et présentation de l'HOGGY

La revue de la littérature effectuée dans le premier chapitre nous a permis de cerner la notion de système d'information et les risques qui y sont associés. La méthodologie de recherche permettra de mettre en place une démarche bien définie pour atteindre le but de notre étude à travers un modèle d'analyse.

Ce chapitre consistera à présenter la méthodologie que nous utiliserons et les outils de collectes nécessaires pour la réalisation de l'étude d'une part et d'autre part à présenter la structure qui a servi de cadre à notre étude.

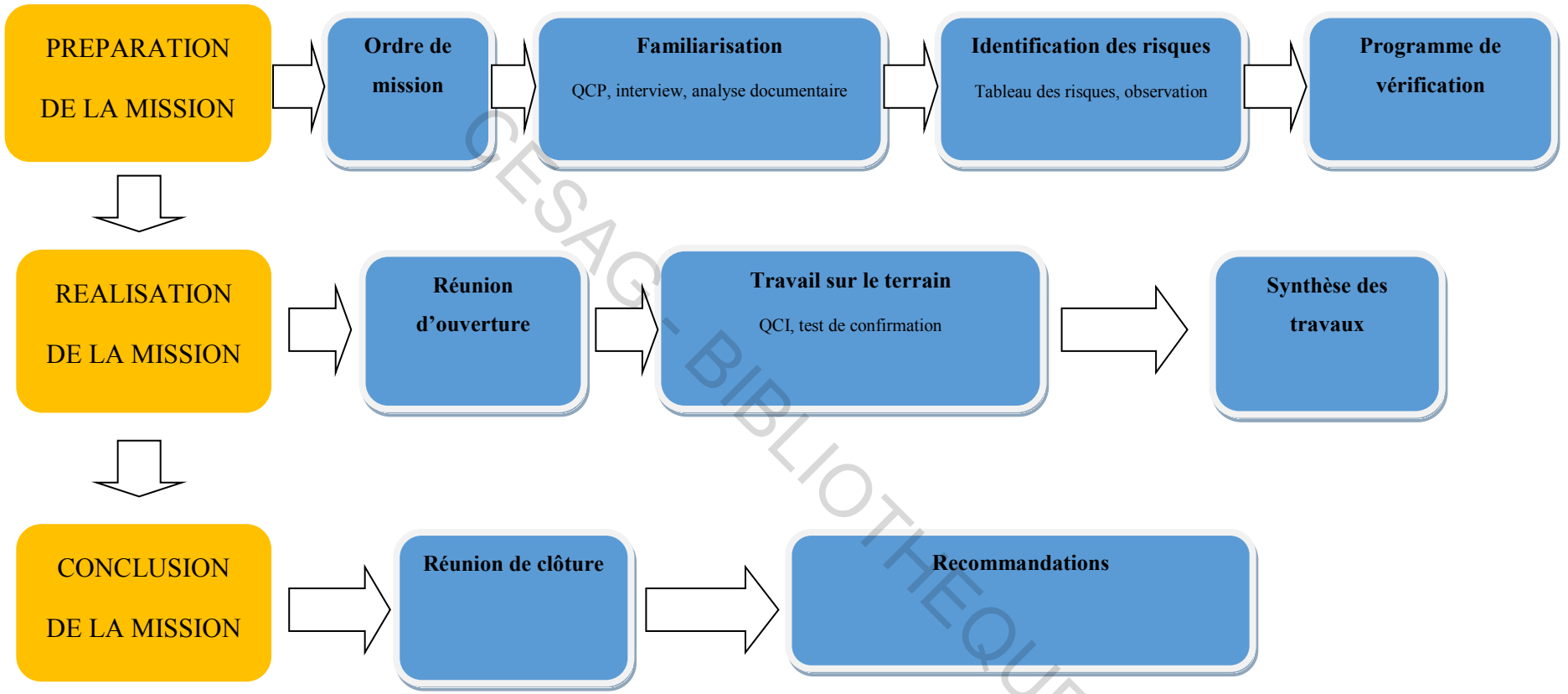
2.1 Méthodologie de la Recherche

Dans cette section nous définirons les éléments de notre méthodologie de recherche, à savoir à notre modèle d'analyse et les outils de collectes de données.

2.1.1 Modèle d'analyse

Le modèle d'analyse est une représentation schématique de la démarche scientifique de la résolution théorique du problème de l'étude.

Figure 2: Modèle d'analyse



Source : Nous-même

2.1.2 Les outils de collecte de données

Cette partie est consacrée à la description des outils de collecte de données nécessaires pour la conduite d'un audit de la sécurité du système d'information. Les outils choisis doivent être pertinents par rapport à la taille de l'échantillon, au temps disponible pour mener l'audit et au type d'information à recueillir.

Cette démarche se fera par :

- ✓ l'analyse documentaire ;
- ✓ le questionnaire de prise de connaissance ;
- ✓ l'entretien individuel ;
- ✓ l'observation ;
- ✓ le flow chart ;
- ✓ la FRAP (Feuille de Révélation et d'analyse de Problèmes).

2.1.2.1 L'analyse documentaire

C'est un outil qui permet de confronter les informations recueillies à travers les entretiens, les observations, les interviews avec ce qui devrait être ou ce qui s'est déjà passé (KEREBEL, 2009 :19).

Cette recherche consiste en l'exploitation des ouvrages et tout document pouvant faciliter la réalisation de notre mission d'audit.

2.1.2.2 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 fait un état des documents à se faire fournir par l'audité. D'après RENARD (2010 : 224), il permet de bien définir le champ d'application de la mission, de prévoir l'organisation du travail, d'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 d'informations à obtenir dès le début de la mission d'audit. Le dépouillement de l'information obtenue permettra de faire une présentation de l'entité, de se familiariser

avec les procédures en place et d'identifier le principal protagoniste à la sécurité du système d'information.

La prise de connaissance de l'entité ou de l'activité à auditer ne doit pas se faire dans le désordre. C'est pourquoi, nous utiliserons ce questionnaire qui récapitule les questions importantes dont les réponses doivent être connues si on veut avoir une bonne compréhension du domaine à auditer.

2.1.2.3 L'entretien

C'est un outil qui 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 les activités au sein de l'entreprise, et d'autre part d'avoir une idée des procédures de fonctionnement de la sécurité et de déterminer les procédures de contrôle qui régissent le domaine audité. Ce recueil d'informations est effectif à travers des questions. L'entretien peut porter sur des questions ouvertes ou sur des questions fermées.

2.1.2.4 L'observation

Selon Renard (2013 :328), l'observation physique est un outil d'application universelle. On peut observer les processus, les biens, les documents ou comportements. L'observation peut être directe (réalisée par l'auditeur) ou indirecte (réalisée par une tierce personne) et conduire à un constat. C'est un outil de validation par excellence lors d'une mission d'audit. 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'identifier et d'observer les différents dispositifs de sécurité et cela grâce à un guide d'observation et de contrôle. Ce sera le principal outil de validation des dispositifs physiques.

2.1.2.5 Le flow-chart

Le flow-chart permet de prendre connaissance des processus de l'entreprise au travers d'un graphique. C'est-à-dire qu'il permet d'indiquer l'origine des documents, leur destination et de donner une vision complète du cheminement des informations et de leurs supports.

Cette description s'opère au moyen d'une description narrative et chronologique des opérations constituant la procédure, d'une représentation simplifiée des documents créés ou utilisés et de lignes de flux retraçant le cheminement des documents.

2.1.2.6 La FRAP

La FRAP est un document normalisé qui s'utilise durant la phase de terrain. Celui-ci aide l'auditeur à conduire et à structurer son raisonnement de façon logique et chronologique.

Ainsi, chaque fois que l'auditeur constate un problème ou un dysfonctionnement, il rédige une FRAP. La finalité de la FRAP est de formuler des recommandations et sert également de base pour la rédaction du rapport.

2.1.3 Les outils d'analyse de données

Apres avoir évoqué les outils de collecte de données nous parlerons dans cette sous-section des outils d'analyse de données

2.1.3.1 Le tableau des risques

Il sert à l'identification des risques. Ce tableau découpe l'activité (fonction ou processus), objet de l'audit en tâches élémentaires. Il permet d'associer à chaque tâche les risques susceptibles de se produire. Il comportera 3 à 8 colonnes et c'est à partir de ce tableau que l'auditeur précisera les objectifs de sa mission (Renard, 2013 :215).

Pour Schick (2007 : 78), le tableau des risques se conçoit en deux phases ;

- ✓ le tableau des risques « référentiel » qui comme son nom l'indique sera un référentiel 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.

2.1.3.2 Le questionnaire de contrôle interne (QCI)

D'après Renard (2013 :235), le QCI est issu du même découpage 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 de contrôle interne existant, de constater les points forts et les points faibles du dispositif de sécurité informatique. Les questions sont du type « fermé » et le questionnaire est conçu de sorte qu'un « non » équivaut à une lacune ou une faiblesse. Un « oui » sera par contre une force et devra ensuite être validé soit par sondage, soit par observation physique.

2.2 Présentation de l'hôpital général de grand-Yoff

Cette section a pour objectif de mettre en exergue la présentation de l'hôpital général de grand Yoff, son historique, ses missions, ses activités et ses services ainsi que son organisation.

2.2.1 Historique

L'historique de l'Hôpital Général de Grand-Yoff (HOGGY) est en continuité avec celui du Centre de Traumatologie et d'Orthopédie (CTO).

Le CTO fut un centre spécialisé dans le traitement des accidents du travail, domestiques et de la voie publique.
Avec un déficit cumulé de 3 milliards puis 6 milliards après seulement cinq ans d'exercices et de lourds contentieux sociaux, la Caisse de sécurité sociale fut obligée de rétrocéder le Centre à l'Etat le 8 janvier 1996.

Le CTO change alors d'objectif et devient l'Hôpital Général de Grand-Yoff avec pour mission d'offrir toutes les prestations d'un hôpital à vocation générale. Le statut juridique de l'HOGGY a évolué depuis sa création à nos jours.
En effet, à ses origines la structure qui portait le nom de Centre de Traumatologie et d'Orthopédie avait un statut d'hôpital privé géré par une institution publique, la Caisse de Sécurité Sociale. Cet hôpital privé passe à un hôpital public à partir de 1996, pour devenir aujourd'hui un Etablissement Public de Santé de niveau trois (3) avec l'avènement de la réforme hospitalière 98-12.

L'HOGGY se finance lui-même à travers ses prestations, reçoit une subvention de l'Etat et prend en charge intégralement les salaires de ses contractuels qui représentent plus de 54% des employés.

2.2.2 Missions

L'HOGGY a les mêmes missions que celles dévolues aux Etablissements Publics de Santé (EPS) c'est à dire :

- ✓ assurer la mission du service public qui demande de veiller à ce que chaque citoyen puisse accéder aux services essentiels,
- ✓ favoriser l'équité et l'égalité d'accès aux soins pour tous,
- ✓ mettre à la disposition des populations des prestations de soins de qualité et des moyens d'information, d'éducation et de communication,
- ✓ développer des ressources humaines par la formation initiale, la formation continue du personnel de santé.

2.2.3 Organisation et fonctionnement

Après avoir décrit les organes directeurs, nous présenterons les différents services existants.

2.2.3.1 Les organes directeurs

Ce sont les différentes instances décisionnaires de l'hôpital.

2.2.3.1.1 Le Conseil d'Administration

Institué par la loi n° 98-12 du 02 mars 1998 en son article 3, il est chargé de définir la politique générale de l'établissement, délibérer sur les mesures de gestion, contrôler l'application des directives présidentielles, notamment celles issues des corps de contrôle, délibérer chaque année sur le rapport de gestion sociale présenté par le directeur.

Il est composé de douze membres ainsi répartis :

- ✓ un représentant de la présidence,
- ✓ un représentant du ministère de la santé et de la prévention médicale,
- ✓ un représentant du ministère de l'économie et des finances,
- ✓ un représentant d'un des consommateurs,

- ✓ deux représentants du corps médical et un représentant du personnel de l'établissement,
- ✓ un représentant de la mairie de Dakar,
- ✓ un représentant de l'UCAD.

Ces administrateurs ont un mandat d'une durée de trois ans renouvelable.

2.2.3.1.2 La Direction

Elle représente l'établissement en justice dans tous les actes de la vie civile (art 14, n°9-702 du 26 aout 1998).

En outre, elle assure la gestion générale de l'établissement, prépare les réunions du conseil d'administration et en assure le secrétariat, exécute les résolutions qui y sont issues, en même temps que les décisions de la tutelle. Elle recrute le personnel de l'institution, veille au fonctionnement régulier des services sur lesquels elle a autorité, assure le recouvrement des prestations fournies par l 'établissement, passe les marchés et contrats et de coordonner l'élaboration du projet d'établissement.

Enfin, elle ordonne le budget, veille à son exécution et établit les comptes annuels qui sont adoptés par le conseil d'administration en fin d'exercice.

2.2.3.1.3 La Commission Médicale d'Etablissement (CME)

Instituée par le décret n°98-701 DU 26 aout 1998, elle est composée de l'ensemble des chefs de services médicaux, pharmaceutiques et d'odontologie ; de trois représentants des corps de médecines pharmaciens et chirurgiens-dentistes élus par leurs pairs.

Elle a pour rôle, en collaboration avec le directeur général, d'élaborer le projet médical, d'organiser les activités médicales, d'orienter et de mettre en œuvre les stratégies nécessaires pour l'amélioration continue de la qualité et de la sécurité des soins et d'initier des plans de formation des personnels médicaux, d'odontologie et pharmaceutiques.

Elle émet un avis consultatif sur l'organisation générale et le fonctionnement de l'institution mais aussi sur les conventions hospitalo-universitaires.

2.2.3.1.4 Le Comité Technique d'Etablissement(CTE)

Il est créé dans chaque établissement public de santé par la loi n°98-08 du 02 mars 1998, en son article 25 portant réforme hospitalière et par le décret n° 98-701 DU 26 août 1998 relatif à l'organisation des établissements publics de santé. Présidé par le Directeur, le CTE est composé des représentants de l'ensemble des catégories professionnelles présentes dans l'établissement. Ainsi, chaque membre est élu dans sa catégorie professionnelle par ses pairs.

C'est un organe consultatif qui se réunit au moins deux fois par an pour donner son avis sur : l'hygiène et la sécurité dans l'établissement, les projets et programmes de l'établissement, les conditions et l'organisation du travail, la lutte contre les infections nosocomiales, la politique générale de formation du personnel et le plan de formation.

C'est ce socle institutionnel qui définit et oriente l'activité de l'établissement dont l'exécution est assurée par les services médicaux, médico-techniques et administratifs.

2.2.3.2 Les services cliniques, médico- techniques et administratifs

Dans cette sous-section nous présenterons les services cliniques, médico-techniques et administratifs de l'HOGGY.

2.2.3.2.1 Les services Cliniques

Ce sont les services de soins qui prennent en charge les malades de l'HOGGY.

- ✓ **Le service de radiologie**

Il effectue des radiographies conventionnelles et des échographies.

- ✓ **Le service des consultations externes**

Il centralise toutes les consultations des médecins de l'hôpital. Il a pour fonction d'accueillir et d'assurer le suivi des malades à titre externe. Il s'appuie sur des salles de pansement et un secrétariat doté de secrétaires qui organisent les consultations des médecins.

- ✓ **Le service des urgences**

Il fonctionne 24h /24 et joue le rôle d'un service de tri, en prenant en charge tous les malades dont l'état nécessite des soins et services médicaux immédiats.

Ces malades sont soit mis en observation dans les trois salles d'observation, soit ils sont transférés dans les services d'hospitalisation.

- ✓ **Le service gynécologie-obstétrique** :

Il assure des consultations gynécologiques, prénatales et des accouchements normaux et dystociques. Les activités du service se déroulent dans deux unités distinctes.

- ✓ **Le service d'orthopédie traumatologie :**

C'est le service traditionnel de l'hôpital. Il assure la prise en charge des accidentés de la circulation, du travail et domestiques et tout autre patient accidenté relevant de la chirurgie traumatologique ou souffrant de maladie orthopédique.

- ✓ **Le service d'urologie et d'andrologie :**

Sa création récente s'est faite avec le processus de diversification des activités de l'hôpital. En prenant en charge tout malade relevant de la sphère uro-génitale, la spécificité de ce service est surtout liée aux malades du troisième âge qui constituent le gros lot de sa clientèle.

- ✓ **Le service d'ophtalmologie**

Il prend en charge les affections oculaires. Il assure aussi des interventions chirurgicales pour certains cas.

- ✓ **Le service d'odontologie-stomalogie**

Il accueille les malades souffrant d'affections odontologiques et stomalogiques et assure certaines interventions de chirurgie maxillo-faciale avec des partenaires externes.

- ✓ **Le service de rééducation fonctionnelle et de kinésithérapie**

Il prend en charge les patients hospitalisés ou suivis à titre externe nécessitant une rééducation fonctionnelle motrice. L'option primaire de l'hôpital, de l'orthopédie et de la

traumatologie lui garantit une position stratégique dans le processus de prise en charge des malades.

- ✓ **Le service de médecine du travail, de l'hygiène et de la sécurité**

Il assure la prise en charge de la santé des travailleurs, de l'hygiène et de la salubrité de l'hôpital, de même que les consultations et prestations de médecine professionnelle au bénéfice des entreprises.

- ✓ **Le service de la réanimation**

Il accueille et prend en charge les malades nécessitant une surveillance en milieu de réanimation. Il a enregistré un renforcement en appareils et équipements de réanimation en vue d'accroitre ses capacités de prises en charges des malades.

- ✓ **Le service du bloc opératoire**

C'est un service commun qui accueille toutes les activités et spécialités chirurgicales. Il compte six salles dont quatre pour la chirurgie propre et deux pour la chirurgie septique. A cela s'ajoute deux salles d'opérations au service des urgences et une salle à la maternité.

- ✓ **Le service de cardiologie**

Il prend en charge, à titre externe comme interne, les malades affectés de problèmes cardiaques. Il comporte une unité de soins intensifs cardiaques qui joue un rôle de réanimation et de surveillance.

- ✓ **Le service de chirurgie générale**

Il accueille tous les malades relevant de la chirurgie viscérale et d'autres spécialités chirurgicales comme la neurochirurgie.

- ✓ **Le service de la médecine interne**

Il prend en charge des malades relevant de la médecine générale et d'autres connotations gastro entérite.

- ✓ **Le service de la pédiatrie**

Il assure la prise en charge des enfants malades et abrite une ludothèque destinée à assurer un accompagnement social aux enfants malades.

- ✓ **Le service d'Oto-Rhino Laryngologie (ORL)**

Il prend en charge les infections touchant les cavités de l'oreille et du larynx. Il assure un suivi externe et interne des malades.

2.2.3.2.2 Les services médico –techniques

Ils ont un rôle de soutien vis-à-vis des services médicaux dans leur processus de prise en charge des malades. Ils apportent leur aide dans le diagnostic d'être doté d'un scanner et d'une nouvelle table radiographique qui ont élargi la gamme de ses prestations. Il fonctionne 24 heures sur 24 et occupe une place prépondérante dans le dispositif médical et médico technique.

- ✓ **Le service des explorations fonctionnelles**

Il fait partie des derniers nés des services. Il réalise des explorations radiographiques et cardiaques auprès des malades hospitalisés ou vus à titre externe.

- ✓ **Le laboratoire d'analyse de biologie médicale**

Il effectue plusieurs types d'analyses liées à la bactériologie, parasitologie, hématologie, biochimie et immunologie. Il abrite également un dépôt de sang qui approvisionne les services en produits sanguins avec souvent la collaboration du Centre National de Transfusion Sanguine (CNTS).

- ✓ **Le service de la pharmacie**

Il assure la fourniture de produits pharmaceutiques aux services médicaux et médico-Techniques. Il comprend aussi un laboratoire galénique et une pharmacie de l'initiative de Bamako (IB).

- ✓ **Le service technique et de maintenance**

Le service de maintenance est aussi ancien que l'hôpital. Il est né avec le CTO. Il a pour mission d'assurer la maintenance des installations et des équipements de l'hôpital par : la promotion d'une maintenance de qualité, la mise en œuvre d'un système d'information et

la planification d'une maintenance préventive. Il est constitué de différentes disciplines : électricité, plomberie, menuiserie, maçonnerie, froid et climatisation, électronique et biomédicale.

Ce service a été notre principal interlocuteur lors de notre mission car abritant la division informatique, réseaux et télécom et la division électricité, froid et climatisation qui sont des acteurs majeurs dans le dispositif de la sécurité du système d'information de l'HOGGY.

- La division informatique, réseaux et télécom assure la gestion des logiciels bureautiques, la gestion des logiciel métiers de l'HOGGY, elle a en charge également l'entretien et la sécurité du réseau informatique et la maintenance du parc informatique.
- La division électricité, froid et climatisation quant à elle a pour mission le contrôle et la maintenance du réseau électrique, d'assurer la maintenance du groupe électrogène, du groupe froid et du parc des climatiseurs.

2.2.3.2.3 Les services administratifs

Ils assurent la coordination et la gestion des activités administratives de l'hôpital.

Outre la direction, on distingue le service administratif et financier, le service de contrôle de gestion, le service d'audit interne, le service des ressources humaines, le service social, le service des soins infirmiers, l'agence comptable particulière et le nouveau service des relations extérieures.

Ces trois groupes de service : services médicaux, services médico-techniques et services administratifs forment l'hôpital. Leur fonctionnalité est assurée par un ensemble de ressources formulé dans un budget annuel dont le montant est estimé à cinq milliards (5 000 000 000).

Comme toute structure hospitalière, l'HOGGY fonctionne à feu continu ; les horaires de travail sont cependant variables et différents d'un service à un autre. En effet, les services administratifs ont adopté la règle des quarante (40) heures soit huit heures par jour ouvrable, c'est-à-dire de 08 heures à 13 heures 30 le matin et l'après-midi de 14 heures 30 à 17 heures.

Quant aux deux autres groupes de services, ils sont contraints au système de feu continu, et épousent le système de garde. Cette garde fonctionne par des équipes de quarante-huit heures en général, avec un repos compensateur égal. Au-delà de ces systèmes, il existe les heures de travail effectuées en dehors des heures normales de travail recommandées par le volume de travail et la complexité des taches : ce sont les heures supplémentaires. Ces différents services sont animés par un effectif diversifié de sept cent quarante-quatre (744) agents répartis entre les différents services (administratifs, médicaux et médicotechniques).

Conclusion du chapitre 2

Ce chapitre a servi dans sa première section de cadre pour le déroulement de notre méthodologie de recherche. Cette méthodologie dans ses grandes lignes a présenté notre modèle d'analyse qui est représentation schématique de la démarche utilisé pour résoudre le problème de l'étude, les outils de collectes et d'analyse de nos données.

La deuxième section quant à elle a été le lieu de la présentation de l'hôpital générale de grand Yoff, cadre de notre étude. Nous avons pu ainsi nous imprégner son historique, ses missions et ses différents services et leur attribution.

Conclusion de la première partie

Cette première partie de notre travail a permis de faire un tour d'horizon sur le système d'information qui représente la moelle épinière de l'entreprise. Elle nous permis également de dérouler notre démarche et enfin à présenter de la structure qui a servi de cadre pour notre étude, l'hôpital général de grand Yoff (HOGGY).

Pour l'hôpital général de Grand Yoff qui est un établissement de taille importante, qui a de nombreux services et qui manipule une quantité importante de données, un système d'information fiable et sécurisé s'impose. C'est pourquoi la deuxième partie de notre travail sera consacrée à l'audit de la sécurité du système d'information. Cet audit fera un état des lieux sur le niveau de vulnérabilité aux risques de l'HOGGY. Ce qui nous permettra de proposer des axes d'amélioration pour l'atteinte des objectifs.

DEUXIEME PARTIE : CADRE PRATIQUE

Introduction de la deuxième partie

Avec le développement accéléré des SI, poussé par le progrès croissant des technologies informatiques la plupart des opérations effectuées se font par l'outil informatique disponible. Les SI sont devenus l'ossature des entreprises. Ce qui a fait apparaitre de nouveaux types de risques jadis inexistants.

De nos jours ces technologies structurent profondément la manière de travailler et déterminent la manière dont se font les échanges avec les différents services. Elles contribuent à la structuration des processus de l'entreprise. Et c'est ainsi que l'audit de la sécurité des systèmes d'informations s'est imposé comme une nécessité afin de permettre à l'hôpital général de grand Yoff afin de faire le point sur son exposition aux risques liés au système d'information.

Cette partie sera donc consacrée à la mise en œuvre de notre audit de la sécurité du système d'information à l'HOGGY. Le chapitre 3 sera le lieu de la description des pratiques de sécurité de système d'information et le chapitre 4 à la présentation des résultats de notre audit et les recommandations pour améliorer les faiblesses constatées.

Chapitre 3 : Description du dispositif de sécurité du Système d'Information de l'HOGGY

Ce chapitre sera consacré à la description du dispositif de sécurité du système d'information. Cette description se fera par une présentation d'une part des différents acteurs en charge du système d'information et de leur méthode de travail et d'autre part, du dispositif pratique de sécurité mis en place tel que nous l'avons observé.

3.1 Les acteurs et l'actif informationnel

Cette section fera l'objet de la présentation des services et des divisions impliqués dans la sécurité du système d'information.

3.1.1 Le Service Technique de Maintenance (STM)

Le service technique de maintenance a pour mission de définir et de mettre en œuvre les mécanismes organisationnels appropriés en collaboration avec les services administratifs et médico-techniques pour appliquer la politique de maintenance définie par le Directeur de l'HOGGY.

Il est subdivisé en plusieurs subdivisions

- ✓ La division biomédicale ;
- ✓ La division Génie civil ;
- ✓ La division des équipements non médicaux ;
- ✓ La division informatique, réseau et Telecom ;
- ✓ La division électricité, froid et climatisation.

Les deux dernières divisons sont celles qui nous intéressent au plus près dans le cadre de cette étude car acteurs majeurs dans le dispositif du système d'information de l'HOGGY.

3.1.1.1 La division informatique, réseau et Telecom

Cette division a à charge d'assurer la gestion des logiciels bureautiques, la gestion des logiciels métiers tels que le SIH, PACS, SAARI, elle assure également l'entretien du réseau, la maintenance du parc informatique de l'HOGGY et l'assistance aux utilisateurs. La division est composée de 6 agents dont 2 stagiaires. Un rapport détaillé de leurs interventions mensuelles est rédigé. Ce rapport mentionne la date d'intervention, le nom de l'utilisateur qui

a bénéficié de l'intervention, le service auquel il appartient, le motif, et le matériel utilisé. Ce rapport est ensuite envoyé au contrôle de gestion pour le calcul des coûts en comptabilité analytique.

3.1.1.2 La division électricité, froid et climatisation

Cette division a pour mission de :

- ✓ contrôler et assurer la maintenance du réseau électrique ;
- ✓ assurer la maintenance du groupe électrogène ;
- ✓ assurer la maintenance du groupe froid ;
- ✓ assurer la maintenance du parc de climatiseur ;
- ✓ assurer la maintenance des ascenseurs.

L'HOGGY est alimenté en électricité par la SENELEC, société nationale d'électricité. Il dispose d'un groupe électrogène pour assurer la continuité de l'activité en cas de coupure d'électricité.

La puissance électrique par différents services est indiquée dans le tableau ci-après.

Tableau 2 : Tableau des puissances électriques par services

BATIMENT	SERVICE	COFFRET	P(KW)	Q(KVA)	I (A)	PUISSANCE PAR SERVICE (KW)
1	ORTHOPEDIE	TD 10 EST ISSUE	3	0.03	5	35
		TD 10SUD ORTHO	9	12.57	23	
		TD 10NORD ORTHO	22	13.48	38	
	UROLOGIE	TD11 SUD	6	4.55	11	6
	ORL	TD11 EST ISSUE	2	2.12	5	19
		TD 11NORD ORL	17	11.34	29	
	CHIRURGIE	TD 12 EST ISSUE	3	3.09	6	14
		TD 12NORD CHIRUR	11	9.26	21	
	CARDIOLOGIE	TD 12 SUD CARDIO	10	6.41	17	11
		TD 13EST ISSUE	1	1.89	3	
	PEDIATRIE	TD 13NORD PEDIA	20	15.02	36	20
	MEDECINE INTERNE	TD13SUD MED INTERNE	12	9.41	22	12
2	URGENCE	TD20G URG	8	10.87	19	12
		TD20 D URG	4	5.15	9	
	MATERNITE	TA SECOND OU EST F	8	6.83	15	23
		TD 20B MATER	3	5.32	9	
		TD20A MATER	6	1.91	9	
		TA SECOND EST F	6	8.49	15	
3	RADIO	TD 30 NORD	17	5.66	26	33
		TD 30 SUD	16	4.18	24	

4	ENDOSCOPIE	TD 40 SUD ENDOSC	23.8	5	34.35	23.8
	LABORATOIRE	TD 40 RADIO NUCL	14.29	12	27	55
		TD 41 AILE GAUCHE	3.1	6	4.47	
		TD 41 AILE DROITE	38	7.13	56	
5	CONSULTATION EXTERNE	TD 50 OUEST	14	3.42	20	36
		TD 50EST	23	11.55	37	
6	SERVICE INTERNE	TD SERVICE ENTREES	16	9.98	27	16
7	KINESIE	TD 70 EST	9	5.61	16	16
		TD 70 OUEST	7	4.83	12	
	DIRECTION	TD 71 OUEST	17	6.59	26	31
		TD 71 NORD	5	3.23	9	
		TD 71 SUD	8	4.79	14	
8	MEDECINE TRAVAIL	TD 80 MED TRAVAIL	21	16.24	38	21
9	NON IDENTIFIE	TD 90 NORD	18	11.69	31	18
10	BUANDERIE CUISINE REFECTOIRE	BUANDERIE BAT 10	71	35.20	115	96
		CUISINE BAT 10	9	12.69	22	
		REFECTOIRE RESTAURANT BAT 10	15	12.36	28	
11	MAINTENANCE	MAINTENANCE BAT 11	21.32	4	30.77	21.32
12	DIALYSE	DIALYSE BAT 12	23	2.28	33	23
	ANCIENNE MORGUE	ANCIENNE MORGUE	3	0.14	5.6	3
13	PHARMACIE	PHARMACIE	9.7	-	14	9.7
14	MORGUE +ANATOMIE	MORGUE +ANATOMIE	17	14.95	33	17
LF	LOGEMENT DE FONCTION	LOGEMENT DE FONCTION	53	13.00	79	53

Source : Service Technique et Maintenance

3.1.2 Le Service Hygiène et Sécurité

Ce service, outre les rôles déjà mentionnés dans le chapitre 2 s'occupe dans son volet santé et sécurité au travail de la prévention incendie de l'HOGGY.

A cet effet, un contrat d'entretien et de vérification des extincteurs a été signé avec une entreprise dans ce domaine, la Sodeci.

L'HOGGY dispose de 46 extincteurs installés dans les bâtiments des différents services. Le contrat avec cette entreprise prévoit un programme de formation des agents sur la prévention incendie à l'issue duquel une simulation doit être réalisée.

La sécurité physique des équipements et des personnes est assurée par une équipe d'agents de sécurité, qui sont postés à l'entrée de l'HOGGY et aussi dans certains lieux sensibles au sein même de l'hôpital. Ils sont au nombre de 38 dont 25 agents de l'HOGGY et les 13 autres provenant du Ministère de la santé.

3.1.3 L'actif informationnel

L'HOGGY dispose d'une diversité d'application pour son fonctionnement tant pour le fonctionnement technico clinique que pour le fonctionnement administratif.

Ainsi donc, l'HOGGY dispose de l'application PACS pour la gestion de l'imagerie médicale, SIH (Système d'Information Hospitalière) en déploiement depuis le mois d'Août 2016 mais plus fonctionnel pour sa partie Gestion des facturations, SAARI COMPTA I7 pour le traitement de l'information financière.

Le système d'exploitation est hétérogène. Nous avons le Windows 7, windows.8.1 et Windows 10, pour les postes de travail et du Windows 8 server, Windows 12 server pour les serveurs.

Pour la suite Office, elle est constituée de Office 2007, Office 2010, Office 2013 et Office 2016.

Pour la protection contre les logiciels malveillants, la licence de l'antivirus Bitdefender a été acquise dans le mois d'Avril 2016 et installé sur la plupart des ordinateurs de l'hôpital.

Au niveau du matériel informatique nous avons pu dénombrer avec l'aide de la cellule informatique 198 ordinateurs répartis par service (annexe 3), 59 onduleurs, 94 imprimantes et 24 switches.

3.2 Dispositif de sécurité du système d'information

Cette section sera consacrée à la description du dispositif de sécurité du système d'information telle que décrit par nos différents interlocuteurs lors des entretiens que nous avons eus avec eux.

3.2.1 Gestion des risques liés au système d'information

Au niveau de l'HOGGY, les risques sont évalués et gérés par la fonction audit interne. A cet effet une cartographie des risques est en cours d'élaboration avec un cabinet spécialisé. Mais une gestion spécifique des risques liés au système d'informatique n'est pas formalisée. Quotidiennement l'équipe de la division informatique assiste les utilisateurs, notamment pour faire face au problème récurrent de réseau ou en cas de défaillance du matériel.

3.2.2 Sécurité du système informatique

Cette description de la sécurité du système prendra en compte la lutte contre les logiciels malveillants, la gestion des accès et la sauvegarde des données.

3.2.2.1 Lutte contre les logiciels malveillants.

L'HOGGY a acquis une licence depuis le mois d'avril 2016 pour l'antivirus BITDEFENDER, et installé sur les serveurs et les postes de travail des utilisateurs, la mise à jour de cet antivirus se fait automatiquement via internet.

3.2.2.2 Gestion des accès

Les applications SIH et SAARI sont logées dans le domaine hoggy.sn auquel les utilisateurs doivent se connecter avec un logging et un mot de passe avant d'y avoir accès. Ensuite, l'accès aux applications SIH et SAARI requiert également un logging et un mot de passe. Pour les autres utilisateurs qui ne sont pas dans le domaine hoggy.sn, seul un logging et un mot de passe est exigé au démarrage de leur ordinateur. Ces mots de passe sont créés par défaut par l'administrateur, ils sont ensuite modifiés selon chaque utilisateur et doivent être renouvelés tous les deux mois.

3.2.2.3 Sauvegarde des données

La sauvegarde des données se fait à travers des serveurs. Pour les données médicales, une sauvegarde est réalisée chaque jour à 18h dans un serveur dédié à cet effet. Les

caractéristiques de ce serveur sont Intel Xeon cpu 3GHz mémoire RAM 64 Go, Windows 12 server. Une réplique est faite dans un serveur back up qui est logé dans un autre bâtiment. Les caractéristiques de ce serveur sont Intel Xeon cpu 2GH mémoire RAM 16 Go, Windows 12 server.

Pour les données du logiciel SAARI et SIH, un autre serveur (Windows 8 server, 12 Go de RAM) les sauvegarde dans une salle serveur chaque jour à 18 h et une réplique est faite dans un serveur back up logé dans le bureau des informaticiens.

Toutes ces données sont sauvegardées également sur des disques externes chaque soir et gardé par les informaticiens.

L'accès aux différentes salles serveurs n'est réservé qu'aux informaticiens et exceptionnellement à des personnes qui ont une autorisation comme cela a été notre cas dans le cadre de notre étude.

3.2.3 Gestion de l'environnement physique

Des agents de sécurité sont postés à l'entrée principale de l'HOGGY et aussi dans des couloirs de certains bâtiments abritant des infrastructures sensibles comme les serveurs. Ces serveurs sont dans des salles à l'intérieur du bâtiment administratif et peu identifiables depuis l'extérieur. L'hôpital général de Grand Yoff possède deux salles serveurs. Une de ces salles a une porte métallique et l'autre a une porte en bois solide. Les serveurs sont tous protégés par des onduleurs et les salles sont dotées des climatiseurs pour assurer le refroidissement des équipements, toutefois dans le bureau informatique le climatiseur installé est hors d'usage et remplacé par un ventilateur. Pour la lutte contre les incendies, l'hôpital est équipé d'extincteurs. Ces extincteurs sont vérifiés tous les six mois par l'entreprise qui les a installé ; la Sodeci.

Conclusion du chapitre 3

Ce chapitre a été le cadre pour nous de présenter le dispositif de sécurité du système à l'hôpital général de grand Yoff, nous avons ainsi présenté les acteurs et les mesures mis en place pour garantir la sécurité du système d'information. Cette description nous a permis d'avoir une idée sur les pratiques existantes. Cette description achevée nous consacrerons le chapitre suivant à leur analyse à travers un audit à la suite duquel nous proposerons des recommandations pour les améliorer.

Chapitre 4 : Audit de la sécurité du système d'information de l'HOGGY

Ce dernier chapitre de notre étude est consacré à la mise en œuvre de l'audit de la sécurité du système d'information de l'hôpital général de grand Yoff. Comme toute mission d'audit, nous avons découpé notre mission dans cet hôpital en trois grandes phases : une phase de préparation, une phase de réalisation sur le terrain et une phase de conclusion. A l'issue de ces travaux, une synthèse des forces et faiblesses de la sécurité sera faite et des recommandations seront proposées pour corriger les faiblesses constatées.

4.1 Préparation de la mission

Notre mission au sein de l'HOGGY s'est ouverte par la phase de préparation au cours de laquelle nous avons pu présenter notre autorisation de stage qui a servi d'ordre de mission dans le cadre cette étude. Il s'en est suivi une étape de prise de connaissance de l'entité et l'identification des risques inhérents à l'activité qui nous a permis d'élaborer notre programme de contrôle.

4.1.1 Familiarisation et prise de connaissance de l'HOGGY

Notre mission a débuté à l'hôpital général dès que nous avons eu notre autorisation de stage signée par le Directeur. Nous avons été mis sous l'autorité du chef de service du contrôle de gestion comme Directeur de Mémoire. Après avoir pris connaissance de notre thème de mémoire, il nous a mis en relation avec le responsable de la cellule informatique qui est une division du service technique et maintenance.

Les différentes interviews que nous avons eu avec le chef de service du contrôle de gestion, le responsable de la cellule informatique, le responsable du service hygiène et sécurité ainsi que l'administration de notre questionnaire de prise de connaissance (tableau ci-après) nous ont permis d'avoir une vue approfondie sur les activités, l'historique, l'organisation ainsi que le système d'information.

Tableau 3 : Questionnaire de prise de connaissance

QUESTIONNAIRE DE PRISE DE CONNAISSANCE	
Objectif : Prendre connaissance de l'HOGGY, de son système informatique et de sécurité	Observation
Présentation de l'entité	
Mission et organisation	Ok
Historique	Ok
Organigramme générale	Ok
Prendre connaissance du système informatique	
L'organisation	Ok
Les missions et l'effectif	Ok
Le manuel de procédures	En élaboration
Visite des locaux	Salle serveur, salle informatique
Documents	
Manuel de procédures	En élaboration
Récapitulatif du matériel informatique	Ok
Organigramme détaillé	Ok
Statuts	Ok

Source : nous-même

4.1.2 Elaboration du tableau des risques

La prise de connaissance de l'HOGGY ainsi faite, nous avons élaboré le tableau des risques conformément à la norme 2200 de l'IIA, nous avons ainsi fait une évaluation des risques inhérents au système d'information. Pour ce faire nous avons découpé le système d'information en processus.

Ce tableau consiste à répertorier les risques associés à chaque processus, d'en évaluer la gravité et vérifier l'existence de bonnes pratiques souhaitables qui peuvent aider à réduire les conséquences.

Tableau 4 : Tableau des risques

Tâches ou processus	Objectifs	Risques associés	Evaluation du risque	Dispositifs de contrôle existant ou souhaitable	Constat
Gestion et évaluation des risques	S'assurer que l'organisation et la gestion du SI est efficace	Non alignement stratégique des objectifs de sécurité par rapport aux objectifs de HOGGY	Moyen	Définition d'une politique de sécurité incluant la sécurité du SI	non
				Communication de la politique de sécurité à tout le personnel	non
				Revue périodique de la politique de sécurité	oui
		Inefficacité dans la gestion de la sécurité de l'information	Elevé	Mise en place d'un comité de gestion de la sécurité du SI	non
				Existence de la fonction de Risk Manager de SI	non
		Inadéquation des moyens mis en œuvre par rapport aux objectifs	Moyen	Existence d'une politique du SI approuvé par la hiérarchie	non
				Existence d'un schéma directeur SI	non
Gestion de la sécurité physique	S'assurer que seules les personnes autorisées ont accès aux SI	Accès non autorisé aux locaux sensibles	Elevé	Formalisation des procédures d'accès aux zones sensibles	non
				port obligatoire de signe visible pour toute personne étrangère accédant aux zones sensibles	oui
		Protection insuffisante des équipements contre les menaces physiques (vol, perte, destruction,)	Moyen	Sécurité des installations électrique	oui
				Vidéosurveillance	non
				Existence des extincteurs	oui
				Service de gardiennage	oui

Gestion de la sécurité logique	S'assurer de l'invulnérabilité des accès logiques	Dénie du droit d'accès	Elevé	Sensibilisation à la tenue des droits d'accès	oui
				Existence de la liste des droits d'accès actifs ou non	non
		Utilisation abusive du SI pouvant entrainer du ralentissement dans le traitement	Moyen	Restriction d'accès à l'information en fonction des droits	oui
				Limitation des téléchargements	oui
				Logiciel antivirus	oui
				Contrôle des accès à internet	oui
Gestion des risques SI	S'assurer de l'existence d'une procédure d'une gestion efficace des risques SI	Identification/inadéquation inadéquate des menaces et vulnérabilités potentielles	Moyen	Existence d'une cartographie des risques comprenant les Risques SI	non
				intégration des procédures de gestion des risques dans les activités quotidiennes	non
				Existence d'une méthode formalisée d'analyse et de gestion des risques	non
	S'assurer de la protection des actifs informationnels	Protection insuffisante des actifs informationnels	Elevé	Existence d'une procédure d'identification et de classification des ressources SI	oui
				Désignation d'un responsable pour chaque ressource	oui
		Destruction de données/du matériel suite à un incendie	Elevé	Extincteurs	oui
				Détecteur de fumée	non
				Formation à l'usage des extincteurs	oui
		Coupure d'électricité	Moyen	Existence d'un groupe électrogène à démarrage automatique	oui

Gestion des mots de passe	S'assurer de la bonne gestion des mots de passe	Mot de passe vulnérable	Moyen	Définition d'une politique formalisée des mots de passe	non
				Renouvellement périodique des mots de passe	non
		Déni de service	Faible	Formation périodique sur l'ingénierie sociale	non
Sauvegarde des données	Etre sûr que les données sont sauvegardées de manière périodique sur différents supports à différents endroits	Absence de sauvegarde régulière	Faible	Procédure de sauvegarde automatisée des données	oui
		Sauvegarde non exhaustif	Faible	Contrôle périodique des sauvegardes (restauration périodique)	non
		Altération du support de sauvegarde	Faible	Diversification des supports de sauvegarde	oui
				Isolation des supports de sauvegarde des principaux sites	non
				Test périodique de la qualité des sauvegardes	non
		Accès non autorisé aux sauvegardes	Moyen	Tenue d'un registre des personnes accédant aux sauvegardes	non
				Salle de sauvegarde avec accès limités et sécurisés	oui
Continuité de l'activité	S'assurer de la continuité de l'activité en cas de sinistre	Panne matérielle	Moyen	Serveur de secours	oui
		Reprise compromise de l'activité	Moyen	Définition d'un plan de secours des activités	non
				Plan de secours informatique	non
				Test et évaluation du plan de continuité de l'activité	non
				Formation du personnel aux procédures de secours et d'urgence	oui
		Perte d'information stratégique	Faible	Duplication des données sur un autre site	non

Sources : Renard (2013 ; 219) ; Schick et al (2010 ; 266-269) ; CHAI (2014 ; 49-55)

L'analyse du tableau des risques au vu de l'objectif général et des objectifs spécifiques nous a permis de définir le champ d'action de notre mission et d'élaborer notre programme de vérification.

4.1.3 Programme de vérification

Le programme de vérification décrit les diligences mises en œuvre, les structures et les personnes avec qui s'entretenir et les informations à collecter pour atteindre notre objectif d'audit.

Tableau 5 : Programme de vérification

Processus ou activités	**Personnes avec qui s'entretenir ou tâches à effectuer**
Gestion et évaluation des risques	Entretien avec l'auditeur interne, entretien avec le responsable de la cellule informatique exploitation de la cartographie des risques
Gestion de la sécurité physique	Entretien avec le chef de service Technique et de maintenance, entretien avec le responsable de la cellule informatique, entretien avec le chef de service Hygiène et sécurité, visite des locaux techniques, observation des bâtiments abritant les serveurs, analyser la cartographie des risques.
Gestion de la sécurité logique	Entretien avec l'administrateur réseau, entretien avec certains utilisateurs, vérifier des antivirus sont installés sur un échantillon de machine et qu'ils sont à jour,
Gestion des risques SI	Entretien avec le responsable de la cellule informatique, entretien avec des utilisateurs, observation, entretien avec le chef service technique et maintenance, vérification de l'existence d'un groupe électrogène
Gestion des mots de passe	Entretien avec l'administrateur réseau, sélection d'un échantillon d'ordinateur et vérifier les droits d'accès
Sauvegarde des données	Entretien avec le responsable de la cellule informatique, visite des salles serveurs
Continuité de l'activité	Entretien avec le responsable de la cellule informatique, vérifier l'existence d'un site de secours,

Source : Nous même

L'élaboration de notre programme de travail est la dernière étape de la phase préparation. Ce qui nous conduit à la phase de déroulement de notre mission.

4.2 Réalisation de la mission

La phase de réalisation de la mission a consisté en un travail sur le terrain en procédant aux différents tests tels que décrits dans la phase de préparation, aux différents entretiens avec les différents acteurs de la sécurité de système d'information, à des constatations sur le terrain ; à la finalisation et à l'administration de notre questionnaire de contrôle interne (voir annexe 2). Les réponses négatives à ce questionnaire correspondent à des faiblesses pour lesquelles l'on doit faire des recommandations. Les réponses positives quant à elles constituent des forces qui devront être confirmées par des tests.

Ainsi donc conformément à notre programme de vérification nous avons conçu ces tests. Nous avons sélectionné un échantillon de 21 ordinateurs en tenant compte du nombre d'ordinateurs par services (annexe 3). Notre échantillon est ainsi reparti :

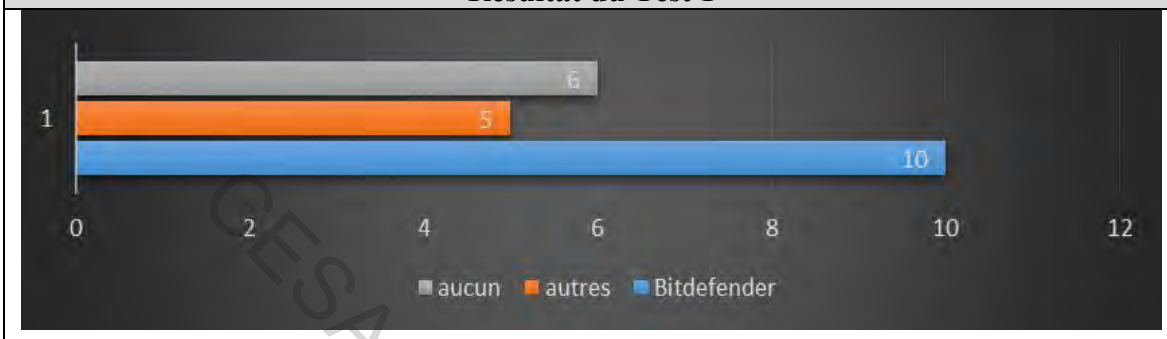
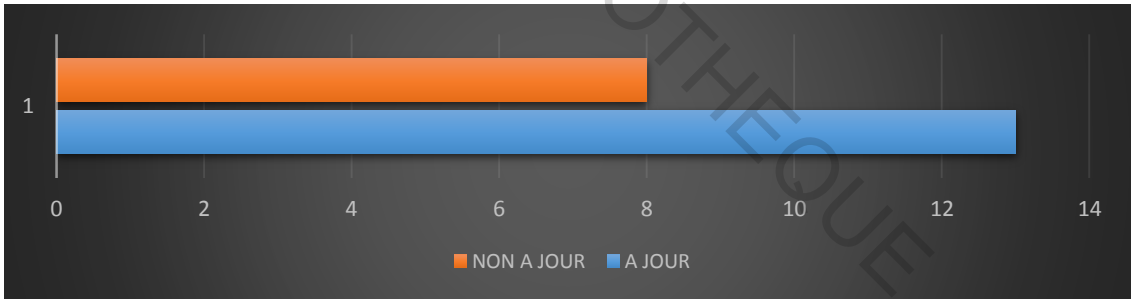
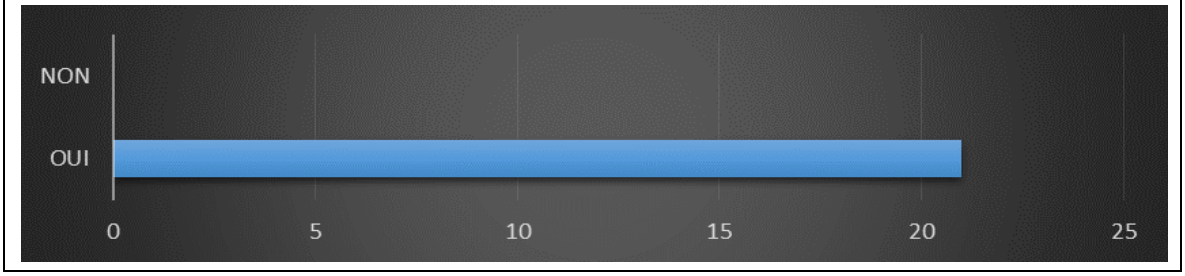
Tableau 6 : Echantillon d'ordinateur pour les tests

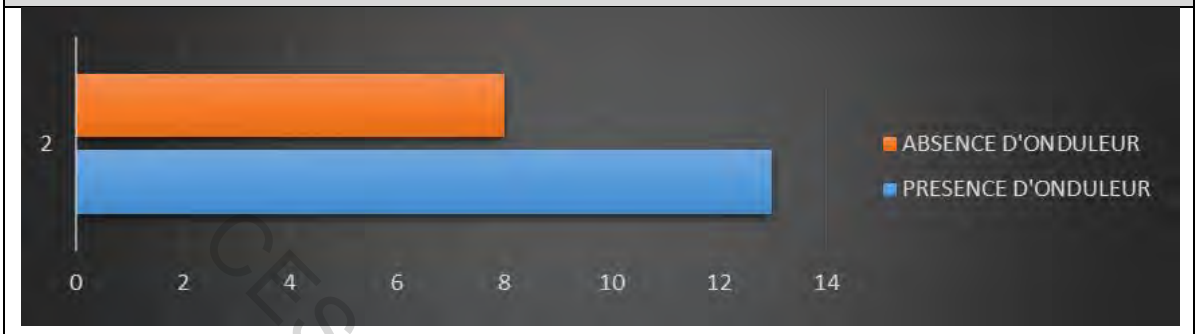
Service	Nombre d'ordinateurs sélectionnés
Agence Comptable	4
Biologie Médicale	3
Cellule communication	2
Cellule Information médicale	2
Contrôle de gestion	2
Ressources Humaines	5
Hospitalisation et soins externes	3
TOTAL	21

Source : nous même

Les résultats de ces tests sont présentés dans le tableau suivant :

Tableau 7 : Tableau des tests de confirmation

Test 1
Vérifier l'installation de l'antivirus Bitdefender sur un échantillon d'ordinateur : ✓ Echantillon : 21 ; ✓ Bitdefender : 10 ; ✓ autres : 5 (Smadav : 3 ; Avast : 1, Windows defender : 1) ✓ aucun : 6 ;
Résultat du Test 1

Test 2
Vérifier que la base virale de l'antivirus pour l'échantillon sélectionné dans le cadre du Test 1 est à jour. ✓ Echantillon : 21 ; ✓ A jour : 13 (Bitdefender : 9 ; Windows defender : 1 ; Avast : 1 ; Smadav : 2) ✓ Non à jour : 8 (Bitdefender : 1 ; Smadav : 1 ; Aucun : 6)
Résultat du Test 2

Test 3
Vérifier l'entrée obligatoire d'un logging et d'un mot de passe pour avoir accès au logiciel SAARI et SIH pour les utilisateurs. ✓ Echantillon 21 ; ✓ Oui : 21 ✓ Non : 0
Résultat du Test 3


Test 4
Vérifier qu'un onduleur protège chacun des ordinateurs pour échantillon d'équipement choisi : ✓ Echantillon 21 ; ✓ Présence d'onduleur : 13 ; ✓ Absence d'onduleur : 8
Résultat Test 4


Source : nous-même

Ces tests que nous avons menés sur le terrain nous ont permis de constater que certains ordinateurs qui ne sont pas dans le domaine hoggy.sn ne sont pas dotés de mot de passe au démarrage. Certains mots de passe sont faibles : ce sont souvent des mots du dictionnaire, des noms de personnes proches de la famille. Ils sont aussi caractérisés par l'absence de caractères spéciaux. Ces mots de passe ne sont pas renouvelés régulièrement. Nous avons également constaté que certains antivirus installés sur des postes de travail sont des versions d'évaluation ou que la clé d'activation a expiré. Nous avons également constaté lors des tests que le pack office d'une machine n'est pas la version authentique.

En plus de ces tests, nous avons aussi fait des visites d'inspection dans les différentes salles abritant les serveurs, la salle informatique et des différents bâtiments afin d'apprécier le dispositif de sécurité. Nous avons consigné les constats de nos visites dans le tableau suivant :

Tableau 8 : Tableau des constats des inspections

Points observés	Etat des lieux
Climatisation des salles	Nous avons constaté que les deux salles serveurs visitées sont dotées de climatiseurs mais dans les salles des informaticiens où est logé un serveur back up, le climatiseur est en panne et remplacé par un ventilateur
Protections des serveurs par des onduleurs	Nous avons constaté que les serveurs sont protégés par des onduleurs
Alarme automatique	Nous n'avons pas constaté d'alarme automatique pouvant attirer la vigilance du personnel
Détecteur de fumée	Aucun détecteur de fumée
Extincteurs	Nous n'avons pas constaté la présence d'extincteurs dans les salles serveurs cependant des extincteurs sont présents dans les couloirs des différents bâtiments
Extincteurs à jours	Une vérification a été faite en Août 2016
Présence de consigne de sécurité	Aucune présence de consigne de sécurité informant le personnel des conduites à tenir en cas de danger
Présence de groupe électrogène	Nous avons constaté la présence d'un groupe électrogène prenant le relais de la SENELEC en cas de coupure électrique
Qualité des murs des salles serveurs	Les murs des salles serveurs sont solides (béton armé)
Qualité des portes	Une des salles serveurs a une porte en acier, l'autre est en bois renforcé
Qualité des fenêtres	Vitre en lamelle protégée avec des barreaux
Présence de poussière	Nous avons constaté qu'une entreprise de nettoyage s'occupe régulièrement des salles et de tous les bureaux
Site de secours	Il n'y a pas de site de secours pour la sauvegarde de données.

Source : nous-même

Des recommandations seront proposées pour les insuffisances de contrôle constatées depuis la phase de préparation et les dysfonctionnements observés lors de l'inspection des locaux.

4.3 Synthèse des travaux

Cette section est le lieu de la présentation des forces et des faiblesses constatées lors de nos différents tests et aussi des inspections des locaux, cette présentation suivra le découpage retenu lors de l'élaboration de notre tableau de risques.

4.3.1 Les points forts de la sécurité du système d'information.

Les points forts de la sécurité du système d'information sont consignés dans le tableau suivant

Tableau 9 : Les points fort de la SSI

Processus ou tâches	Points forts
Gestion et évaluation des risques	✓ Une cartographie des risques est en cours d'élaboration
Gestion de la sécurité physique	✓ Les salles serveurs sont à l'abri d'intempéries ✓ Les salles serveurs ne sont réservées qu'aux informaticiens et aux personnes autorisées ✓ Des agents de sécurité assurent la sécurité des hommes et aussi de équipements
Gestion de la sécurité logique	✓ Les postes de travail sont protégés par un logging et un mot de passe avant tout accès aux applications métiers
Gestion des risques SI	✓ Une cellule informatique existe au sein de l'HOGGY
Gestion des sauvegardes	✓ Une sauvegarde des données est faite chaque jour ✓ Les données sont répliquées dans des serveurs back up ✓ Une copie de ces données est faite quotidiennement sur des disques externes
continuité de l'activité	✓ Un groupe électrogène assure le relais de e la fourniture en électricité en cas de coupure

Source : Nous-même

4.3.2 Les points faibles de la sécurité du système d'information.

Les points forts de la sécurité du système d'information sont consignés dans le tableau suivant :

Tableau 10 : Les points faibles de la SSI

Processus ou tâches	Points forts
Gestion des risques	✓ Il n'n'existe pas la fonction de risk-manager au sein de l'hôpital général de grand Yoff
Gestion de la sécurité physique	✓ Une des portes des salles serveur est en bois ✓ Aucune consigne de sécurité n'est affichée informant le personnel des conduites à tenir en cas de danger ✓ Il n'existe pas de détecteur de fumée
Gestion de la sécurité logique	✓ Certains postes de travail n'exigent pas de d'identification et authentification avant d'y avoir accès ✓ Certains postes ne sont pas dotés d'antivirus ou lorsqu'ils existent ne sont pas à jour
Gestion des risques SI	✓ L'audit de la sécurité du système d'information n'a jamais été fait et aucun n'est prévu dans le planning d'audit ✓ Il n'existe pas de charte informatique ✓ La cartographie en cours d'élaboration n'intègre pas les risques spécifiques au système d'information ✓ Il n'existe pas de schéma directeur du système d'information ✓ La fonction Responsable de la sécurité du système d'information (RSSI) n'existe pas
Gestion des sauvegardes	✓ Les données ne sont pas sauvegardées sur un autre site à l'extérieur de l'HOGGY ✓ Il n'y a pas de test régulier de restauration des sauvegardes
continuité de l'activité	✓ Les données ne sont pas sauvegardées sur un autre site pour assurer la continuité de l'activité en cas de sinistre sur le site actuel

Source : Nous-même

4.4 Recommandations

L'audit de la sécurité du système d'information de l'hôpital général de grand Yoff nous a permis de mettre en évidence certaines insuffisances dans sa gestion. Cette section sera le lieu de proposer des recommandations pour l'améliorer.

4.4.1 Recommandation à la Direction Générale

Nous proposons ainsi à la direction générale :

- ✓ De créer un service autonome en charge de la gestion du système d'information et de définir clairement ses tâches et qui intégrera la fonction de RSSI,
- ✓ De prendre en comptes les risques liés au système d'information dans l'élaboration de la cartographie des risques,
- ✓ D'élaborer un schéma directeur informatique,
- ✓ D'augmenter le nombre d'agents de l'actuelle division informatique afin de réduire le délai d'attente lorsqu'ils sont sollicités,
- ✓ De tenir compte de l'audit des systèmes d'information lors de la planification des missions d'audit.
- ✓ De renforcer le niveau des membres du service d'audit de l'HOGGY sur les risques liés au système d'information.
- ✓ De créer la fonction de Risk Manager qui aura pour rôle d'identifier, d'évaluer, de communiquer et de sensibiliser sur les risques de l'entreprise.
- ✓ D'élaborer une charte informatique dont le but est de délimiter les droits et obligations en matière de système d'information à tout le personnel de l'hôpital général de grand Yoff.
- ✓ Communiquer la politique de sécurité du système d'information à tout le personnel
- ✓ D'installer un serveur de sauvegarde des données sur un autre site afin d'assurer la continuité de l'activité en cas de sinistre.
- ✓ D'afficher des plaques signalétiques indiquant au personnel les conduites à tenir en cas de danger.
- ✓ Mettre en place un système de détection de fumées afin de prévenir des risques d'incendie.
- ✓ Faire intégrer le logiciel de facturation et celui de la comptabilité afin de traiter de façon automatique les données financières.

4.4.2 Recommandation à la division informatique

A la division informatique nous recommandons

- ✓ D'installer l'antivirus Bitdefender sur toutes les machines et de veiller à leur mise à jour régulière.
- ✓ De définir une politique formalisée de la gestion des droits d'accès.
- ✓ De s'assurer que tous les ordinateurs de l'HOGGY exigent un logging et un mot de passe au démarrage.
- ✓ De veiller au renouvellement de ces mots de passe et s'assurer qu'ils sont suffisamment forts pour ne pas être cassée facilement
- ✓ D'étendre l'installation d'onduleurs sur tous les ordinateurs de l'HOGGY afin d'assurer la disponibilité de l'information en cas de coupure de l'électricité
- ✓ De renforcer la porte de la deuxième salle serveur avec une porte métallique
- ✓ D'installer des extincteurs dans les salles serveurs.
- ✓ De sensibiliser les utilisateurs aux risques liés au système d'information.
- ✓ De procéder à des tests réguliers de restauration des disques de sauvegardes pour s'assurer de leur intégrité
- ✓ De renforcer le dispositif de sécurité des salles serveurs en les munissant d'équipement de vidéosurveillance ou d'ouverture de la porte par badge électronique.

Conclusion du chapitre 4

Ce dernier chapitre de notre étude a été le cadre pratique pour la mise en œuvre de notre audit de la sécurité du système d'information au sein de l'hôpital générale de grand Yoff. Nous l'avons fait en trois phases : la phase de préparation, la phase de réalisation et phase de conclusion à l'issu desquelles nous avons pu dégager les points forts et les points faibles de la sécurité du système d'information. Des recommandations ont donc été proposées en vue d'améliorer les points faibles constatés.

CONCLUSION GENERALE

L'environnement concurrentiel des organisations est de nos jours, de plus en plus rude et sans merci. Respecter les délais de livraison et communiquer efficacement entre différentes entités d'une même compagnie deviennent des préoccupations majeures pour toute organisations, qu'elle soit petite ou grande. Une réponse efficace à ces préoccupations demeure l'automatisation de leur système d'information qui n'a cessé d'évoluer. Toutefois cette automatisation s'accompagne avec des risques qui lui sont spécifiques et qui s'ils sont mal gérés peuvent compromettre la vie de l'organisation quant à l'atteinte de ses objectifs.

Dès lors, la question de la disponibilité, d'intégrité et de confidentialité de l'information revêt pour nous une préoccupation importante. Ce qui a été l'objet de notre étude au sein de l'hôpital général de grand Yoff (HOGGY). Nous l'avons fait dans une première partie à travers une revue de littérature qui a porté sur le système d'information, les risques qui y sont associés et leur gestion. La deuxième partie a concerné le cadre pratique qui nous a permis de faire une description du système d'information de l'hôpital général de grand Yoff et de mener un audit de la sécurité du système d'information. Au terme de notre analyse nous pensons avoir globalement atteint les objectifs spécifiques de départ à savoir :

- ✓ définir les notions de systèmes d'information et de sécurité du système d'information
- ✓ analyser les risques liés au système d'information ;
- ✓ dérouler les différentes étapes d'un audit des systèmes d'information ;
- ✓ identifier les contrôles et les dispositifs mis en place par l'HOGGY et vérifier leur conformité par rapport aux lois, règlements et bonnes pratiques en la matière ;
- ✓ analyser ce dispositif pour en dégager ses forces et ses faiblesses
- ✓ proposer des recommandations permettant d'améliorer la sécurité du système d'information.

L'analyse du dispositif du système d'information nous a permis de relever des points forts et des points faibles. Les points forts devront constituer pour l'HOGGY l'objet d'amélioration continue. Pour les points faibles, ils devront faire l'objet d'une attention particulière en tenant compte des différentes recommandations proposées.

D'autres études plus techniques du système d'information, notamment concernant la sureté de son fonctionnement pourront être menées à travers l'étude de son réseau et peuvent faire l'objet de recherche. Cette étude aura pour but de prévenir certaines défaillances pouvant aller jusqu'à remettre en cause sa survie.

ANNEXES

Annexe 1 : Guide d'entretien

Avec la cellule informatique

- ✓ Existe-il un organigramme de la fonction informatique ?
- ✓ Quels sont les attributions de la cellule informatique ?
- ✓ Combien d'agents dispose la cellule informatique ?
- ✓ Disposez-vous d'une cartographie des risques informatiques ?
- ✓ Comment gérez-vous les risques ?
- ✓ Quelles sont les applications « métier » de l'HOGGY ?
- ✓ Sous quel système d'exploitation sont-elles installées ?
- ✓ Comment sauvegardez-vous les données ?

Avec l'auditeur interne

- ✓ Qui s'occupe de la Gestion des risques au niveau de l'HOGGY ?
- ✓ Existe-il un risk manager au niveau de l'HOGGY ?
- ✓ Disposez-vous d'une cartographie des risques ?
- ✓ La cartographie des risques prend-elle en compte les risques liés au système d'information ?
- ✓ Un audit de la sécurité du système d'information a-t-il été déjà effectué au niveau de l'HOGGY ?

Avec le Responsable Hygiène et sécurité

- ✓ Quelles sont les attributions du service hygiène et sécurité ?
- ✓ Disposez-vous d'un contrat de lutte contre les incendies ?
- ✓ Quelle est la périodicité de révision des extincteurs ?
- ✓ Le personnel est-il sensibilisé à la lutte contre les incendies ?
- ✓ Comment assurez-vous la sécurité physique des équipements ?

Annexe 2 : Questionnaire de contrôle interne

Entité : HOGGY **Rubrique : Gestion des risques**	**Question de contrôle interne**	**Exercice : 2016** **Folio : 1/7**

Objectifs de contrôle interne s'assurer que les risques sont évalués et gérés

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Existe-il un référentiel de gestion de risque ?	X			Cartographie en cours d'élaboration
Y a-t-il un référentiel spécifique pour la gestion des risques informatiques ?		X		
Le contexte de risque informatique est-il compris ?		X		
Les menaces sont-elles identifiées ?	X			Une cartographie est en cours d'élaboration
Existe-il un processus de gestion des risques informatiques ?		X		
Un plan d'action pour la gestion des risques est-il mis en action ?			X	
Établi par : Innocent YAO le 05/12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion de la sécurité physique**	**Question de contrôle interne**	**Exercice : 2016** **Folio 2/7**

Objectifs de contrôle interne : S'assurer d'une gestion efficace de l'environnement physiques.

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Est-ce qu'il existe une procédure pour contraindre les sites informatiques de respecter les mesures de sécurité physiques et contrôle d'accès ?		X		
Est-ce que l'accès aux sites informatiques sensibles est limité ?	X			
Est-ce que les signes d'identification des sites extérieurs sont discrets et n'identifie pas de façon formelle le site depuis l'extérieur	X			Les salles machines sont à l'intérieur des bâtiments et non identifiable de l'extérieur
Est-ce que les sites sensibles sont régulièrement contrôlés par le personnel de sécurité (même pendant le weekend) ?			X	
Est-ce qu'un règlement impose aux visiteurs d'être accompagnés ?	X			
Etabli par : Innocent YAO le 05 /12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion de la sécurité logique**	**Question de contrôle interne**	**Exercice : 2016** **Folio : 3/7**

Objectifs de contrôle interne s'assurer de l'invulnérabilité des accès logiques.

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Existe-il une authentification obligatoire avant tout accès au système?	**X**			
Existe-il une procédure pour évaluer et changer les droits d'accès au système?	**X**			
Existe-il une politique de prévention des logiciels malveillants?	**X**			L'entreprise a acquis une licence d'un an de l'antivirus BITDEFENDER et est renouvelé chaque année
Les logiciels de protections sont-ils à jour?	**X**			La mise à jour se fait automatiquement via internet
Établi par : Innocent YAO le 05 /12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion des risques du système d'information**	**Questionnaire de de contrôle interne**	**Exercice 2016** **Folio : 4/7**

Objectifs de contrôle interne : S'assurer de la gestion efficace de la sécurité du système d'information.

Questions	Oui	Non	N/A	Commentaires
L'entreprise dispose t'elle politique informatique?		X		
La politique de sécurité informatique est-elle intégrée dans la politique générale de l'entreprise?		X		
Existe-il des procédures de sécurité pour : Les ordinateurs? L'utilisation d'internet? Pour les mails?	X X X			L'accès de certain site aux heures de travail est interdit, HOGGY a acquis un domaine hoggy.sn pour les mails à déployer pour tous les utilisateurs en vue de l'envoie et réception des mails
Existe-il un organigramme informatique?		X		
Établi par : Innocent YAO le 05/12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion des mots de passe**	**Question de contrôle interne**	**Exercice : 2016** **Folio : 5/7**

Objectifs de contrôle interne s'assurer de la bonne gestion des mots de passe.

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
L'usage des mots de passe est-il généralisé sur tous les postes?	X			
Les mots de passe sont-ils renouvelés régulièrement ?	X			
Existe-il une politique formalisée à la gestion des mots de passe ?		X		
Les utilisateurs sont-ils sensibilisés à la gestion des mots de passe ?	X			
Établi par : Innocent YAO le 05 /12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion des sauvegardes**	**Question de contrôle interne**	**Exercice : 2016** **Folio : 6/7**

Objectifs de contrôle interne s'assurer que les données sont sauvegardés de manière périodique.

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Existe-il une procédure de sauvegarde des données clairement définies	X			
Disposez-vous d'une armoire spécifique pour la conservation des supports de sauvegarde?			X	
Des tests de relecture sont il fait de façon régulière sur ces support?		X		
Les supports sont-ils conservés dans un endroit suffisamment éloignés des sites sensibles?	X			Une copie des sauvegardes est sur un disque externe est conservée par le responsable de la cellule informatique
La sauvegarde concerne t elle Les serveurs? Les ordinateurs?	X		X	
Établi par : Innocent YAO le 05 /12/2016		Validé par Alioune DIOUF, administrateur réseau		

Entité : HOGGY **Rubrique : Gestion de la continuité de l'activité**	**Question de contrôle interne**	**Exercice : 2016** **Folio : 7/7**

Objectifs de contrôle interne s'assurer que la reprise de l'activité ne sera pas compromise.

Questions	**Oui**	**Non**	**N/A**	**Commentaires**
Existe-il un plan de secours des activités bien défini ?		X		
Ce plan est-il testé et évalué régulièrement ?		X		
Le personnel est-il formé aux procédures d'urgence ?	X			
Les données sont-elles sauvegardées sur un autre site à l'extérieur de l'HOGGY		X		
Établi par : Innocent YAO le 05 /12/2016		Validé par Alioune DIOUF, administrateur réseau		

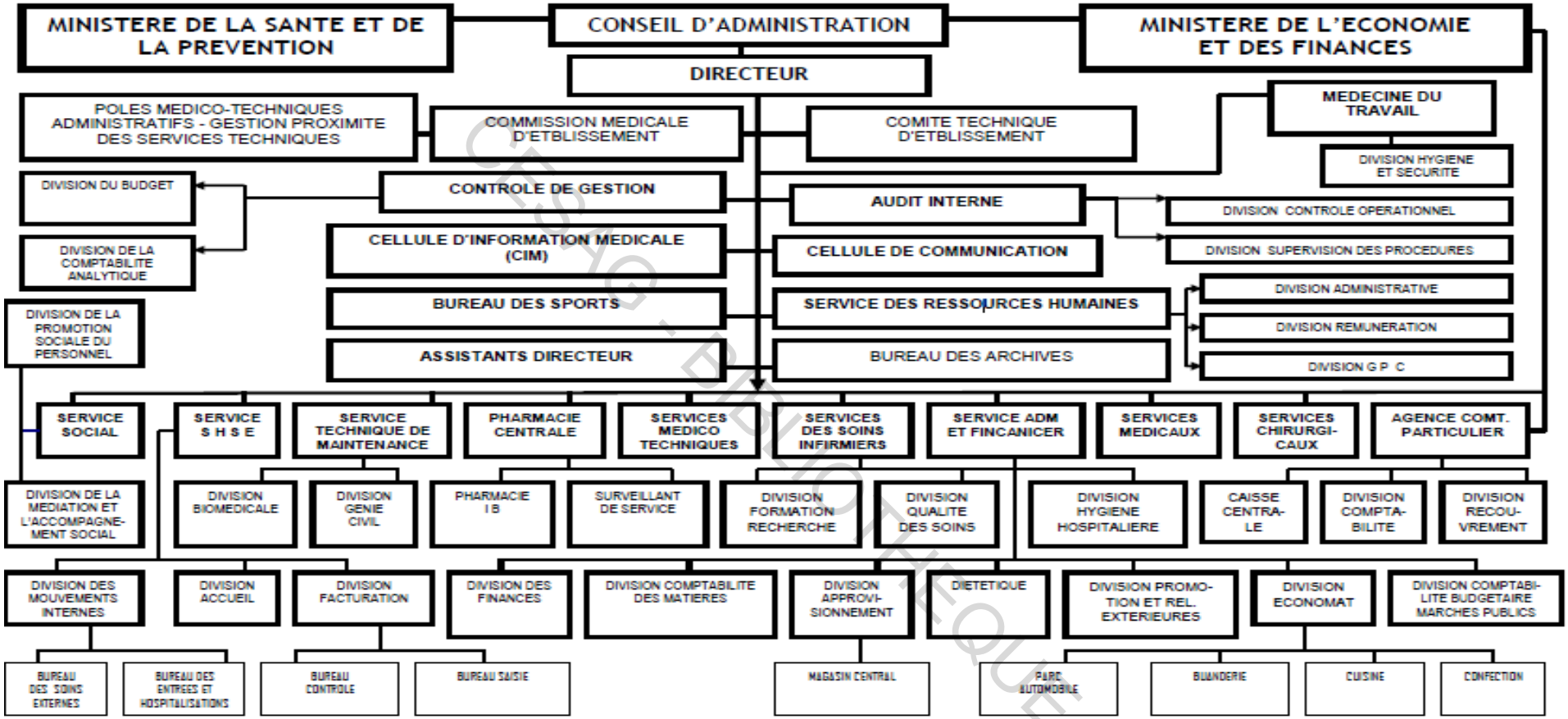
Annexe 3: Cartographie des équipements de l'HOGGY

Service	Nombre d'ordinateurs
Agence Comptable	29
Anapath	3
Anesthésie	3
Audit Interne	4
Biologie Médicale	10
Bloc Opératoire	3
Cardiologie	3
Exploration Fonctionnelle	5
Cellule communication	6
Consultation Externe	4
Cellule Informatique	3
Commission Médicale	1
Chirurgie Générale	2
Cellule Information Médicale	2
Contrôle gestion	3
Direction	2
Hémodialyse	2
IPM	2
Maternité Gynécologie	3
Kinésithérapie	2
Médecine Interne	2
Médecine Nucléaire	4
Neuro Chirurgie	4
Ondonto	3
Ophtalmo	3
ORL	3
Orthopédie	4
Pédiatrie	3
Pharmacie	10
Radiologie	10
Ressource Humaine	9
Service administratif et financier	18
Service Social	2
Hospitalisation et soins externes	21
Service technique et maintenance	3
Urgence	3
Urologie	4
TOTAL	**198**

Autres équipements	Nombre
Onduleurs	59
Imprimantes	94
Switches	24

Source : Service Technique et Maintenance

Annexe 4 : Organigramme de l'HOGGY



Source : Service Contrôle de Gestion de l'HOGGY

BIBLIOGRAPHIE

Ouvrages

1. CALE Stéphane (2007), *La sécurité informatique : Réponses techniques, organisationnelles et juridiques*, édition LAVOISIER, Paris, 282 pages.
2. CHAI (2014), *Guide d'audit des systèmes d'information*, CHAI, 112 pages.
3. CIGREF, IFACI, AFAI (2009), *Gouvernance des systèmes d'information : guide d'audit*, IFACI, 106 pages.
4. COSO II Report (2009), *Le management des risques de l'entreprises*, édition d'organisation, Paris, 338 pages.
5. DARSA Jean-David (2014), 365 *risques en entreprises*, 2ème édition, Gereso, Le Mans 420 pages.
6. DEIXONNE Jean Luc (2007), *Piloter un projet ERP : transformer l'entreprise par un système d'information intégrer et orienté métier*, 2ème édition, Dunod, Paris, 263 pages.
7. DEXONNE Jean Luc (2011), *Piloter un projet ERP : transformer l'entreprise par un système d'information intégrer et orienté métier durablement*, 3ème édition, Dunod, Paris 304 pages.
8. DEYRIEUX André (2004), *Le système d'information, nouvelle outil de stratégie : direction d'entreprise et DSI*, édition Maxima, Paris, 185 pages.
9. DOMNIQUE Moissand, FABRICE Garnier de Labareyre (2009), *Cobit pour une meilleure gouvernance des systèmes d'information,* Eyrolles, Paris 258 pages.
10. GILLET Michelle, GILLET Patrick (2010), *Management des systèmes d'information*, Dunod, Paris, 459 pages.
11. GILLET Michelle, GILLET Patrick (2011*), Les systèmes d'information de A à Z*. Dunod, Paris, 215 pages.
12. GRAEVE, Jean de POITIER (2001), *Système d'information, Management et Acteurs*, Les éditions SAPIENTIA, Paris, 135 pages.
13. IFACI (1993*), Audit et contrôle des systèmes d'information*, module 8, sécurité, IFACI, 126 pages.

14. IFACI (1993), *Audit et contrôle des systèmes d'informations*, module 1 : Management de l'audit et du contrôle interne, IFACI, 110 pages.
15. IFACI (1993), *Audit et contrôle des systèmes d'informations*, *module 2 : Les outils informatiques de l'audit*, IFACI, 129 pages.
16. ISACA (2013), *Manuel de préparation du CISA 2013*, Rolling Meadows, USA.
17. JIMENEZ Christian, MERLER Patrick et CHELLY Dan (2008*), Risques opérationnels : de la mise en place du dispositif à son audit*, Edition Revue Banque, Paris, 273 pages.
18. KEREBEL Pascal (2009), *Management des risques, Edition d'Organisation*, Paris, 184 pages.
19. MADERS Henry Pierre et MASSELIN Jean Luc (2006), *Contrôle interne des risques, Edition d'Organisation,* Paris, 261 pages.
20. MONACO Laurence (2014), *Les carrés DCG8- Système d'information de gestion,* 3ème édition, édition Gualino, Paris, 224 pages.
21. NGUENA Octave Jockung (2008), *Management des risques*, Ellipse, 188 pages.
22. REIX Robert (2002), *Système d'information et management des organisations*, 4ème édition, Vuibert, 444 pages.
23. REIX Robert, FALLERY Bernard, KALILA Bernard et ROWE Frantz (2011), Système d'information et management des organisations, 6ème édition, Vuibert, Paris, 472 pages.
24. RENARD Jacques (2010), *Théorique et pratiques de l'audit interne*, 7ème édition, Paris, Edition d'Organisation, Paris, 470 pages.
25. RENARD Jacques (2013), *Théorie et Pratique de l'audit interne*, 8ème édition, Eyrolles, Paris, 452 pages.
26. SCHICK Pierre (2007), *Mémento d'audit interne : méthode de conduite d'une mission*, Dunod, Paris, 217 pages.
27. THOMAS Jean-Louis (2007), *ERP et PGI. Sélection, Méthodologie de déploiement et gestion du changement*, 5ème édition, Dunod, Paris, 328 pages.
28. THORIN Marc (2000), *L'audit informatique*, édition HERMES Sciences, Paris, 184 pages.

Revue

1. Alter S.L. (1996), Information systems: a management perspective*, Cummings Publishing Company Inc*., Canada.
2. GIARD, V. (2003), Gestion de production et des flux, *Economica*, Paris
3. REIX Robert (2007), La spécificité de la recherche francophone en système d'information, *revue française de Gestion* (n° 176).

Sites internet consultés

1. ISO/IEC 27002 (2013), *Système de management de la sécurité de l'information-exigences,* http://www.iso.org/iso/fr/catalogue_detail? Consulté le 04 juillet 2016.
2. http://www.journaldunet.com/management/pratique/vie-de-l-entreprise/15293/charte-informatique-que-contient-elle.html (Octobre 2016)
3. PESENTI Emmanuel (2016), *Gouvernance et modélisation du SI* http://ea-is.blogspot.sn/2011/03/systeme-informatique-ou-systeme.html,

TABLE DE MATIERE